RESEARCH ARTICLE OPEN ACCESS

Application of advance encryption algorithm for enhanced Cloud security

Yashraj Mishra, Sanjay Pal

Department of Computer Science & Engineering, Oriental Institute of Science and Technology Bhopal
Department of Computer Science & Engineering, Oriental Institute of Science and Technology Bhopal

ABSTRACT

Tremendous change has been brought into IT infrastructures by cloud computing, particularly in making resource utilization scalable, dynamic, and cost-efficient. Increasingly, organizations are buying into cloud solutions to be able to avail flexible computing power and storage capacity. Yet, moving to the cloud involves some serious security issues, especially those concerning confidentiality, access control, and integrity of data. It is, therefore, very critical for maintaining trust and securing sensitive information to provide secure data transmission and storage in cloud environments. The greatest threat is the invasion of unauthorized access or cyber threats so that data confidentiality and integrity can be compromised. The policies are very complex concerning access control management within multi-tenanted cloud platforms. To manage the risks, robust implementations of encryption techniques are necessary. Advanced Encryption Standard, Elliptic Curve Cryptography, and Rivest-Shamir-Adleman algorithms are considered as the most effective algorithms in securing data either at rest or in transit. The encrypted ciphertext does not allow prying eyes to decrypt it. An overview of security challenges that cloud computing can introduce has been covered in this paper and the evaluation of how effective the various encryption algorithms are in solving these problems. In comparative perspectives, it brings how encryption improves data security, generates the possibility of compliance with regulations, and secures cloud services from modern cyber threats, thus reinforcing today's information technology infrastructures.

Keywords: Cloud computing, advanced encryption, AES, ECC, RSA, cloud security.

I. Introduction

Cloud computing has altered software deployment and management significantly, shifting the paradigm away from the traditional IT infrastructure toward a more flexible, scalable, and economical model. Cloud computing has totally transformed the way businesses deploy, maintain, and scale their software applications by providing on-demand access to computing resources over the internet. Examining how cloud computing influences software deployment and management will enable the reader to understand what these changes are doing to the contemporary IT processes. Businesses can scale resources according to demand, develop applications more quickly, and maximize operational efficiency thanks to the cloud's capacity to provide resources as services, including networking, storage, and processing power [1]. Many IoT-related fields, such as Genomics Data Processing, Education and Learning, Small and Medium Business Services, E-Learning Method, Augmented Reality, Manufacturing, Emergency Recovery, Smart Cities, and others, Remote Forensics, Hospitality Business, E-Government and Human Resource Administration, and Internet of Cars, use cloud computing services [2].

It is common practice to store data from different project phases in silos, such as team servers or desktops, individual computers, laptops, and smartphones. Consequently, the absence of access to a full perspective of data often leads to poor decisions that could impact the profitability and project's performance as well as cause delays, making data integration essential for overall project coordination. The traditional (information and communication technology) ICT solution is a sophisticated system for holding, processing, and evaluating data from its subcontractors. Deploying a solution on-site involves a large running expense burden as well as significant overhead (cooling, electricity, security, availability, and upgrades). The high initial cost of on-site ICT equipment makes it impossible to commission it for every project. Furthermore, internal computer capacity is set, and it is usually more expensive to upgrade it to meet unforeseen increases in processing demands. The pay-as-you-go pricing model of cloud computing technologies provides affordable and scalable computer resources. Features of cloud computing are therefore suitable for SMEs. The expense of buying, setting up, and maintaining computer infrastructure has greatly limited the use of ICT in the construction sector; cloud computing lowers these costs [3]. Both consumer and business users can benefit from cloud computing. By investing in a cloud server, consumers can reduce computing expenses by avoiding the need to purchase numerous machines. To optimize the efficiency of computer resource consumption, cloud service providers can dynamically schedule computing resources based on users' access requirements. In cloud computing, resource allocation must be done rationally. In cloud computing resource allocation, customers arrive sequentially, and the cloud computing center has restricted cloud resources. The cloud computing center receives requests from each user to use a certain amount of cloud resources at a specific time [4].

