International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

The Proposed Framework for Cloud Computing System Security and Privacy Services

Neerav Nishant[1], Vaishali Singh[2]
[1]Research Scholar
Department of Computer Science & Engineering
Maharishi University of Information Technology
Lucknow, India
contactnnishant@rediffmail.com
[2]Assistant Professor
Department of Computer Science & Engineering
Maharishi University of Information Technology
Lucknow, India
singh.vaishali05@gmail.com

Abstract— Public cloud computing has emerged as a popular and efficient solution for organizations to store, process, and access their data and applications. However, with the increasing adoption of public cloud services, concerns regarding security have become a critical factor in decision-making processes. This study aims to investigate the security aspects of public cloud computing and identify potential vulnerabilities and threats that organizations may face. The aim of this study is to examine the challenges associated with cloud computing and its security concerns. Cloud computing is a technology that utilizes the internet to share data and resources. It is characterized by five key features: On-Demand self-service, Resource Pooling, Broad network access, Rapid elasticity, and Measured Service. However, despite these benefits, cloud computing has several open issues, including Security, Availability, Scalability, and Interoperability. Traditional security techniques are insufficient in fully securing cloud computing. Security and privacy issues often arise during cloud deployment and delivery models. As a result, researchers are interested in learning more about cloud computing security and its methods. Industries are creating architectural models with a high level of protection for their data center to solve current security challenges. This article examines the security of cloud deployment strategies and analyzes cloud security and privacy challenges. The cloud computing service models are also discussed, along with any security issues. The study emphasizes the significance of Audit as a key factor in offering a security solution that covers all relevant security characteristics as determined by the literature. The study's conclusions present a fresh challenge to cloud service providers and suggest a new security paradigm that explains customer security needs. Overall, this study offers a parameter-by-parameter assessment of available security solutions and makes recommendations for enhancements to address cloud security issues.

Keywords- Cloud computing, Cloud Deployment Models, Cloud Security, Security, Services.

I. INTRODUCTION

The internet is a vast network that connects various resources globally. It allows us to access any service or information we require instantly. This has given rise to cloud computing, which refers to the remote access to computing resources provided by third-party services connected to the public internet. The cloud computing market is the fastest-growing segment in the IT industry, and it is revolutionizing the way businesses operate. Cloud computing has evolved from various other computing models such as distributed computing, utility computing, grid computing, P2P computing, virtualization, and server clusters [14]. Cloud computing focuses primarily on web-based applications and provides flexible sharing of IT resources such as software, hardware, and operating systems over the internet. Cloud service models, cloud storage, and cloud providers like Microsoft Azure, Amazon EC2, Salesforce.com, Google App Engine (GAE), 3Tera, IBM Blue Cloud, etc., enable this sharing of IT resources. Cloud computing is like having a magic computer that can give you anything you need, like games or homework help. There are three types of things it can give you: software, platforms, and infrastructure. Software is like apps you can use on the internet, like Facebook or Google. Platforms are like tools that help you make your own apps or websites. Infrastructure is like the stuff that makes the internet work, like servers and storage. Different deployment models for cloud computing are also discussed, including private, public, hybrid, and community clouds. Private cloud is geared towards a single organization and offers many benefits of distributed computing, while public and hybrid clouds are available to multiple tenants. Public cloud may be more cost-effective, while hybrid cloud offers greater customization and control. Community cloud is tailored to a specific industry or region and is shared by multiple organizations. Overall, provides an overview of various aspects of cloud computing and highlights its potential benefits for businesses and industries [13].

Infrastructure as a Service (IaaS) offers network capacity, internet processing, and storage of information in a virtualized setting. IaaS offers a collection of programming interfaces for applications that let users manage and interact using the system's components in other ways and its benefits, as well as different deployment models for cloud computing [15]. IaaS includes storage, network resources, and processing power, and is often referred to as utility computing. The benefits of cloud computing include speed and ease of deployment, as well as improvements to the economics of various industries. The Cisco and National Institute of Standards and Technology (NIST) definitions of cloud computing are provided, with both emphasizing on-demand access to scalable resources that shows in Fig. 1.

