iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VII **Month of publication:** July 2024

DOI: https://doi.org/10.22214/ijraset.2024.63567

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 12 Issue VII July 2024- Available at www.ijraset.com

A Review: Security Mechanisms in Cloud Computing

Vikas Kumar
Assistant Professor, Department of Computer Applications, Galgotias College of Engineering and Technology, Greater Noida, India

Abstract: ***Several administrations, including programming, gathering, and coordinating equipment assets, are included in Cloud Computing (CC) and made available to service users online. The advantages of Cloud Computing are flexibility, competence, and high unwavering quality. Numerous organizations are already exchanging data to the Cloud, and as a result, this data needs to be protected against unauthorized assaults, service rejection, and other threats. Information is deemed secure if classification, accessibility, and uprightness are all available. The challenges and problems related to Cloud Computing security are illustrated in this paper. Additionally, research on security protocols for Cloud-based settings is carried out.***
Keywords: Cloud Computing, Cloud Security, Confidentiality, Integrity.

I. INTRODUCTION

Cloud is simply a set of servers and data centers in a variety of regions, on-demand services are provided to the user with these data centers and servers via the internet. On the user's computer, the Cloud service is not assembled[1]. The user can and should register for these services to receive access to them. The main advantage of Cloud Computing is that it does not make it compulsory for the user to be physically available in the same place as other hardware devices. As shown in figure 1, the Cloud allows access and storage the data from any place, at any minute without any thought of storage space, hardware, or software. Each of the above services is provided at a low cost to subscribers[2]. The Clouds are broadly classified as Private, Public, and Hybrid Clouds.

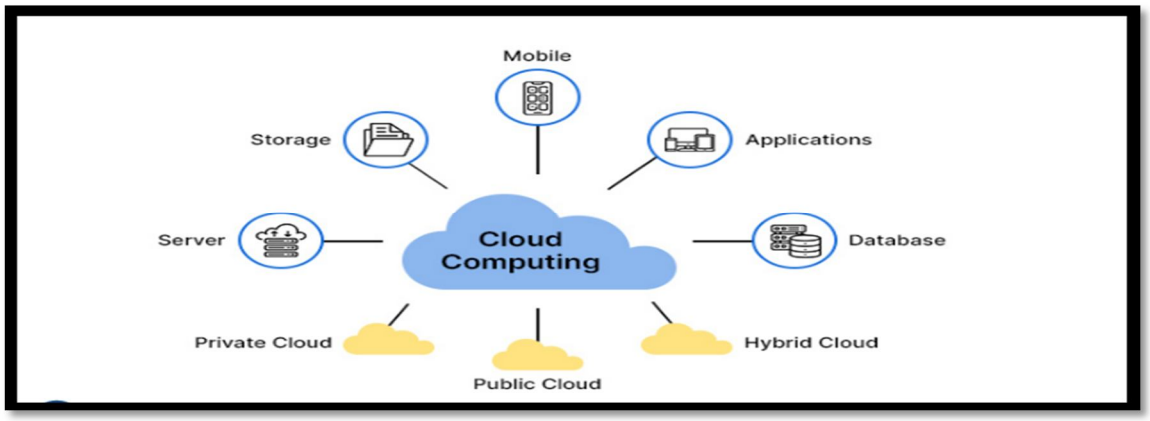


Figure. 1. Types of Cloud& Services Provided [3]

A. *Benefits of Cloud Computing*

CC offers a number of benefits, some of which are[3][4][5]:

1) *Cost Savings:* When launching new projects, having quick access to the company's data after it has been stored in the Cloud will save time and money.
2) *Flexibility:* In comparison to using the Cloud, hosting on a local server gives organizations less flexibility. Moreover, a cloud-based solution could quickly accommodate more bandwidth demand instead of requiring a costly (and challenging) upgrade to your IT infrastructure. This extra freedom and flexibility may significantly boost the organization's overall efficiency.
3) *Mobility:* Cloud Computing enables mobile access to corporate data through smartphones and other devices. Businesses can offer information via the Cloud that is conveniently accessible to mobile sales staff, independent contractors, or remote workers for a better work-life balance.

4) *Collaboration:* Cloud Computing facilitates effortless collaboration. Coworkers can view and share information quickly and securely on a cloud-based platform.
5) *Disaster Recovery:* One of the factors that affect a company's success is control. However, there will always be operational problems that are beyond your organization's control, and in the current market, even a little bit of unnecessary downtime can have a negative impact. Downtime results in lost productivity, revenue, and brand reputation for the service. CC greatly helps in recovering from such situations.
6) *Centralized Data Security:* When organizations employ cloud computing, data backups are kept centrally in the cloud providers' data centers, negating the need for individual users or teams to maintain their backups locally or remotely. This lessens the possibility of data loss if one backup fails or is damaged due to a disaster. The data can be recovered from a backup copy stored in the cloud storage of the cloud service provider, which is updated when new data is added.