Cloud computing's innate versatility stands as one of its more enticing features. Companies are enabled to dynamically redefine computing resources in line with varying demands, allowing for the unbroken expansion or scalability of applications depending on the needs of the business. Greater flexibility and agility in work are given when applications can be deployed and managed from anywhere. Also, cloud platforms facilitate fusing innovation in fields such as artificial intelligence, machine learning (ML), and big data analytics with conventional business processes and marketing campaigns. Figure 1 outlines the essentials of cloud computing. It demonstrates the range of services offered by cloud computing and how it links providers and customers. The worldwide accessibility of cloud computing is another essential advantage. Cloud services make it possible to collaborate in real time across multiple geographies and provide services to a worldwide clientele with minimal downtime by removing geographical constraints. This global reach improves operational efficiency and creates untapped advertising opportunities, putting businesses in a more competitive position on a global scale [5].

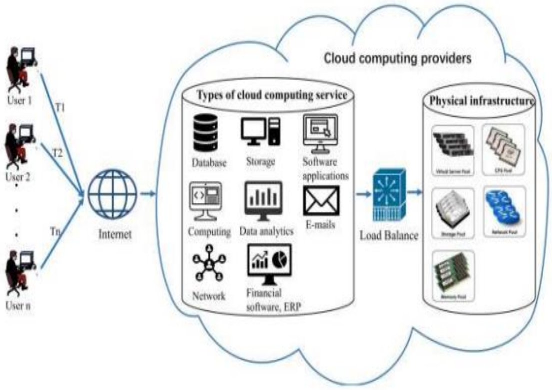

Figure 1 Overview of Cloud Computing [5]

II. Cloud Computing Services

There are three categories of cloud computing services that are determined according to the mode of deployment. A cloud computing service is the service likely to be available in terms of resources under that cloud computing service. Such are examples of cloud computing services, namely, software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

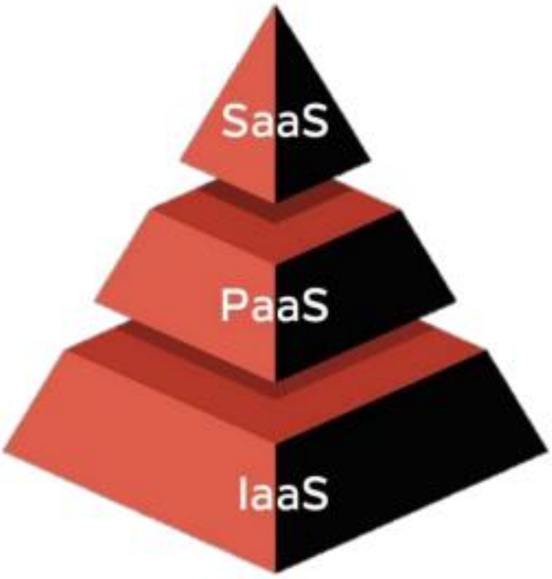

Figure 2 Cloud Models [6].

A. **Software as a service (SaaS)**: Customers will employ cloud-based applications from a supplier with this service. Actually, users will only be able to make little adjustments to applications, such where corporate logos are placed, language settings, and look-and-feel options. All of the layers are outsourced in this instance. These programs would be available to everyone, at any time, from any location, via a straightforward interface like a web browser. The commercial value of the application can be advantageous to users. Software as a Service (SaaS) gives third-party services authority over software deployment and administration. It is conceivable that an application in its totality can be rearranged, possibly that was absolutely imagined, on the basis of an invariable set of configuration settings.

B. **Platform as a service (PaaS)**: This cloud service would allow customers to develop and use their applications with the programming languages and the tools supported by the cloud. The application is managed along with certain platform environment configurations on the customer side; over the integrated infrastructure, however, there is no control or management. One of the examples of PaaS is web hosting; those companies which provide web-hosting also provide an environment with a programming language such as PHP. Under this kind of manifestation, the platform does not belong to the customer. The network, servers, storage, and other services required for hosting the consumer's application are completely dependent on the service provider. PaaS options allow the customer to deploy the application on the cloud without incurring the expense and the overhead involved in the ownership and management of supporting hardware and software, alongside providing hosting services.

C. **Infrastructure as a Service (IaaS)**: This service grants a virtual data center so developers can maintain their databases, install their own operating systems, and support software. In fact, a subscriber is allowed access to an infinite pool of resources like compute resources with an unlimited storage and networking facility, which essentially grant them the installation and execution of any software-theirs for operating systems and applications. Users of such a cloud service do not have any operational rights over the underlying cloud architecture; they still might manage storage, deployed applications, OS, and networking elements. Many of the tasks associated with management and maintenance get abstracted and offered as a collection of services that are callable and automatable from code- and/or web-based management consoles when IaaS is being used. Even though the physical infrastructure is no longer part of their domain, developers must still design and build complete applications from scratch, and administrators have to install, maintain, and use third-party patch solutions. By launching from a web-based management console or contacting an application programming interface (API), the virtual infrastructure with Infrastructure as a Service (IaaS) can be up and operating in minutes and is available on-demand [7] [8].