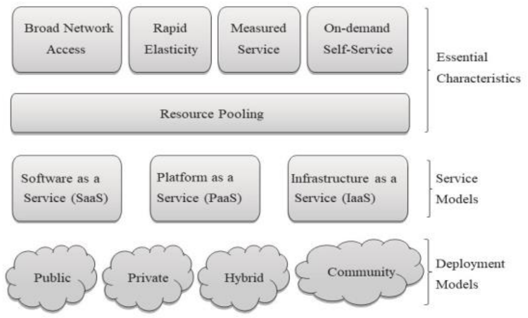

Fig. 1. National Institute of Standards and Technology model of cloud computing [1].

Service-oriented architecture PaaS refers to a cloud-based platform for creating and releasing applications, and it is built on top of the infrastructure provided by IaaS. Developers can use the service provider's given programming languages and tools to launch apps with PaaS. This service provides the essential infrastructure to back the full application development and distribution lifecycle for internet-accessible web apps and services, and it also provides application building blocks for configuring new business applications. Google App Engine, Microsoft Azure, Engine Yard, and Collabnet are only few of the providers of platform as a service.

SaaS, sometimes known as "on-demand software," is constructed atop IaaS and PaaS. It offers a variety of business apps that may be used by either individuals or corporations. SaaS is the most widely used cloud service and may be accessed by virtually anybody with an internet connection. Salesforce.com, Google Docs, and Microsoft Online Services are just a few examples of the many successful SaaS services aimed at both consumers and businesses. These programs can be accessed from any client device with a thin client interface, like a web browser.

Table 1. Cloud Deployment Model’s Concerns

Model	Operated by	Maintained by
“Public”	External “CSP”	External “CSP”
“Private”	Client or external “CSP”	Client or external “CSP”
“Hybrid”	Client and external “CSP”	Client and external “CSP”
CSP, Content service provider		

Table 1 demonstrates the variety of cloud deployment techniques available in terms of control, ownership, location, and access to data.

1.1. Public

Public cloud is a service provided by one service provider to numerous clients who simultaneously share the cloud's computing resources. Applications, processing power, network resources, and data storage space are shared by clients using public clouds. According to the resource, various levels of categorization are offered.

1.2. Private

A single organization is the only customer for a private cloud. The cloud could contain many different divisions, yet they all belong to the same company. Virtualization is used in many private clouds to maximize the use of an organization's existing server infrastructure [16]. Fast deployment and removal are possible because of the provisioning and metering infrastructure present in a private cloud. This paradigm is like the common approaches to IT outsourcing, but it can also be used within an organization. Many different private cloud architectures are now in use.:

1. Dedicated private cloud: These are managed by internal IT teams and housed in customer-owned data centers or collocation facilities.
2. Community private cloud: These are hosted elsewhere by a provider that is responsible for their upkeep and is bound by service level agreements (SLAs) and other contractual provisions that ensure their security and compliance.
3. Managed private cloud: In this setup, the customer owns the underlying infrastructure but a third-party handles management.

1.3. Virtual Private

A virtual private cloud, or VPC, is a kind of private cloud that functions as an extension of the larger shared or public cloud, often known as the "Inter-cloud." The Inter-cloud is made up of various clouds and aging technology that are all linked together. Through Amazon Virtual Private Cloud, offered by Amazon Web Services, the Amazon Elastic Compute Cloud service may be linked to on-premises hardware by way of an IPsec virtual private network. The Secure Data Connector service offered by Google App Engine accomplishes the same goals.

1.4. Hybrid

A combination of two or more of the deployment patterns is known as a hybrid cloud. In comparison to the other deployment methods, each of the three cloud deployment models has unique benefits and drawbacks. A hybrid cloud makes use of the benefits of various cloud models to offer users a better overall experience. Users can get levels of failure tolerance and locally quick usability by employing the hybrid cloud architecture without relying on Internet connectivity.

The study begins by analyzing the fundamental security challenges associated with public cloud environments, including data breaches, unauthorized access, and insider threats. It then delves into the security measures provided by cloud service providers, such as encryption, authentication, and access control mechanisms. Additionally, the study examines the shared responsibility model, which clarifies the division of security responsibilities between cloud service providers and their customers. Furthermore, the research explores various security best practices and strategies that organizations can adopt to enhance the security of their cloud-based systems. It investigates the importance of regular security assessments, incident response plans, and the implementation of robust security controls. The study also highlights the significance of employee awareness and training programs to mitigate human-related security risks.