B. Limitations of Cloud Computing.

Some of the limitations of Clouds are[6]:

1) *Internet Connectivity:* All data, including pictures, audio, and video, are saved in the cloud in cloud computing and accessed online. If the internet connection is unreliable, it cannot be accessed. There isn't any other way to access cloud-based data.
2) *Limited Control:* Control is one of the factors that influence a company's success. However, there will always be operational challenges that are out of your organization's control, and in the current market, even a small amount of unnecessary downtime can have a negative effect. Downtime results in lost productivity, revenue, and brand reputation for the service. CC greatly helps in recovering from such situations.
3) *Cloud Security and Data:* The majority of Cloud service providers apply necessary security standards and trade certifications to maintain the security of the Cloud environment. However, storing crucial data and files in a virtual data center may put the organization in danger.

Typical dangers include:

- Data leakage, account or service hijacking, and data loss or theft
- Unsafe Interfaces and APIs
- Attacks that disrupt services
- Technological flaws, particularly in communal settings

II. LITERATURE REVIEW

1) Singh et al. have proposed an algorithm; a hybrid of RSA and SHA1 which aids the creation of new security solutions for different types of threats. The major point in the proposed work is data security, and the authors strived to achieve this scoring opportunity with the hybrid algorithm[1].
2) Bahnaswami et al. evaluate and develop the Application Specific Integrated Circuit (ASIC) of some of the most common security algorithms in IoT applications. They use the ASIC approach in the implementations, which are analyzed using the UMC 130nm CMOS technology. This comparative review examines various aspects that are primary constraints of IoT applications, such as power consumption, probability, throughput, area, and attack immunity. The algorithms used in this work are AES, 3DES, Twofish, and RSA[15].
3) Cordova et al. assess and contrast the performance of the RSA, Blowfish, and AES (Rijndael) algorithms. According to findings, the Blowfish has a higher time efficiency ratio under different data loads and memory size as compared to AES and RSA[16].
4) Bhandari et al. explored different aspects of cryptography during communication and its use in Cloud Computing to increase the security of encrypted text or data on Cloud servers while greatly minimizing the resources, memory, and time required for encryption and decryption.[17]
5) Islam and Riyas discussed the various benefits and major security challenges of Cloud Computing, in addition to discussing the various cryptographic encryption algorithms as major solutions to security challenges. Besides this, in this paper, the efficiency of each algorithm in Cloud Computing has been compared. The authors concluded that the homomorphic algorithm is the best solution for securing sensitive data in a Cloud computing environment. Homomorphic algorithms offer higher security than other algorithms like RSA, DES, and AES since they can operate on encrypted data[18].

6) Abdullah has provided a summary of the AES algorithm, detailed several of its essential components in depth, and provided examples of prior research on it in comparison to competing algorithms like DES, 3DES, Blowfish, and others. According to research findings, AES has a considerably greater capacity for security than other algorithms like DES, 3DES, and so forth[19].
7) Khan and Tuteja have reviewed various Cloud security issues and cryptographic algorithms that could be employed to strengthen Cloud security. Using cryptographic techniques to improve Cloud security from various Cloud users' perspectives, this research study proposes a work strategy to allay data privacy worries. The researchers presented a mechanism that uses multilevel encryption and decryption to enhance the security of Cloud Storage[20].
8) Mushtak et al. analyzed the security aspects and procedures of various popular symmetric encryption algorithms, such as Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Blowfish, Advanced Encryption Standard (AES), and Hybrid Cubes Encryption Algorithm (HiSea). The performance of these algorithms was evaluated and compared using criteria such as throughput, key size, avalanche impact, memory, correlation assessment, and entropy. The researchers aimed to identify a suitable encryption method that would best meet the requirements of customers. Based on the findings, it was concluded that an effective approach to enhancing overall encryption security would involve the development of a hybrid encryption algorithm that combines multiple encryption methods, considering all relevant criteria.[21].
9) Vennela et al. analyzed that the Blowfish algorithm performed better than other algorithms when encrypting text files and movies, whereas AES performed better than other algorithms when encrypting images. Based on this analysis, authors have created an effective interface for using the right methods to encrypt various file formats. Authorized users have access to this interface, which allows them to upload and download files from the Cloud. Finally, these findings demonstrate that the performance of the algorithms changes depending on the type of file being encrypted, with Blowfish and AES performing best for text and video files, respectively[22].
10) Bhardwaj et al. studied symmetric and asymmetric algorithms with a focus on symmetric ones to determine which one, from a security standpoint, should be used for Cloud-based applications and services that demand data and link encryption. As the authors looked at symmetric algorithms for various key encryption and encoding techniques, they discovered that AES was a good contender and that MD5 was quicker when encoding[23]
11) Semwal and Sharma in this study compared numerous cryptographic encryption algorithms in terms of their key characteristics, and their performance costs are then discussed concerning a few critical criteria. The algorithms used include DES, 3DES, IDEA, CAST128, AES, Blowfish, RSA, ABE, and ECC[24].
12) Abdulsalam and Hedabou reviewed multiple publications in the literature to assess the effectiveness of suggested models in addressing Cloud security issues and their ability to prevent future breaches. The study utilized the STRIDE technique to examine the security risks of Cloud computing from the user's perspective. In addition, the research analyzed ineffective methods found in the literature and provided recommendations for establishing a secure and adaptable Cloud environment.[25].
13) Farsi et al. conducted a comprehensive and critical assessment of the existing literature concerning security threats, Cloud computing models, and security techniques. The researchers aimed to identify the limitations of current research in the field of Cloud computing. The study specifically evaluated various data security methods, including encryption and other approaches used to enhance security in the Cloud.[26].
14) Zuliffqar et al. discussed some applications for Cloud computing. This study demonstrates that integrating this technology into a company after addressing data security concerns can result in significant adjustments[27]. Here, the authors have covered some crucial Cloud data security challenges, computers, problem-solving methods, and advantages and disadvantages of Cloud computing. This study demonstrates that CC offers the ability to employ resources from a resource pool, which aids in the reduction of E-Waste. Future research will need to assess several Cloud-related issues, including security, privacy, effectiveness, property, economics, and other non-technical concerns. As a result, research teams encounter several challenges and must research both technology and non-technical problem answers. The security issues have to be thoroughly investigated.
15) Albugmi et al. outlined three main security concerns and emphasized the hazards and threats to cloud-based data security[28]. Virtualization is studied to assess the risks posed by the hypervisor. Similar issues caused by public clouds and multitenancy have been considered. Data security, particularly its threats and potential solutions in cloud computing, was one of this essay's key concerns. We've investigated the methods that work for encrypting data on the Cloud, along with data in various states. A brief explanation of the block cipher, stream cipher, and hash function used to encrypt Cloud data, whether it is at rest or in transit, was provided in the paper.