III. Cloud Deployment Models

Six Deployment Models exist: Private Cloud, Public Cloud, Hybrid Cloud, Community Cloud, and Virtual Private Cloud. Inter-Cloud is being used to refer to Deployment models and has two different types of clouds: Federated Cloud and Multi-cloud. These clouds can be categorized into three main types: Private Cloud, Public Cloud, and Hybrid Cloud.

A. **Private Cloud:** The term private cloud deployment model is also known as the internal or corporate model. A private cloud is made for the consideration of any single company. Management and control of the system is centralized within that entity. However, in some cases, the private cloud server can be managed or hosted by a third-party provider or service provider. Most businesses prefer holding the hardware in their own data center and so have an internal team look after and manage everything.

B. **Public Cloud:** The public cloud model is one of the most established models for cloud computing. This kind of cloud is particularly favored for activities such as file-sharing, web application services, and non-confidential data storage. It is recommended for collaborative projects as well as software development. The service provider is the owner and operator of all the requisite hardware that supports the public cloud. Vendors set up their hardware in large data centers. Turning towards development and testing, the public cloud delivery mode is important in cases where public cloud infrastructure is used largely by developers mainly for testing and development purposes. A public cloud is the best in creating testing environments, which makes them economical, easy to set up, and fast to deploy.

C. **Hybrid Cloud:** Hybrid clouds comprise both public and private clouds. They are designed to enable the seamless transfer of data and applications as well as an easy platform-to-platform interaction. Hybrid cloud is the best answer for a company or organization that requires some features of both, usually depending on size and some industry aspects. It is a private cloud that originally was integrated into some public cloud services. When businesses have sensitive data that cannot be kept on cloud servers or when they have to comply with regulations requiring data storage, protection, and other measures, this deployment approach makes sense [9]. In addition to the corporate sector, educational institutions can use the hybrid cloud to expand their legacy on premise systems. They can create applications for resource management, employee data management, student data management, and other tasks on the public cloud, freeing up their IT staff to work on other projects. As an illustration, certain student databases may be stored on an on-site server, while student front-end web apps may be hosted on a public cloud. They can also dynamically shift workloads between public and private clouds, possibly for a certain amount of time, depending on particular performance or regularity requirements. Sensitive information on students, employees, and institutions can be protected with their own firewall and antivirus software. On the other hand, without requiring the installation of any extra hardware or software, the public cloud can offer a number of appealing advantages, such as research opportunities, study and lecture materials from distinguished instructors, virtual labs, and trends in job opportunities [10].

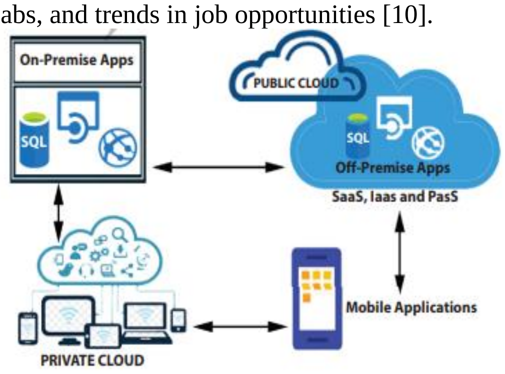

Figure 3 General architecture of hybrid cloud [10]

IV. Big Data

Big data is much larger and more difficult to manage and analyze compared to ordinary data. The enclosure of vast amounts of data requires the development of scale-out architecture, as well as efficient storage and housekeeping. The three Vs that define big data are volume, velocity, and variety. These attributes were put forth by Gartner in order to capture the varied challenges of big data. New-generation architecture has resulted in propounding the maintenance of data in various formats, thereby extending the three Vs to include value and veracity.

A. **Volume**: Data is ever-growing due to a plethora of sources such as sensors, social networks, smartphones, etc. The Internet generates vast amounts of data at a global scale. In 2012, an estimated 2.5 exabytes (EB) of data were being generated every day. The International Data Cooperation research asserts that by 2013, the amount had skyrocketed to 4.4 zettabytes (ZB). In 2020, this number grew significantly to reach 40 ZB.