To gain insights into real-world challenges and practices, the study conducts a comprehensive review of existing literature, industry reports, and case studies on public cloud security. It analyses notable security incidents and breaches in the public cloud domain, examining the underlying causes and the subsequent lessons learned. Based on the findings, this study offers recommendations for organizations to strengthen their security posture in public cloud computing. It emphasizes the need for a holistic and proactive approach to security, encompassing a combination of technical controls, policy frameworks, and ongoing monitoring. The study concludes with insights into future trends and developments in public cloud security, such as the integration of artificial intelligence and machine learning for threat detection and prevention.

Overall, this study contributes to the existing body of knowledge by providing a comprehensive analysis of the security aspects of public cloud computing. It equips organizations and decision-makers with valuable insights to make informed choices, mitigate risks, and ensure the confidentiality, integrity, and availability of their data and applications in the public cloud environment.

II. FUNDAMENTALS OF CLOUD SECURITY

Securing cloud computing systems has become a critical concern for businesses and organizations of all sizes. As more data is being stored and processed on the cloud, the risk of cyber-attacks and data breaches has increased significantly. Therefore, it is essential to implement robust security measures to protect cloud computing systems from potential threats. One of the most effective ways to secure cloud computing systems is to use multi-factor authentication. This method requires users to provide two or more authentication factors to access the system, such as a password and a biometric scan. This helps to ensure that only authorized users are granted access to the system, reducing the risk of unauthorized access and data breaches. Another important security measure is to encrypt all data stored on the cloud. Encryption is the process of converting data into a code that can only be read by authorized users with the decryption key. This helps to protect sensitive data from unauthorized access, even if it is stolen or intercepted by cybercriminals.

Regular system updates and patches are also crucial to maintaining the security of cloud computing systems. These updates often address security vulnerabilities and fix bugs that can be exploited by hackers. Therefore, it is essential to keep the system up to date with the latest security patches and updates. In addition, businesses should implement a strong password policy to prevent unauthorized access to cloud computing systems. This policy should require users to create strong passwords that are difficult to guess and should be changed regularly. Furthermore, businesses should conduct regular security audits of their cloud computing systems to identify potential vulnerabilities and threats. These audits can help to identify security gaps and provide recommendations for improving the security of the system [20].

Today, protecting a network is an essential aspect of providing any kind of online service. Since more and more of our daily business is conducted online, safety measures have become paramount. Network security is especially challenging to manage in a dynamic and demanding setting like cloud computing. In addition to saving money on infrastructure, cloud computing also frees up time and energy for employees to concentrate on running their businesses rather than maintaining their IT infrastructure. A wide range of technologies, including virtualization, autonomic-computing, grid-computing, and many more [1], have contributed to the development of cloud computing. New technologies often come with fresh problems to solve. The provision of sufficient security to cloud is the most critical challenge for effective operation. Securing a cloud computing infrastructure is not radically different from securing any other information technology infrastructure. Cloud computing, on the other hand, may pose new hazards to an organization that aren't present in the case of traditional IT solutions. These risks may be attributable to the cloud service models used, their operational models, and the technologies used to allow cloud services. There are basically three main security objectives of the cloud computing system:

Confidentiality: To maintain privacy, data must be protected from accidental or malicious disclosure. Intellectual property rights, covert channels, traffic analysis, encryption, and inference all play a role in keeping cloud-based systems secure and private.

Integrity: Assuring that data has not been tampered with while being transferred over a network and protecting it against deletion and unlawful change.

Availability: The accessibility of cloud information is guaranteed by its availability. Availability ensures that systems may be accessed and used when necessary. Furthermore, this idea ensures that the cloud system's security services are operational. Availability can be threatened, for instance, by a denial-of-service assault.

However, two additional goals can be included to the previous list in view of the development of novel technologies and hazards.

Authentication: confirming the identity of the party carrying out the communication.