16) Wang et al provide a summary of large-data Cloud computing conceptions, traits, and sophisticated technologies[29]. Data security concerns related to data quality and privacy controls are detailed. In the end, virtualization architecture and related tactics are suggested to counter attacks and improve data security in big data Cloud computing.

17) Pansotra and Singh have concluded that there are numerous data security algorithms, including DES, AES, and Triple DES[30]. As opposed to RSA, Diffie-Hellman Key Exchange, and homomorphic equations, which employ two different keys for encryption and decryption, these symmetric key methods use a single key for both encryption and decryption. These algorithms need to improve their security because they are currently insecure.

18) Alemami et al. utilized a recent assessment of Cloud security risks, difficulties adopting Cloud services, and encryption techniques in Cloud environments[31]. The study presented a summary of the methodologies and frameworks employed in several previous investigations. The objective was to determine the most suitable security algorithm for safeguarding Cloud data through a literature review on Cloud data security. The research compared encryption algorithms such as RSA, AES, DES, Blowfish, and IDEA. The results indicate that IDEA, AES, Blowfish, and DES are symmetric algorithms, whereas RSA is an asymmetric algorithm. AES, Blowfish, and DES were found to offer greater security compared to RSA and IDEA, with Blowfish utilizing the least amount of memory. The AES method was identified as capable of encrypting large volumes of data.

19) Tyagi et al. concluded that while the RSA algorithm has some features, it is not a reliable system for protecting banking information stored in the Cloud[32]. Similar to how twofish cannot be the best option for encryption because it is slower than AES and there may be flaws with S-boxes as well. Since passwords are the primary key component in the banking business, it will endeavor to discover another reliable method to safeguard Cloud data in the future. As a result, steps will be taken to generate the most secure key utilizing password-based key derivation function, cryptographic algorithms

20) Maddineni and Ragi et al. concluded that it can be very difficult to identify security risks and mitigation strategies across a wide range of Cloud computing services[33]. As part of the identifying process from research techniques with the help of (SLR and Survey), the authors were able to identify a sufficient number of obstacles and potential solutions that can be applied both now and in the future.

21) Hasan et al. have organized all the data privacy techniques for cloud computing data storage and presented them all in one place[34]. The researchers also compare all the protection methods based on five criteria: (i) local proxy overhead, (ii) data accuracy retention, (iii) level of data protection, (iv) transparency, and (v) operation support.

Table 1. Summary of Literature Review

S. N	Author	Technique used	Focus On
1.	Singh et al.[1]	RSA, SHA1	Data security with a hybrid algorithm
2.	Bahanaswami et al.[15]	ASIC	Comparative review of hardware security algorithms
3.	Cordova et al.[16]	RSA, AES, Blowfish	Comparative analysis of the performance of selected security algorithms
4.	Bhandari et al.[17]	Use of cryptography concepts	Improve the anonymity of encrypted and encrypted data
5	Islam and Riyas[18]	Various cryptographic encryption algorithms	Benefits and security challenges of Cloud Computing
6	Abdullah[19]	AES	Compete for algorithms like –DES, 3DES, Blowfish
7	Khan and Tuteja[20]	Security issues	Strengthen Cloud Security
8	Mushtak et al.[21]	DES, AES, HiSea	Use of appropriate encryption algorithm
9	Kaur and Kinger[22]	DES , 3DES , AES , RSA , IDES	Covered various symmetric and asymmetric algorithms
10	Bhardwaj et al. [23]	Symmetric and Asymmetric algorithm	Focus on symmetric algorithm
11	Semwal and Sharma[24]	Revolution of IT by Cloud Computing	Implementation of security for Cloud Computing
12	Abdul Salam and Hedabou [25]	STRIDE	Highlighted the security risks associated with the user
13	Farsi et al.[26]	Encryption	Security threats and limitations of present cloud computing
14	Zuliffqar et al. [27]	Applications for CC	Discussed applications for cloud computing
15.	Wang et al. [29]	Sophisticated technologies	Focus on data quality and privacy control
16	Pansotra and Singh [30]	Opposed RSA	Focused on the improvement of an algorithm
17	Alemami et al. [31]	Encryption	Summary of methodologies
18	Tyagi et al.[32]	Analysis of encryption algorithms	More reliable keys will be searched
19	Maddineni and Ragi [33]	RSL and Survey	Identification of various obstacles