B. **Velocity:** Currently, data is expanding rapidly and exponentially. Each day millions of devices are added into the net which increases the volume and velocity of the data. For example, YouTube is one of the data-generating engines, which generates mountains of data in no time. Figure 4 shows the five Vs of big data.

C. **Variety:** Numerous formats of data are produced by sensors, smartphones, and social networks. Data logs, photos, videos, audio, documents, and text are some of the formats in which these tools generate data. Moreover, data might be either unstructured, semi-structured, or structured.

D. **Value:** One vital aspect of big data is value. It all has to do with the treatment of data-how to change it into meaningful information.

E. **Veracity:** Noteworthy, veracity refers to the quality, accuracy, and reliability of data; hence, the integrity of data should be retained. For instance, smaller amounts of data can be synonymous with half or incomplete messages, whereas large amounts of data can lead to confusion.

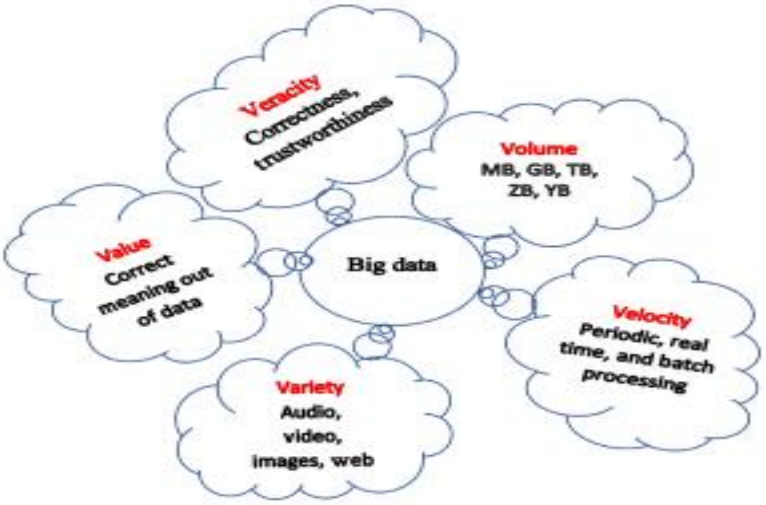
Veracity
Correctness, trustworthiness
Volume
MB, GB, TB, ZB, YB
Value
Correct meaning out of data
Big data
Velocity
Periodic, real time, and batch processing
Variety
Audio, video, images, web

Figure 4 Five Vs of big data [11]

Batch and stream data processing are the two primary categories. Batch processing is generally all about how data is processed in blocks that usually take quite an extended period to store. This implies that batch processing takes a longer time to complete because it tends to handle larger amounts of data. Hadoop is widely considered the best framework for batch processing of data because such an approach would prove effective when large amounts of data would have to be processed for more profound insights and would not need immediate or real-time analytics. On the contrary, streaming would refer to real-time data processing and analysis. Processing of incoming data without delay makes it possible for stream processing. The resulting analytics are then provided immediately to tools for detection and reporting. Such would be indicated, for example, in an anomaly that instantly points a finger to fraud. Real-time processing would also suit online retailers because it could easily tie together broader histories of consumer interaction with promotions to encourage immediate purchases. Cloud computing refers to delivering computer services through the Internet, or "the cloud," such as: servers, storage, databases, networking, software, analytics, intelligence, and everything else, to provide flexible resources, faster innovation, and costs efficiencies." Cloud computing has thus revolutionized the abstraction and utilization of computer infrastructure. Anything that can be considered a service, therefore, falls under the cloud umbrella (hence "x as a service"). With its many benefits, including elasticity, pay-as-you-go or pay-per-use, minimal upfront costs, etc., cloud computing has become a highly sought-after and viable option for big data management, analytics, and storage. Big data comprises many important factors for almost all businesses and industries today; hence, big data platforms from service providers like Amazon, Google, and Microsoft charge a very affordable price for it. These solutions become viable to businesses of all sizes through scalability [12].