Auditing: Systems inspections and monitoring are the two primary tools used by businesses for regulating operational assurance. Depending on the assets' design and deployment, either the cloud customer or the cloud service provider can use these strategies. To begin, a system audit is an occasion, either once or repeatedly, at which security is assessed. Second, when we talk about monitoring, we're referring to ongoing actions that investigate the system or the users, such as identifying attacks.

Finally, in the event of a security breach or data loss, it is crucial to have a disaster recovery strategy in place. Data backup, restoration, and business continuity protocols should all be part of this plan to lessen the blow of any security breaches.

III. PROPOSED CLOUD SECURITY FRAMEWORK

The Internet's primary design goal was resilience, not security. A distributed application's attack surface is substantially larger than that of a locally hosted one. Pooled, virtualized, and outsourced resources introduce new vulnerabilities into cloud computing, on top of those inherent to Internet-based applications. When it comes to cloud security, not all service models are created equal [7]. When it comes to built-in security, we'll get the least from an Infrastructure as a Service provider and the most from a SaaS one. Because of this, the cloud service model and cloud environment in which we place our applications each have their own unique set of hazards. Safety in the cloud must be implemented on both the provider and user sides. The Cloud service provider is responsible for protecting the server from any potential outside attacks. When it comes to protecting their customers and end users, the cloud computing service provider has delivered. The user must ensure that their actions will not result in the loss of data, the theft of data, or the alteration of data for other users of the same cloud. Only if the cloud service provider takes security properly for its customers will they be considered an appropriate choice. Therefore, based on the security we have proposed a security framework for the cloud computing-based system to protect the data and maintain the privacy issues in the frameworks shown in Fig. 2.

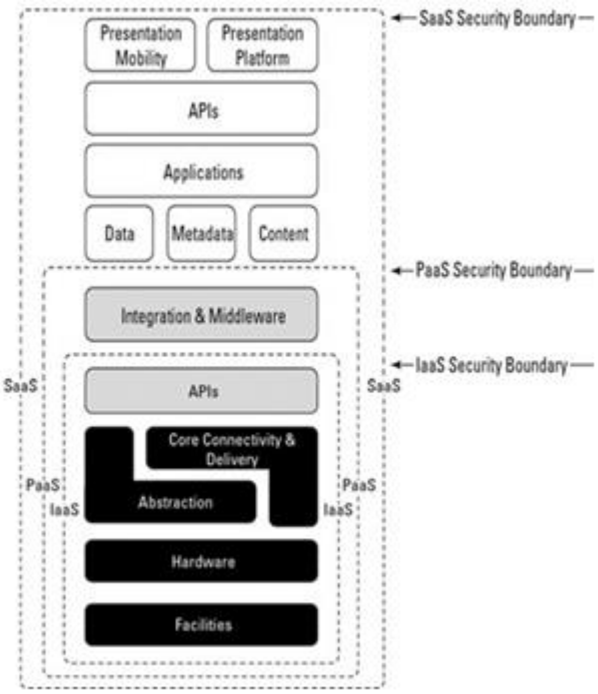

Fig. 2. Proposed framework for the cloud security

Every individual cloud service delivery system is described in the Cloud Reference Models architecture, along with the security boundary that marks the point at which the cloud service provider's obligations end and the customer's obligations begin [9] [11]. Any security measure below the security boundary must be integrated into the system, and any measure above it must be kept up to date by the client. As we advance up the stack, it is more crucial than ever to include security type and level in our service level agreement.

Each service model inherits all the underlying security problems and risk considerations, as well as the capabilities of the model contained within it. SaaS is an operating environment containing applications, management, and the user interface, whereas IaaS provides the infrastructure and PaaS includes application development frameworks, transactions, and control structures. IaaS has the lowest levels of integrated functionality and integrated security as we advance up the stack, whereas SaaS has the highest levels [21]. With the compliance, governance, and responsibility levels outlined in the contract for the whole stack, the vendor in the SaaS model delivers security as part of the Service Level Agreement. The vendor may set the security barrier for the PaaS model to cover the middleware layer and software framework. In the PaaS paradigm, the client would oversee the application's and user interface's top-level security. The IaaS approach, where anything involving software of any kind is the customer's concern, has the least security built into it.