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VII July 2024- Available at www.ijraset.com

III. SECURITY

The practices, tools, and personnel used to protect a company's digital assets are referred to as information technology (IT) security [7]. Unauthorized users, sometimes referred to as threat actors, are prevented from stealing, utilizing, or disrupting these assets, devices, and services by IT security. These risks could be internal or external, and they could have a purposeful or inadvertent origin and character. The crucial components of security include:

1) *Confidentiality:* The secrecy of data and information is demonstrated by limiting access to them to those who are authorized. The following are some of the most popular security precautions for maintaining confidentiality: Employees are granted authorizations and access rights under the nature of their jobs. Data and information are classified according to their value (measured as the influence that information exposure has on the organization), on multiple levels, ranging from public to top secret. Information can be protected so that no one can reach it unnecessarily and leak it by using the technique of encryption [5].
2) *Integrity:* Data and information integrity refer to the need to maintain their accuracy and completeness and to prevent any unauthorized changes, whether unintentional or purposeful. Backups, access control, employee training, etc. as measures for maintaining the data and information integrity. Hash functions of Cryptography are very important for ensuring that consumers can trust their data to be accurate.
3) *Availability:* Information should be available to the intended audience. It ensures that users with permission can access the system and data whenever it's essential.

IV. CLOUD SECURITY

Cloud security is a method of cyber security provided for securing Cloud Computing systems[8]. It involves keeping data safe and providing it security on online platforms. Cloud security which is also termed Cloud Computing security is a combination of security measures that are framed to protect infrastructure, data, and applications based on the Cloud. These standards guarantee user and device assertion, access control of resources and data, and also protection of privacy[9]. Some of the top security benefits of Cloud Computing:

1) *Lower Upfront Costs:* One of the greatest advantages of using Cloud Computing is that there is no need to pay for hardware. It helps to save a sufficient amount of money in the starting stage and is also helpful in upgrading security. Once Content Security Police (CSPs) are hired security handling becomes easy. This in turn reduces costs and also the risks of hiring an internal security team to safeguard the hardware.
2) *Reduced Ongoing Operational and Administrative Expenses:* With Cloud security, administrative and operational expenses can also be reduced. This will be done by CSP as it will handle all the security needs and there is no need to hire a staff that will provide manual security updates. Organizations can also enjoy greater security, as the expert staff of CSP will handle all kinds of security issues.
3) *Increased Reliability and Availability:* Immediate access to data is always needed. Because pre-made data and apps are accessible to authorized users, cloud security also ensures this. To enable prompt response to any potential security issues, a dependable approach to accessing Cloud apps and information is constantly available.

V. CLOUD CRYPTOGRAPHY

A collection of methods known as Cloud cryptography is used to protect data that is handled and stored in Cloud Computing environments. By utilizing encryption and secure key management methods, it offers data privacy, integrity, and secrecy**.**

To safeguard that only the person for whom it is intended should read it and exchange data in contact, cryptography can be considered as a means of obscuring and storing classified info in a cryptic form. Using cryptography, authentication, and cautiously allocating keys, security algorithms and competitors strive to minimize cyber threats. Therefore, encoding is the science of protecting data and messages by transforming the user data that will be transmitted into a private, encrypted form and encrypting or scrambling the plaintext using the user data. The figure illustrates the cryptography process steps. 2.

Figure. 2. Steps of Cryptography

A. Cryptography Algorithms

A mathematical procedure for transmitting data is described as an encryption algorithm. Information is encoded into cipher text using an algorithm and a key, and to change the data back into its original form, a "key" is needed.

For technology to enable effective and secure identification, as well as integrity and encryption, algorithms are a fundamental requirement. Cryptographic protocols and algorithms are used for fraud protection, restricting unauthorized access to public and private telecommunications networks, and safeguarding user data.

1) Algorithms for Public-Key Security[10][4][11]

a) Rivest Shamir Adleman (RSA): RSA is a cryptographic algorithm that involves the use of both a private key and a public key. Messages are encrypted using the publicly available key, while decryption of the encrypted messages can only be done using the corresponding private key. Figure 3 shows the Psesodocode of this algorithm.