V. Security Challenges

On the one hand, the adoption of cloud computing, while offering many advantages, has given rise to a complex challenge with respect to security: essentially, a security challenge is thrown at the organizational side, at the technological side, and at the legal side. Accordingly, all these would require a totality approach to risk management and security strategy. Cloud computing, in essence, poses very many unique challenges in governance organizationally, technically, and legally. For example, cloud computing takes away direct control from organizations over their IT infrastructure, thereby launching a new need for governance. The geographically distributed nature of cloud resources further complicates audit and compliance requirements. Human error, insider threats, and the risk of vendor lock-in further heighten concerns, especially in multi-tenant environments where co-tenant actions can impact performance and security. Technological challenges include risks from resource sharing, insecure APIs, and the potential for DDoS attacks, which exploit cloud elasticity to disrupt services or inflate costs. Centralized data storage makes cloud environments attractive targets for cybercriminals, with vulnerabilities in shared components posing systemic risks, including cross-tenant breaches. Legally, conflicting data protection laws and jurisdictional issues complicate compliance, especially for regulations like GDPR and HIPAA. Data sovereignty requirements and outdated software licensing models add further complexities, emphasizing the need for innovative strategies to address the evolving challenges of cloud computing [13].

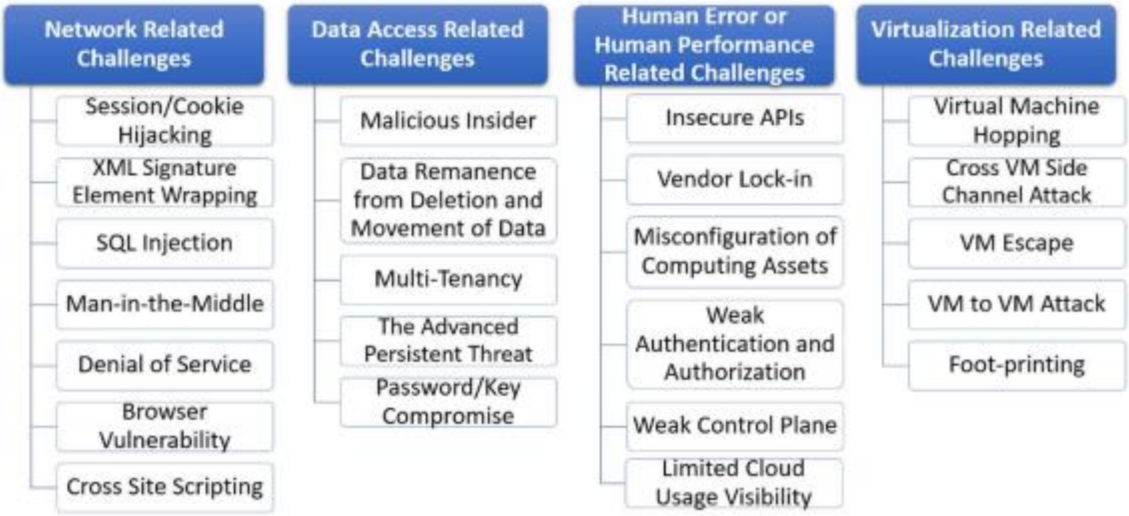
Network Related Challenges
Session/Cookie Hijacking
XML Signature Element Wrapping
SQL Injection
Man-in-the-Middle
Denial of Service
Browser Vulnerability
Cross Site Scripting
Data Access Related Challenges
Malicious Insider
Data Remanence from Deletion and Movement of Data
Multi-Tenancy
The Advanced Persistent Threat
Password/Key Compromise
Human Error or Human Performance Related Challenges
Insecure APIs
Vendor Lock-in
Misconfiguration of Computing Assets
Weak Authentication and Authorization
Weak Control Plane
Limited Cloud Usage Visibility
Virtualization Related Challenges
Virtual Machine Hopping
Cross VM Side Channel Attack
VM Escape
VM to VM Attack
Foot-printing

Figure 5 Cloud Security Challenges and Threats [14]