IV. SECURITY ISSUE IN CLOUD COMPUTING

There are several advantages and disadvantages to using cloud computing. When considering the obstacles, security is a major roadblock for cloud computing to overcome. Applications, platforms, and infrastructure are all parts of what make up cloud computing. Each division is responsible for distinct tasks and sells a variety of products to customers all around the globe. Networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control, and memory management are just a few of the many technologies involved in cloud computing, which raises a wide range of security concerns [6]. Cloud computing raises security concerns for many of these systems and technologies [4][5]. For instance, a cloud's interconnected systems necessitate a safe and reliable network. There are also other security issues because of the virtualization concept used in cloud computing. For instance, the process of securely mapping virtual computers to actual machines must be implemented. Cloud computing location transparency is a significant form of adaptability. Data protection act provisions in various regions may be significantly impacted and breached if the precise location of data storage is unknown. As a result, protecting cloud users' privacy is a major issue in the cloud. Encrypting data and enforcing strict rules for its dissemination are both essential components of data security. The following are some of the main privacy and security issues with cloud computing.

4.1. Multiple Safety Challenges

4.1.1 Data storage location

Depending on the terms of their contracts, some clients are unaware of the location of their data.

4.1.2 Restoration

To preserve customer data, every cloud service needs to have a disaster recovery plan.

4.1.3 Support for inquisitiveness

If a client detects improper behavior by the provider, there may not be many legal avenues open to it to pursue an inquiry.

4.1.4 Data isolation

Since encrypted data from many firms may be kept on the same hard drive, the supplier should have the tools to separate data. Data ownership requires businesses to spend the necessary time learning as much as they can about their service providers and local laws, and they frequently begin by granting privileged users access to extremely low-risk apps.

4.1.5 Regulatory compliance

Since they have the option to select a provider who welcomes audits from impartial, independent security organizations or one who does not, customers are on guard for the security of their solution.

4.2. Privacy in Cloud Computing

Consumer services like email, social networks, and virtual worlds are currently the most well-known cloud applications. Terabytes of sensitive data are gathered by the firms running these services and stored in data centers in several nations. A basic human right is the right to privacy. The "right to be left alone" and "control of information about ourselves" are just two examples of several types of privacy [10]. To build a risk/benefit analysis, it can be useful to start with a taxonomy of privacy that focuses on the negative effects that result from breaches of privacy.

Cloud consumers require assurances that their private data will not be misused by the cloud provider.

Cloud service providers should set privacy policies that fit their business strategy. They should disclose such policies and offer clients fair advance notice of any modifications. They need to let clients decide on such adjustments when necessary.

V. MANAGE CLOUD COMPUTING SYSTEM ISSUES

First, we must protect any devices that are openly connected to the Internet from the usual risk of illegal access. Second, we need to safeguard information while it travels across the network, and third, we must prioritize getting high-quality, trustworthy connections to the cloud.

5.1. Limiting Network Access Via Safety Groups

In Fig. 2, we see how the network is partitioned into secure sub networks. While firewalls are mostly used to divide networks, they can also serve as a helpful supplementary layer when combined with other network restrictions. This is especially useful when many subnets use the same directory service. A security group (SG) in a PaaS environment can function as a firewall, allowing the customer to control which network protocols and ports are accessible from the outside world. A security group in Amazon EC2 is a collection of firewalls ACCEPT rules for incoming TCP, UDP, or ICMP packets. When an instance is launched with a specific Security Group (SG), the rules for that SG's distributed internal firewall are applied to that instance [17].

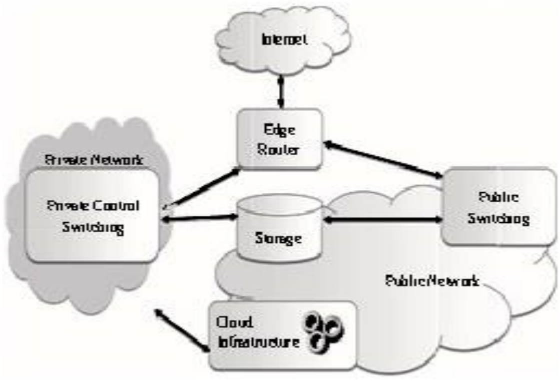

Fig. 3. Network Separation via Safety Groups.