1: **Input Values:** p and q
2: **Compute:**
3: n = p x q
4: (n) = (p-1) (q-1)
5: **Select Integer values:** e [(gcd (), e) - 1; 1 < e < ϕ (n)]
6: **Compute:** d de *mod* ϕ (n) = 1
7: C = Cg 1 *mod* (z)
8: **Encryption:** M < n C = M (*mod* n)
9: **Decryption:** CM = C(*mod* n)

Fig. 3. RSA[12]

b) Message-Digest algorithm (MD5): The encryption algorithm in dispute is very effective. It encodes a variable-length message into an output that is fixed-length and 128 bits lengthy by using a hash function with a 128-bit hash value. Blocks of 512 bits are used to fragment the input message. The message is then padded to make it divisible by in a bid to make the message's length divisible by 512, padding is then appended. To encrypt the message in this circumstance, the sender uses the key to encrypt a message. The message is encrypted, and the responder decrypts it using its private key. The steps of the MD5 algorithm are shown in figure 4.

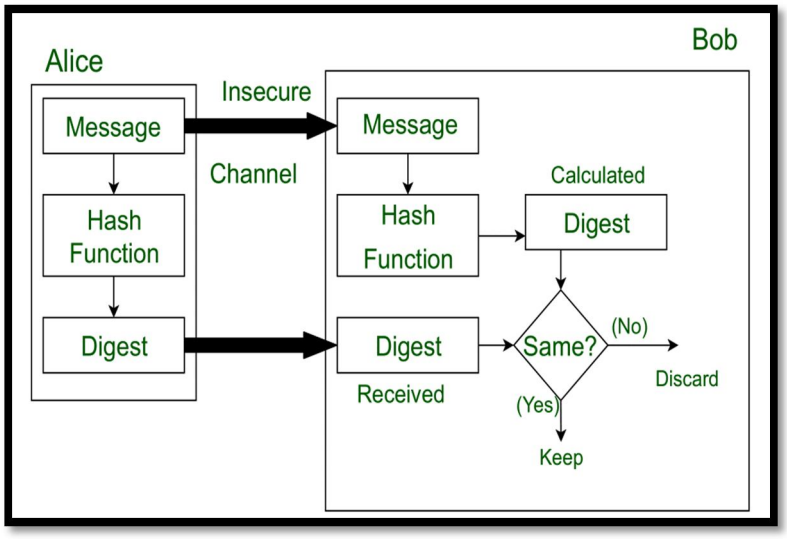


Fig. 4. MD5[13]

c) *Digital Signature Algorithm (DSA):* Digital Signature Algorithm is a cryptographic algorithm that is used to create digital signatures, stop message tampering and confirm who sent a digital communication. Two keys are needed for DSA to operate: a sender's private key and a receiver's public key. The steps of the DSA algorithm are shown in figure 5.

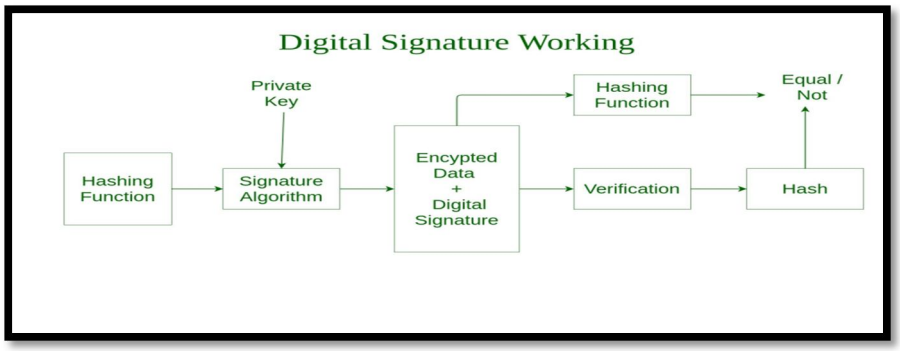


Fig. 5. DSA[13]

d) *Elliptic Curve Digital Signature Algorithm (ECDSA):* One of the more difficult public key cryptography encryption systems is called the Elliptic Curve Digital Signature Algorithm, or ECDSA. Elliptic curve cryptography produces keys that are generally smaller than those produced by digital signing techniques. Public key cryptography based on elliptic curves over finite fields' algebraic structure is known as elliptic curve cryptography. To generate digital signatures and pseudo-random numbers, among other things elliptic curve cryptography is used mostly. In a digital signature, a digital certificate and a public key pair are used as a signature, which is a genuine technique, to confirm the identity of the receiver or sender.