Cloud systems are vulnerable to various attacks that exploit sessions, cookies, and other security gaps. Session hijacking occurs when attackers gain access to valid session IDs, enabling them to impersonate users and access private cloud-stored data. XML Signature Element Wrapping involves altering SOAP messages to mislead users, compromising data integrity. SQL Injection abuses the weaknesses of SQL scripting and is used to gain access to sensitive information in the databases. Man-in-the-Middle (MiTM) attacks, on the other hand, intercept communications between two parties, read and modify the contents, and steal the confidential data. A variant, termed Man-in-the-Cloud (MiTC), focuses on attacking session management of the cloud systems. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks tend to comprise a flood of such cloud resources, owing to which those resources become unavailable to legitimate users. Such attacks may target various layered networks and also take advantage of server protocol vulnerabilities to bring the service down. Finally, exploitations by means of vulnerabilities found in browsers pose another threat, which allows attackers to break into the cloud illegally by means of exploiting the weak authentication mechanisms. Another such attack, Cross-Site Scripting (XSS), allows attackers to inject client-side scripts into web applications, which results in data leakages. Cloud environments demand consistent security configurations across diverse and dynamic resources, including virtual machines, databases, and serverless functions. Fast creation, scaling, and termination of resources complicate the maintenance of security settings. Security misconfigurations, such as faulty firewall rules or erroneous access policies, are a major contributor to data breaches, which ultimately allow unauthorized access to sensitive resources. Problems become graver under multi-cloud and hybrid strategies, which distribute services across different providers, regions, and accounts, making uniform security enforcement practically impossible. Manual configuration efforts often deviate from best practices, leading to "configuration drift" that weakens the overall security posture. Compliance with regulatory standards requires continuous alignment with organizational security policies, with failures risking legal and financial penalties. APIs, critical for cloud service interactions, present vulnerabilities when inadequately secured. Vulnerable API architecture, weak authentication, poor data handling, and denial of robust authorization mechanisms enhance the risks such as breach of data, injection attacks and unauthorized access. Third-party APIs expand the attack surface, complicating security in multi-cloud and hybrid environments [14] [15].

VI. Encryption Algorithm for Enhanced Cloud Security

The goal of ensuring the confidentiality and availability of the data to the legitimate recipient without allowing any compromise from a third party is achieved through encryption methods. A schematic view of encryption and decryption is presented in Figure 6. According to Figure 6, the user would send the message through the communication channels after encrypting it using a secret key, with the recipient decrypting the message using the same secret key. Moreover, cryptography does provide some other guarantees of data privacy-and so on-preventing from data alteration, just to mention a few.

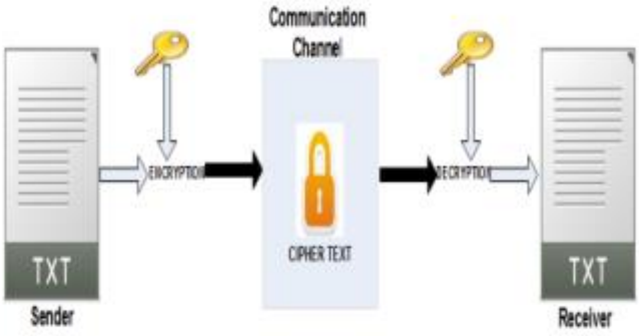

Figure 6 Working of Encryption and Decryption [16].

AES is one of the most popular encryption protection schemes today. It was developed by Joan Daemen and Vincent Rijmen in 1998, and the NIST confirmed it in 2000. Due to its superior performance, the AES has been widely adopted. The sizes of blocks and the keys are involved. The key may have a length of 128, 192, or 256 bits, whereas the data block is 128 bits long. The algorithm's difficulty is determined by the key's size and repetition. Complexity and CPU utilization increase with increased key size or repetition. This work requires less processing time. Then, a key size of 128 bits is adequate. The operational measures for transforming rounds during the encryption operation include sub-bytes, shift-rows, mix-columns, and add-round key operations. The sub-bytes consist of an S-box table which is based on Shannon's principle of confusion because it replaces each byte from the block with another new block. When the Shift Rows are used, the ith row of the matrix is cyclically shifted to the left by i positions. The Shannon diffusion principle is duly taken care of. A state-matrix-length uniform matrix is multiplied with the state matrix to carry out the mix-columns transformation. This step also employs the Shannon diffusion principle, to finish with round key XORed with the state matrix to yield an intermediate matrix. ECC came in as a public key revolution after the year 1987 with its short operand lengths in comparison with previous asymmetric methods. ECC benefits from fast computation and lesser power and memory requirements. With respect to digital signatures, key exchange, and authentication, ECC can be used for all these purposes. Following is the equation for an elliptical curve:

$$y^2 = x^3 + ax + b$$

(i)

Suppose x and y are finite fields, be it primary or binary fields, both fixed values for parameters a and b. A point P is multiplied by an integer k to produce a new point Q belonging to the curve in the point multiplication of ECC. The longest operation in ECC is point multiplication. ECC is based on scalar multiplication, and it is calculable with diverse algorithms. The most commonly used type immune from side channel attacks is Montgomery scalar multiplication. To calculate point multiplication Q = k.P, two basic operations have to be computed, namely PA and PD. While PA computes a third point on the curve when two different input points are used, PD computes a third point on the curve with the inputs being the same point. PA and PD are arithmetic operations comprised of addition, multiplication, squaring, subtraction, and inversion. In both PD and PA, Lopez and Dahab projective operations are used to evade modular inversion. The capacity of conducting the multiplication of hashes and other point treatments is directly related to the security degree of ECC. It can be noted that both parallel operations are computed independently using the Montgomery algorithm [17].