5.2. Prevent physical access to servers and application

One of the most salient features of cloud computing is that it enables users to "self-service." It's a way to gain access to a large pool of servers over the web. Typically, only direct, or on-premises connections are allowed between administrators and servers in conventional data centers. This administrative access with cloud computing must be done over the Internet, which increases vulnerability and risk. Restricting and monitoring administrative access is crucial for keeping track of who makes what changes to the system and why. Problems with data access typically stem from lax security measures taken to protect user information [22].

5.3. Securing data within the cloud

Cloud security challenges revolve around sensitive data.

Although the information stored in the cloud might be common, private, or sensitive, anybody can access it anytime, anywhere. Many cloud computing service consumers and providers edit data simultaneously. Cloud-based computing requires data integrity methods.

Theft of data is an important issue in the cloud computing environment.

One of the most frequent issues with cloud storage is data loss. There is an opportunity for data loss for users of cloud computing services if the company goes out of business or takes legal action. Moreover, data can be lost or damage or corrupted due to miss happening, natural disaster, and fire. Due to the above condition, data may not be accessible to users.

Data placement is a cloud computing issue. Data location is vital. Cloud security is the biggest issue. It's crucial that users can't see each other's Internet traffic. Multi-tenant networking risk. Cloud users can construct encrypted VPN connections between their cluster and corporate infrastructure using open networking. This system encrypts data end-to-end for large clients. Authentication, integrity, and non-modification ensure data travels where the client wants it. SSL/TLS are utilized here.

5.4. Virtual Protection

Virtualization is one of a cloud's essential elements. Virtual machines are dynamic, meaning they may be readily paused, resumed, and swiftly returned to earlier instances. One of the main tasks of virtualization is to guarantee that several instances running on the same physical computer remain isolated from one another. Additionally, they may be easily copied and transferred across physical servers [24]. It is challenging to develop and maintain continuous security because of this dynamic nature. It's possible for vulnerabilities or setup mistakes to spread unintentionally. Additionally, it is challenging to keep an auditable record of a virtual machine's security status at any given time.

5.5. Providing Network Security

The infrastructure and network that are employed in a standard enterprise setting can be clearly defined in terms of utilization. Because traffic is predictable, it is possible to set up a very static network setup that only permits the predicted types of traffic while blocking all others. The likelihood of being a victim of hostile assaults by other tenants (or against them) is, of course, nil in a single tenant scenario [25]. When we go to a multi-tenant public cloud environment, everything changes. We now have diversified, unpredictable networking traffic that might alter drastically from hour to hour. As a result, it's critical to maintain a top-notch networking infrastructure for a variety of very distinct needs. The first thing to realize is that a general-purpose network won't ever operate as predictably and efficiently as a dedicated network for a particular purpose.

VI. CLOUD SECURITY MONITORING AND SAFETY PROCEDURE

It is recommended that all network devices, servers, and applications have their security logs automatically collected. For legal reasons and so that they may be queried in the event of an alert, it is important to keep these records in their original formats. Threats can be identified, vulnerabilities can be disclosed, an audit trail can be maintained, and forensics may be made possible with the help of security monitoring. Logs from the operating system (such as event logs and syslogs), applications, IDS/IPS systems, antivirus software, network devices, and storage devices are likely to contain information on security incidents. These security events are bundled into streams and sent off to a centralized collecting service, often a Security Information and Event Management (SIEM) system, over a network. In Fig. 4 shows all the stages in the lifecycle of security monitoring.

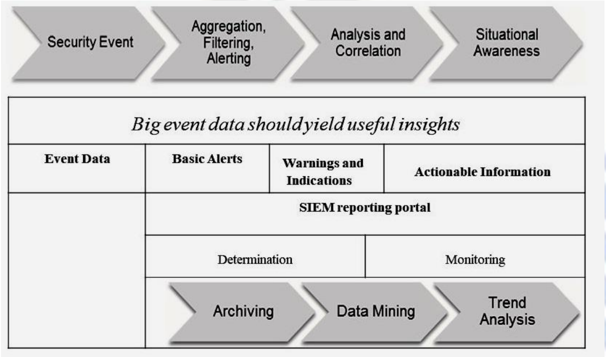

Fig. 4. Lifecycle of Security Monitoring

The data security in the cloud is paramount because of the sheer volume of users and the sensitive nature of the information stored there. Encryption algorithms serve a crucial role in ensuring safe online communication. It's the primary method of keeping sensitive information safe. An encryption algorithm takes "the key" and transforms the data or plaintext message into cipher text, which may then be decrypted by the user. One and the same key is utilized for both the encryption and decryption processes in symmetric key encryption. Asymmetric key encryption is another option; this method employs a pair of keys, called a private key and a public key, to encrypt data. Encryption is performed using the public key, and decryption uses the private key [12].