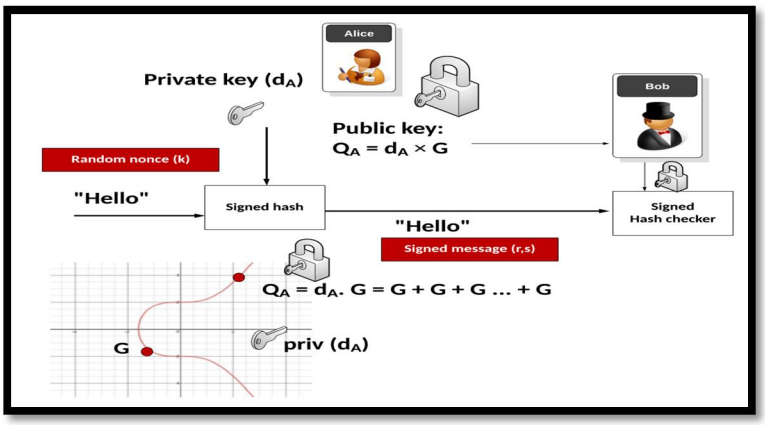


Fig. 6. ECDSA[13]

e) *Error-correcting code (ECC):* Error-correcting code memory is a kind of computer data storage. ECC memory employs an error correction code (ECC) to identify and fix n-bit data corruption that develops in memory. Most computers employ ECC memory in applications that cannot tolerate data corruption, such as industrial control software, crucial databases, and infrastructure memory caches.

2) *Attacks [14]*

Just like any other computing environment, Clouds are also prone to several attacks. Some of these attacks are:

a) *Attack employing Distributed Denial of Service (DDoS):* Competitors can interrupt services by targeting known vulnerabilities, which involves adopting various methods of information systems and deluging a single node with messages, by using a distributed denial of service attack to reduce server resources. The DDoS attack tools might be either elaborate or uncomplicated. Agobot, Mstream, Trinoo, Extensible Markup Language (XML) based Denial of Service (X-DoS), and Hypertext Transfer Protocol (HTTP) based Denial of Service (H-DoS) are examples with both complex and simple tools, respectively.

b) Side-channel Assaults: Through the start-up of a malicious virtual machine nearby the Cloud an attacker tries to compromise it. Deploying a side-channel attack even when within striking distance of a target Cloud server

c) Attacks on Authentication: The use of hosted and virtual services authentication is a shortcoming that is disproportionately impacted. It is possible to authenticate users in a variety of ways. If, for particular, the measures used to guarantee the authentication process are depending on what they are aware of, embody, or are and the strategies adopted are frequently the focus of attackers, then the circumstances are not optimum.

d) Cryptographic Man-in-the-Middle Attacks: When the attacker stands in the middle of two users, the attack is conducted. Attackers can interrupt or impede the flow of communication at any time.

VI. CONCLUSION

The Cloud Computing model of viewership is helping push the IT industry into a long-awaited era. Nowadays, it is a utility, such as water, LPG, electricity, and wireless communications. The vital result of on-demand services is an attainable effect for many SMEs, which pretty much exclusively reduces overall infrastructure costs. Cloud Computing is still evolving, primarily in terms of security. Because history has repeatedly demonstrated that security should be prioritized.

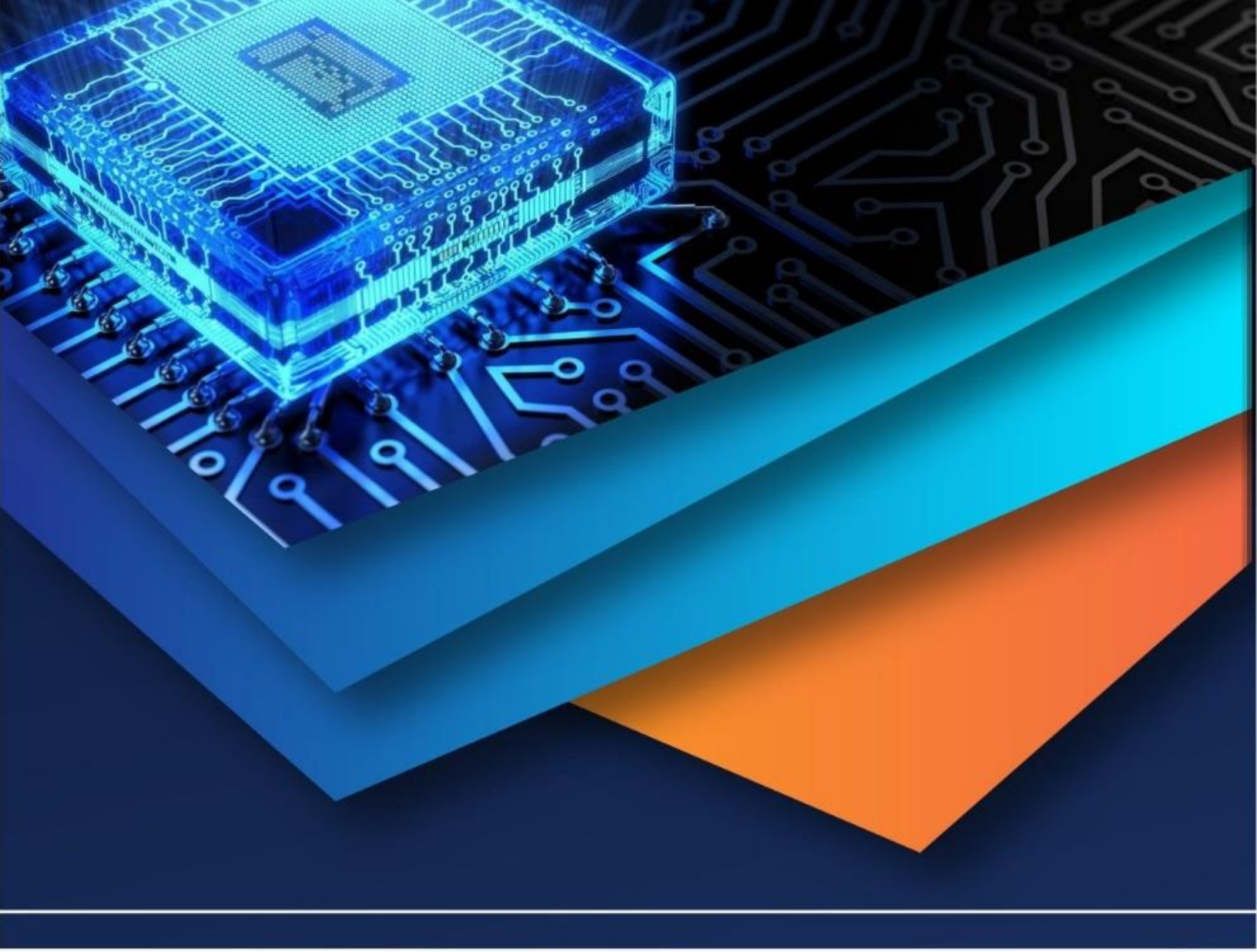
This paper indicates how Cloud security issues should be addressed by analyzing the literature. This review reveals a significant desire and momentum for the development of a safe Cloud and informational intentions for educational and commercial environments. As this field matures, solid supporting means to meet the rigid requirements of Cloud environments should be provided.