Diffie-Hellman public key was the first public key system to be presented to the world, and, initially, it only allowed for key exchange between parties who knew each other. The ElGamal system extended this to allow for full public key encryption and signature systems for ECC cryptography. Shortly following Diffie-Hellman was the public release of the RSA cryptosystem (Rivest Shamir Adleman). The RSA algorithm allows for two keys to be used in cryptographic contexts: one for encryption, called the public key, which is available to anyone interested in secure communication with the owner of that key, and the other for decryption. The private key is kept private and used for decryption. RSA algorithm security relies on the separate mathematical problems: the RSA problem, which states that deriving the private key from the public key cannot be computed in polynomial time and thus is practically infeasible; and the factorization of big numbers, which becomes practically impossible when the numbers are large enough. Standard RSA most recently finds application in key exchanges, digital signatures, web browsers, chat applications, emails, VPNs, and any other type of communication that requires transmission of data from one party to another. The security of RSA relies fundamentally on the practical difficulty of factoring the product of two large prime numbers, the 'factoring problem'. There is this problem in breaking the RSA codeknown as the RSA problem. RSA algorithm is a relatively slow algorithm compared to other widely used ones. It is rarely used for encryption. Instead, it encrypts the shared keys computed from symmetric key cryptography for bulk encryption - decryption. A lot of data information has been secured over the years by means of the RSA algorithm at different areas of application. These include areas like cloud servers, key exchanges, and internet protocol, and any area that requires two parties' secure transmission of data. Nowadays, more and more researchers are conducting studies on how to make RSA more applicable in IoT devices as well as smart and lightweight gadgets. The reason for such a vast application of RSA is that it offers security unbreachable by normal day PCs and systems. However, there exist many reports lately concerning the breaking of RSA ciphers for shorter key sizes, which would eventually warrant researchers and cryptographers to come up with an improved version of RSA. Whether it is any symmetric cryptosystem or public cryptosystem, RSA is one the most considerable algorithm among all, and numerous research works are going on a continuous basis on its enhancement in terms of its security and performance to make the RSA more complex and reliable along with increasing its encryption and decryption speed [18] [19].

Table 1 Comparison of AES, ECC and RSA

Feature	**AES (Advanced Encryption Standard)**	**ECC (Elliptic Curve Cryptography)**	**RSA (Rivest-Shamir-Adleman)**
Type	Symmetric-key encryption	Asymmetric-key encryption	Asymmetric-key encryption
Key Sizes	128, 192, or 256 bits	160–512 bits (smaller keys	1024, 2048, 4096 bits (larger

		for equivalent security to RSA)	keys for equivalent security)
Performance	Fast encryption/decryption, low computational overhead	High computational efficiency, low resource consumption	Slower encryption/decryption, higher computational demand
Security	Based on substitution-permutation network; resistant to brute force	Security depends on the hardness of the Elliptic Curve Discrete Logarithm Problem.	Given the difficulty of factoring large primes
Usage Scenarios	Bulk data encryption, VPNs, databases, storage encryption	Secure key exchange, digital signatures, lightweight devices	Secure data transmission, digital signatures, key exchanges
Strengths	- High speed and efficiency	- Strong security with small keys	- Strong security for key exchanges
	- Widely supported and standardized	- Suitable for resource-constrained devices	- Well-established, broadly supported
Limitations	- Requires secure key distribution	- Less established than RSA in legacy systems	- Slower compared to ECC and AES
	- Vulnerable to side-channel attacks if not implemented carefully	- Complex to implement correctly	- Large key size increases computational cost
Best for	- Encrypting large data blocks quickly	- Devices with limited processing power	- Scenarios needing secure transmission and key exchange

VII Conclusion

Cloud computing, shouldering the heavy burden of transforming the technological landscapes, has turned the IT world upside down, thereby fostering hurriedly-deployed, scalable, managed resources. However, the inherent vulnerabilities of cloud environments, such as misconfigurations, session hijacking, and insecure APIs, necessitate robust security measures. Advanced encryption algorithms like AES, ECC, and RSA play a critical role in safeguarding cloud systems by providing confidentiality, ensuring data integrity, and controlling access. AES is highly efficient for large data sets, ECC offers strong security with minimal computational overhead, and RSA ensures secure key exchanges. Together, these encryption techniques provide a multi-layered approach to securing cloud services against modern cyber threats. Future developments in encryption, including quantum-resistant algorithms, will be crucial in maintaining cloud security as threats evolve.

References

[1] Segun-Falade, O. D., Osundare, O. S., Kedi, W. E., Okeleke, P. A., Ijomah, T. I., & Abdul-Azeez, O. Y. (2024). Assessing the transformative impact of cloud computing on software deployment and management. *Computer Science & IT Research Journal*, *5*(8).

[2] Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, *1*(2), 1-7.

[3] Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., ... & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. *Automation in Construction*, *122*, 103441.

[4] Zhang, Y., Liu, B., Gong, Y., Huang, J., Xu, J., & Wan, W. (2024, April). Application of machine learning optimization in cloud computing resource scheduling and management. In *Proceedings of the 5th International Conference on Computer Information and Big Data Applications* (pp. 171-175).

[5] Mistry, H. K., Mavani, C., Goswami, A., & Patel, R. (2024). The impact of cloud computing and ai on industry dynamics and competition. *Educational Administration: Theory and Practice*, *30*(7), 797-804.

[6] Fatima, E., Sumra, I. A., & Naveed, R. (2024). A comprehensive survey on security threats and challenges in cloud computing models (SaaS, PaaS and IaaS). *Journal of Computing & Biomedical Informatics*, *7*(01), 537-544.

[7] Rostami, A. (2021). Cloud Service Models-IaaS, PaaS, and SaaS.

[8] Nguyen, V. N. H. (2021). SaaS, IaaS, and PaaS: Cloud-computing in Supply Chain Management. Case study: Food Service Ltd.

[9] Patel, H. B., & Kansara, N. (2021). Cloud Computing Deployment Models: A Comparative Study. *International Journal of Innovative Research in Computer Science & Technology (IJIRCST)*.

[10] Deb, M., & Choudhury, A. (2021). Hybrid cloud: A new paradigm in cloud computing. *Machine learning techniques and analytics for cloud security*, 1-23.

[11] Sandhu, A. K. (2021). Big data with cloud computing: Discussions and challenges. *Big Data Mining and Analytics*, *5*(1), 32-40.

[12] Berisha, B., Mëziu, E., & Shabani, I. (2022). Big data analytics in Cloud computing: an overview. *Journal of Cloud Computing*, *11*(1), 24.

[13] Adeusi, O. C., Adebayo, Y. O., Ayodele, P. A., Onikoyi, T. T., Adebayo, K. B., & Adenekan, I. O. (2024). IT standardization in cloud computing: Security challenges, benefits, and future directions. *World Journal of Advanced Research and Reviews*, *22*(05), 2050-2057.

[14] Chuka-Maduji, N., & Anu, V. (2021). Cloud computing security challenges and related defensive measures: A survey and taxonomy. *SN Computer Science*, *2*(4), 331.

[15] Vakhula, O., Opirskyy, I., & Mykhaylova, O. (2023). Research on Security Challenges in Cloud Environments and Solutions based on the" Security-as-Code" Approach. In *CPITS II* (pp. 55-69).

[16] Muhammed, R. K., Faraj, K. H. A., Gul-Mohammed, J. F., Al Attar, T. N. A., Saydah, S. J., & Rashid, D. A. (2024). Automated Performance analysis E-services by AES-Based Hybrid Cryptosystems with RSA, ElGamal, and ECC. *Advances in Science, Technology and Engineering Systems Journal*, *9*(3), 84-91.

[17] Hafsa, A., Sghaier, A., Malek, J., & Machhout, M. (2021). Image encryption method based on improved ECC and modified AES algorithm. *Multimedia Tools and Applications*, *80*, 19769-19801.

[18] Ugbedeojo, M., Adebiyi, M. O., Aroba, O. J., & Adebiyi, A. A. (2024). RSA and Elliptic Curve Encryption System: A Systematic Literature Review. *International Journal of Information Security and Privacy (IJISP)*, *18*(1), 1-27.

[19] Imam, R., Areeb, Q. M., Alturki, A., & Anwer, F. (2021). Systematic and critical review of rsa based public key cryptographic schemes: Past and present status. *IEEE access*, *9*, 155949-155976.