We are presenting some popular security algorithms used for data security in cloud computing.

RSA algorithm: The RSA algorithm, developed by Rivest, Shamir, and Adleman (RSA), has become the standard for Public Key cryptography [18]. To put it simply, RSA is a public-private key encryption/decryption technique. The public key is accessible to the public and is used to encrypt messages, while the private key is required to decrypt them. Therefore, in our Cloud infrastructure, the Public-Key is accessible to everyone, while the Private-Key is only known to the data's original owner. Thus, the Cloud service provider encrypts data and the Cloud user or consumer decrypts it. After information is encrypted with the Public Key, only the associated Private-Key may decrypt the information.

DES algorithm: One of the most used symmetric key algorithms is Data Encryption Standard (DES). The National Institute of Standards and Technology (NIST) officially endorsed it as the first encryption standard. The entire communication is encrypted and transformed into 64-bit cipher text blocks [19]. Encryption and decryption both make use of the same algorithm and key. This method takes a 64-bit key as input but uses a 56-bit key internally. The disadvantages of DES include that it is only fast in hardware and not in software, and that the key used in DES is relatively little and its security can be broken easily.

AES algorithm: NIST now recommends using Advanced Encryption Standard (AES) instead of DES for symmetric key encryption [23]. The only known assault that can break its encryption is a brute-force attack, in which the attacker systematically attempts every possible combination of letters. Block ciphers describe both AES and DES. The key length of these ciphers' ranges from 128 bits to 192 bits to 256 bits. Fast and adaptable, AES encryption is a must-have. It's adaptable to many systems and particularly useful for use in portable gadgets.

Instructions for ensuring cloud computing system security:

1. Make use of certificates and encrypt all confidential data.
2. Don't utilize the vendor-supplied default passwords and other security parameters; instead, provide strong authentications for all remote users.
3. Maintain isolation by utilizing exclusive (virtual) networks and IP address spaces.
4. Offer geographic independence by allowing virtual machines and networks to be physically positioned in any data center.
5. Install antivirus software on every hardware.
6. Configure a firewall and keep it up to date. Use firewall technology anywhere you can, and block unused services, ports, and protocols [3].
7. Instruct everyone on "safe Internet skills."

Cloud computing is a developing technology. Experts in the field of security are working to handle the new threats that constantly emerge. To take advantage of the cheap cost and increased flexibility provided by this revolutionary technology, businesses who are considering a move to the cloud should proceed with caution and carefully analyze the dangers. There are security concerns as the number ofbusinesses using cloud services continues to grow rapidly. The security of shared resources and data is a major concern with the cloud computing concept. In this study, we've laid out the many security and privacy concerns and future research directions in cloud computing. The report also offered solutions to these problems. The paper provided general cloud security recommendations as well. In conclusion, securing cloud computing systems is essential to protecting sensitive data and preventing cyber-attacks. By implementing robust security measures such as multi-factor authentication, encryption, regular updates and patches, strong password policies, security audits, and disaster recovery plans, businesses can ensure the safety and security of their cloud computing systems.

VII. CONCLUSION

Cloud computing is a developing technology. Experts in the field of security are working to handle the new threats that constantly emerge. To take advantage of the cheap cost and increased flexibility provided by this revolutionary technology, businesses who are considering a move to the cloud should proceed with caution and carefully analyze the dangers. There are security concerns as the number of businesses using cloud services continues to grow rapidly. The security of shared resources and data is a major concern with the cloud computing concept. In this study, we've laid out the many security and privacy concerns and future research directions in cloud computing. The report also offered solutions to these problems. The paper provided general cloud security recommendations as well. In conclusion, securing cloud computing systems is essential to protecting sensitive data and preventing cyber-attacks. By implementing robust security measures such as multi-factor authentication, encryption, regular updates and patches, strong password policies, security audits, and disaster recovery plans, businesses can ensure the safety and security of their cloud computing systems

REFERENCES

[1] Buyya R., Broberg J., Goscinski A. (2010). Cloud Computing: Principles and Paradigms, John Wiley & Sons, Vol. 87.

[2] Mohammed M. (2014). Alani: Securing the cloud: threats, attacks and mitigation techniques, Journal of Advanced Computer Science and Technology, Vol. 3, No. 2, pp. 202-213.

[3] Buecker A., Lodewijkx K., Moss H., Skapinetz K., Waidne M. (2009). Cloud security guidance, IBM Red Paper 2009, p. 12.

[4] Padhy R.P., Patra M.R., Satapathy S.C. (2011). Cloud computing: security issues and research challenges, IRACST-International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 11.

[5] Tiwari P.K., Mishra B. Cloud computing security issues, challenges and solution, International Journal of Emerging Technology and Advanced Engineering. Vol. 2.

[6] Prince Jain: security issues and their solution in cloud computing, International Journal of Computing & Business Research.

[7] Anantwar R.G., Chatur P.N., Anantwar S.G. (2012). Cloud computing and security model: a survey, International Journal of Engineering Science and Innovative Technology (IJESIT), Vol. 1.

[8] Tim M., Subra K., Shahed L. (2009). Cloud security and privacy: an enterprise perspective on risks and compliance, O' Reilly Media, USA.

[9] Barrie S. (2011). Cloud Computing Bible, Wiley Publishing Inc.

[10] Pearson S., Azzedine B. (2010). Privacy, security and trust issues arising from cloud computing, 2010 IEEE Second International Conference Cloud Computing Technology and Science (CloudCom), pp. 693-702.

[11] Hamouda S.K., Glauert J. Security, Privacy and Trust Management Issues for Cloud Computing, Taylor & Francis Group.

[12] Shakeeba S.K., Tuteja R.R. (year). Security in cloud computin using cryptographic algorithms, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3.

[13] Oztemel, E., Gursev, S. Literature review of Industry 4.0 and related technologies. J Intell Manuf 31, 127–182 (2020). https://doi.org/10.1007/s10845-018-1433-8

[14] P. D. Kaur and I. Chana, "Unfolding the Distributed Computing Paradigms," 2010 International Conference on Advances in Computer Engineering, Bangalore, India, 2010, pp. 339-342, doi: 10.1109/ACE.2010.80.

[15] Jouini, M., & Rabai, L. B. A. (2019). A security framework for secure cloud computing environments. In Cloud security: Concepts, methodologies, tools, and applications (pp. 249-263). IGI Global.

[16] Dhaya, R., Kanthavel, R., & Venusamy, K. (2021). Dynamic secure and automated infrastructure for private cloud data center. Annals of Operations Research, 1-21.

[17] Bolívar, H., Parada, H. D. J., & Roa, O. (2019, October). Modeling cloud computing security scenarios through attack trees. In 2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI) (pp. 1-6). IEEE.

[18] Barrett, P. (2000, December). Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor. In Advances in Cryptology—CRYPTO'86: Proceedings (pp. 311-323). Berlin, Heidelberg: Springer Berlin Heidelberg.

[19] Hamouda, B. E. H. H. (2020). Comparative study of different cryptographic algorithms. Journal of Information Security, 11(3), 138-148.

[20] Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.

[21] Josyula, V., Orr, M., & Page, G. (2011). Cloud computing:

Automating the virtualized data center. Cisco Press.

[22] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.

[23] Pandey, S., & Farik, M. (2017). Best symmetric key encryption-A Review. International Journal of Scientific & Technology Research, 6(6), 310-312.

[24] Kosta, S., Aucinas, A., Hui, P., Mortier, R., & Zhang, X. (2012, March). Thinkair: Dynamic resource allocation and parallel execution in the cloud for mobile code offloading. In 2012 Proceedings IEEE Infocom (pp. 945-953). IEEE.

[25] Varghese, B. et al.: Cloud Futurology Computer. 52, 9, 68–77 (2019). https://doi.org/10.1109/MC.2019.2895307.