Data encryption mechanisms are the most popular to maintain the CIA. In the future, a hybrid model will be proposed to enhance the security of Clouds.

REFERENCES

[1] S. Singh and T. Nafis, “Cloud Computing: Security Issues,” Int. J. Comput. Intell. Res., vol. 13, pp. 1419–1429, 2017, doi: 10.7763/ijcce.2014.v3.332.
[2] C. V. Raghavendran, G. N. Satish, P. S. Varma, and G. J. Moses, “A Study on Cloud Computing Services,” Int. J. Eng. Res. Technol., vol. 4, no. 34, pp. 1–7, 2017.
[3] A. A. Abdulateef, A. H. Mohammed, and I. A. Abdulateef, “Cloud Computing Security for Algorithms,” 4th Int. Symp. Multidiscip. Stud. Innov. Technol. ISMSIT 2020 - Proc., 2020, doi: 10.1109/ISMSIT50672.2020.9254372.
[4] Salesforce, “12 Benefits of Cloud Computing and Its Advantages - Salesforce.com,” Benefits Of Cloud Computing. 2022. [Online]. Available: https://www.salesforce.com/products/platform/best-practices/benefits-of-cloud-computing/
[5] F. Okeke, “Disadvantages of cloud computing,” Https://Www.Techrepublic.Com/Article/Disadvantages-Cloud-Computing/. 2022.
[6] J. Van Der Ham, “Toward a Better Understanding of ‘Cybersecurity,’” Digital Threats: Research and Practice, vol. 2, no. 3. 2021. doi: 10.1145/3442445.
[7] A. Jain and R. Kumar, “Confidentiality Enhanced Security Model for Cloud Environment,” Proc. Second Int. Conf. Inf. Commun. Technol. Compet. Strateg. - ICTCS ’16, pp. 1–6, 2016, doi: 10.1145/2905055.2905199.
[8] S. Zhang, H. Yan, and X. Chen, “Research on Key Technologies of Cloud Computing,” Phys. Procedia, vol. 33, pp. 1791–1797, 2012, doi: 10.1016/j.phpro.2012.05.286.
[9] A. Hamza and B. Kumar, “A Review Paper on DES, AES, RSA Encryption Standards,” Proc. 2020 9th Int. Conf. Syst. Model. Adv. Res. Trends, SMART 2020, pp. 333–338, 2020, doi: 10.1109/SMART50582.2020.9336800.
[10] S. Kumar, B. K. Singh, Akshita, S. Pundir, S. Batra, and R. Joshi, “A survey on symmetric and asymmetric key based image encryption,” 2nd Int. Conf. Data, Eng. Appl. IDEA 2020, 2020, doi: 10.1109/IDEA49133.2020.9170703.
[11] R. Abid et al., “An optimised homomorphic CRT-RSA algorithm for secure and efficient communication,” Personal and Ubiquitous Computing. 2021. doi: 10.1007/s00779-021-01607-3.
[12] “How does Digital Signature Algorithm (DSA) work_ - The Security Buddy.”
[13] M. A. Bahnasawi et al., “ASIC-oriented comparative review of hardware security algorithms for internet of things applications,” Proc. Int. Conf. Microelectron. ICM, vol. 0, pp. 285–288, 2016, doi: 10.1109/ICM.2016.7847871.
[14] R. S. Cordova, R. L. R. Maata, A. S. Halibas, and R. Al-Azawi, “Comparative analysis on the performance of selected security algorithms in cloud computing,” 2017 Int. Conf. Electr. Comput. Technol. Appl. ICECTA 2017, vol. 2018–Janua, pp. 1–4, 2017, doi: 10.1109/ICECTA.2017.8252030.
[15] A. Bhandari, A. Gupta, and D. Das, “Secure algorithm for cloud computing and its applications,” Proc. 2016 6th Int. Conf. - Cloud Syst. Big Data Eng. Conflu. 2016, pp. 188–192, 2016, doi: 10.1109/CONFLUENCE.2016.7508111.
[16] N. K. V Islam and M. K. V Riyas, “International Journal of Computer Science and Mobile Computing Analysis of Various Encryption Algorithms in Cloud Computing,” Int. J. Comput. Sci. Mob. Comput., vol. 6, no. 7, pp. 90–97, 2017, [Online]. Available: www.ijcsmc.com
[17] A. Muhammad Abdullah, “Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data View project Call for papers View project Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt,” no. June, 2017, [Online]. Available: https://www.researchgate.net/publication/317615794
[18] S. S. Khan and P. . .R. Tuteja, “Security in Cloud Computing using Cryptographic Algorithms,” Int. J. Innov. Res. Comput. Commun. Eng., vol. 3, no. 1, pp. 148–154, 2015, doi: 10.15680/ijircce.2015.0301035.
[19] M. F. Mushtaq, S. Jamel, A. H. Disina, Z. A. Pindar, N. S. A. Shakir, and M. M. Deris, “A Comprehensive Survey on the Cryptographic Encryption Algorithms,” Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 11, pp. 333–344, 2017.

[20] G. S. Vennela, N. V. Varun, N. Neelima, L. S. Priya, and J. Yeswanth, "Performance Analysis of Cryptographic Algorithms for Cloud Security," Proc. Int. Conf. Inven. Commun. Comput. Technol. ICICCT 2018, no. Icicct, pp. 273–279, 2018, doi: 10.1109/ICICCT.2018.8473148.
[21] A. Bhardwaj, G. V. B. Subrahmanyam, V. Avasthi, and H. Sastry, "Security Algorithms for Cloud Computing," Procedia Comput. Sci., vol. 85, no. Cms, pp. 535–542, 2016, doi: 10.1016/j.procs.2016.05.215.
[22] P. Semwal and M. K. Sharma, "Comparative study of different cryptographic algorithms for data security in cloud computing," Proc. - 2017 3rd Int. Conf. Adv. Comput. Commun. Autom. (Fall), ICACCA 2017, vol. 2018–Janua, pp. 1–7, 2018, doi: 10.1109/ICACCAF.2017.8344738.
[23] Y. S. Abdulsalam and M. Hedabou, "Security and privacy in cloud computing: Technical review," Futur. Internet, vol. 14, no. 1, 2022, doi: 10.3390/fi14010011.
[24] M. Farsi, M. Ali, R. A. Shah, A. A. Wagan, and R. Kharabsheh, "Cloud computing and data security threats taxonomy: A review," J. Intell. Fuzzy Syst., vol. 38, no. 3, pp. 2529–2537, 2020, doi: 10.3233/JIFS-179539.
[25] I. Zulifqar, S. Anayat, and I. Kharal, "A Review of Data Security Challenges and their Solutions in Cloud Computing," Int. J. Inf. Eng. Electron. Bus., vol. 13, no. 3, pp. 30–38, 2021, doi: 10.5815/ijieeb.2021.03.04.
[26] A. Albugmi, M. O. Alassafi, R. Walters, and G. Wills, "Data security in cloud computing," 5th Int. Conf. Futur. Gener. Commun. Technol. FGCT 2016, no. August, pp. 55–59, 2016, doi: 10.1109/FGCT.2016.7605062.
[27] F. Wang, H. Wang, and L. Xue, "Research on Data Security in Big Data Cloud Computing Environment," IEEE Adv. Inf. Technol. Electron. Autom. Control Conf., vol. 2021, pp. 1446–1450, 2021, doi: 10.1109/IAEAC50856.2021.9391025.
[28] A. Pansotra and S. P. Singh, "Cloud security algorithms," Int. J. Secur. its Appl., vol. 9, no. 10, pp. 353–360, 2015, doi: 10.14257/ijsia.2015.9.10.32.
[29] Y. Alemami, A. M. Al-Ghonmein, K. G. Al-Moghrabi, and M. A. Mohamed, "Cloud data security and various cryptographic algorithms," Int. J. Electr. Comput. Eng., vol. 13, no. 2, pp. 1867–1879, 2023, doi: 10.11591/ijece.v13i2.pp1867-1879.
[30] K. Tyagi, S. K. Yadav, and M. Singh, "Cloud data security and various security algorithms," J. Phys. Conf. Ser., vol. 1998, no. 1, 2021, doi: 10.1088/1742-6596/1998/1/012023.
[31] V. S. K. MAddineni and S. Ragi, "Security Techniques for Protecting Data in Cloud," 2011. doi: 10.35940/ijitee.a5043.129219.
[32] J. Hassan et al., "The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges - A Systematic Literature Review (SLR)," Comput. Intell. Neurosci., vol. 2022, no. 5, 2022, doi: 10.1155/2022/8303504.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY