International Journal of

INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Designing a Security Framework for Mitigating Flaws in Cloud Based Web Hosting for Privacy and Confidentiality Services

[1]Surbhi Khare, [2]Dr. Vijayant Verma

Submitted: 09/05/2023 **Revised**: 16/07/2023 **Accepted**: 07/08/2023

Abstract: The rapid growth in popularity of computing clouds has attracted and allowed intensive processing on resource-constrained client devices. Smart mobiles can install data- and computation-intensive programs thanks to the demand service model utilized by distant data centers Outsourcing personal and sensitive data to far-off data centers, on the other hand, creates significant privacy and security issues. It is necessary to improve the traditional advanced encryption standard (AES) algorithm in order to fulfill the rising security concerns in the cloud. Among the various advantages presented in this research are, for example, increased data security and owner privacy. The encryption speed is increased from 128 to 1000 bits per second with the help of a double round key. There was once a round key that could handle 800 blocks per second. Network trust and resource management may be enhanced while consuming less power and better load balancing by adopting the suggested strategy. In the proposed framework, AES will be utilized with plain text sized at 16, 32, 64, and 128 bytes. The simulation results are shown to show how well the algorithm meets quality standards. The proposed architecture, according to the results, reduces energy use by 14.43%, network utilization by 11.533%, and delay by 15.673%. This new design increases security while also making better use of resources and reducing the amount of time it takes to build new computational cloud services.

Keywords: *Resource constraint, privacy, AES, Far-off data, Network Trust, computing clouds*

1. Introduction

Various architectures, services that integrate other technologies, and software design methods all make advantage of cloud technology [1]. Models for delivering on-demand cloud services include those that use platforms as well as those that use software as well, as well as those that use infrastructure (IaaS). Four cloud platform deployment paradigms are used to design architecture solutions for public, private, community, and hybrid clouds [2]. While traditional online computing and storage methods have flexibility, accessibility and capacity, cloud computing offers all of these and more. [4] Worries about privacy and data security with cloud service providers as well as (ii) concerns about user security abound in the age of cloud computing. There have been several attempts to weaken the AES (advanced encryption standard) algorithm in the literature [5.]. The AES (advanced encryption standard) structure is attacked and defects are introduced with the goal of recovering the secret information [6].

In addition, standard cloud computing strategies, such as the use of computational resources to provide exceptional computer application, telecommunications service, social networking, and web service performance [7, 8], may suggest some potential service activities. Users may save and remotely retrieve their data at any time without extra burden thanks to cloud storage in data centers [9, 10]. The main concern with cloud data storage, on the other hand, is security. Consequently, to ensure the accuracy and integrity of cloud-stored data, cloud data centers must have safeguards in place.

While encrypting/decrypting data, current cybersecurity solutions focus on only one or two features: poor security and high time consumption. As a result, the process will take longer, using more network resources, power, and causing a delay in the network [12–16]. Security is a key component of cloud computing; therefore, it must be given to users. Cloud computing is a platform for effectively exchanging data and resources. Because of this, cloud service providers have a duty of care to guarantee security across all dimensions, including the usage of resources like electricity, network latency, and time. Already, currently available approaches are incapable of accurately quantifying the security of cloud services. Cloud computing's secure framework is a means for simplifying the management and access to computer resources, and a cost-effective solution is critical. The framework should consume little power, time, and latency on the network, while encrypting and decrypting data to improve data security in cloud computing. By implementing a novel encryption/decryption strategy, the study adds to the design of the security framework. Additionally, it establishes the critical components of the cloud computing community's security framework. Cloud users and cloud service providers with similar security needs would benefit from this. Framework allows quicker calculation with reduced network use and network latency thanks to smart algorithm. The framework establishes confidence between users and enables the usage of trusted

[1] *Department of CSE, MATS School of Engineering & IT Raipur, India*

[2] *Department of CSE, MATS School of Engineering & IT Raipur, India*

[1] *surbhikhare20@gmail.com*

[2] *drvijyantverma@matsuniversity.ac.in.*

gateways through the use of a symmetrical encryption mechanism. The suggested framework incorporates crucial aspects such as better security and data privacy for the owner. By utilizing the double round key feature, it alters the 128 AES method to enhance the encryption process's speed to 1000 blocks per second. In the past, a single round key was capable of processing 800 blocks per second, which was rather impressive.

By using the proposed method, network trust and resource management will be improved while using less power and providing better load balancing. AES will be used with plain text sized at 16, 32, 64, and 128 bytes, respectively, in the proposed framework. A visualization of the simulation results demonstrates the algorithm's appropriateness for achieving certain quality requirements. The energy consumption of this framework is lowered by 14.43 percent, network use is decreased by 11.53 percent, and latency is reduced by 15.67 percent. As a result, the proposed architecture improves security, increases resource efficiency, and minimizes the amount of time required to develop a computational cloud-based service.

Recently, cloud computing has emerged as a cutting-edge contemporary technology, and it is widely expected to take off in the future years. The use of cloud computing raises new security issues and challenges [17]. In recent years, it has gone from being just an idea to making up a significant chunk of the IT industry. The use of virtualization, SOA, and utility computing is often referred to as cloud computing, which utilizes three different architectures: SAAS, PAAS, and IAAS. Issues and difficulties are specific to each cloud computing platform. PCI-DSS, ITIL, and ISO-27001/27002 standards [18], [19] are used to handle and assess security risks and problems.

Three major components of cloud computing are software as a service, platform as a service, and infrastructure as a service (infrastructure as a service). As depicted in Figure 1, a large number of clients have access to an application housed in the data center of a SaaS provider. There are several well-known SaaS systems, such as Oracle CRM on Demand or Salesforce.com.

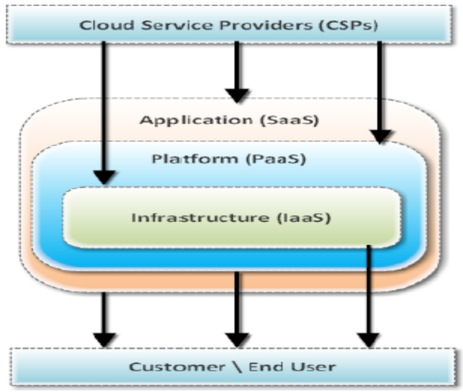


Fig 1: Environment of Cloud Computing

Customers no longer have to make long-term commitments to conventional hosting because of this advancement, which allows them to use resources as needed. Amazon Web Services' Elastic Compute Cloud (EC2) and Secure Storage Service are two instances of Infrastructure as a Service (IaaS) products (S3). There are a number of significant issues with cloud computing that need to be addressed. Securing cloud computing data has become a top priority, since it is both a driving factor behind its growing popularity and a major constraint. In recent years, cloud services have experienced a rash of security breaches. For instance, Google leaked a large quantity of papers in March 2009. For approximately 22 hours, the Microsoft Azure platform was unavailable. In April 2011, Amazon's EC2 service was disrupted, affecting Quora, Reddit, and other services. When these security breaches occurred, they resulted in significant loss, if not destruction. As a result, addressing security issues is critical before a company or organization may use cloud computing services. [20][21].

2. Literature Review

Providers of cloud data management systems have been advised to use a generic security management framework to develop and execute complex security rules. Using an expressive policy description language, they developed a framework to identify and prevent a broad range of attacks, which they then integrated into a number of data management systems effortlessly. BlobSeer was used to evaluate their security architecture, and the results showed that the system could effectively protect itself against an attack. Blob Seer's resilience to a denial-of-service attack was tested on the Grid 5000 tested.

[22] looked at the problem of ensuring a client that his cloud data is accurate and intact. Cloud computing allows users to check the integrity of their data even when it is not physically available to them. This is especially important if they have sensitive information in their cloud storage. By showing the data's integrity, customers may verify that their cloud-based data is accurate according to a technique developed by the authors. This proof may be accepted by both the cloud provider and the customer, and it will be included in the SLA. Thin clients benefit from this approach since it minimizes client-side storage requirements.

According to [23] cloud computing raises a number of security and privacy issues. To address these issues, four methods were suggested, including the following: It is possible to construct a single algorithm, referred to as cloud-based RBAC, by using Role-Based Access Control (RBAC) [24] and cloud computing together. This technique's author discusses such fundamentals as Cloud User, Permission, Role, and Session. Cloud Users may opt to have certain tasks allocated to them at the beginning of each session (permissions). Certain requests become acceptable after the Role is active. Attacks on user data may be stopped using this strategy since a user must be authorized to conduct anything of the kind. This system handles the challenge of having several policies while also choosing dynamically the dominant policy during a certain data processing operation. Finally, an identity management technique is used to prevent secondary data from being used without the proper authorization.

As a result of virtualization, people using the cloud are losing control of their data. User-centric identity management was given the Cloud Privacy Label (CPL) by the author [25]. The Third-Party Auditor (TPA) [26] was created by the author to ensure that cloud service providers and cloud clients are equally capable of resolving this issue.. Authors have emphasized that even if their solutions focus on just a few aspects of cloud security, new techniques will be required to guarantee a more secure cloud.

[27-30] looked at cloud computing security from an academic perspective. There was a lot of discussion about cloud service security and how to combat it. Some of the concerns mentioned were VM-level assaults, failure to isolate, compromising of the management interface, and regulatory compliance difficulties. Assaults and attacks might be thwarted using the architecture of cloud security they demonstrated. According to the authors, the architecture incorporates a defense-in-depth strategy, a single administration dashboard, and security for virtual machines (VMs).

[31-35] Wayne: There are many benefits to using cloud computing, but there are also many concerns about cloud security that must be addressed. Securing mission-critical systems requires planning and design. The end user's security concerns must be addressed. Cloud computing security is a challenge that academics and industry specialists must work together to solve. To prevent unwanted access to corporate data centers and cloud servers, strict security measures must be established. According to the findings of this study, there are many major cloud security issues. It also looks at major privacy and security issues. It focuses mainly on public clouds, which require careful consideration, and provides businesses with the data and statistics they need to make informed data security choices. One of the most important security challenges discussed in this article is that of end-user trust, as well as access control and identity management as well as security on the servers themselves.

Of particular significance has been the discovery and explanation of cloud computing security problems, as well as the education of end users on the security and privacy dangers connected with cloud services itself. It is a concern that no framework or instrument has been proposed to deal with the difficulties that have been brought to light. When cloud service providers apply appropriate designs for implementing security measures despite their deep-seated anxieties and misgivings about cloud computing, users may benefit from the benefits of cloud computing without anxiety, according to M. Okuhara et al. [36]. Fujitsu provides an overview of their security architecture to address cloud computing security concerns.

Security should not deteriorate as cloud computing advances. [37] examines in great detail the security risks with cloud computing. If consumers are not to endure a security retreat, computer technology and security must both grow together. According to [38], the cloud may be better for business intelligence than the isolated alternative as long as developments in trustworthy computing and computing that permit encryption continue. [39] describes the physical and operational security procedures used by Amazon Web Services (AWS) to protect networks and buildings under its management. Additionally, it offers security solutions unique to Amazon Web Services (AWS).

Numerous modifications have been made to AES in attempt to improve its performance and security by adding complexities to the algorithms. There are many software and hardware platforms where these alterations are made. The preview framework's security, on the other hand, is a source of concern owing to the limitations and problems that come with cloud computing. On order to keep your data safe in the cloud, you need utilize cryptography methods.

Massive encryption methods are used in cloud computing security frameworks. Several of them are discussed in this article. The security architecture relies on a multicloud environment to keep digital data safe. They divided the input appearance into several pieces using a segmentation method to prevent data leaking. The accuracy of the watermarking procedure is made possible by the reliability of the outsourced customers' data. The digital signature and watermarking approaches can be used to detect any unintended changes to outsourced clients' data [40]. This study focuses on the computation of several strategies for increasing data security in order to prevent various security assaults and breaches. ECC and MD5 were employed as mitigation techniques for the HMAC (Hashed Message Authentication Code) in this research. Since it is built on a security hierarchy, the suggested method provides access control as well as authentication and secrecy. According to the authors, they verified and tested the security solution in a genuine cloud computing environment in real time, and found that it had a very low upload and download service time overhead. This study's structure is more secure and protects user data better. Using this design, data is separated into discrete bit blocks. Every second block of bits, a genetic algorithm is used. Genomic algorithms generate ciphertext and bits in two different ways. In the cloud, each ciphertext is kept independently and without security. Because of this, attackers will have a harder time figuring out exactly where the ciphertext is stored. In order to determine the minor block size, the new security architecture uses a genetic process. This increases security. Data is encrypted and accessed via a proficiency list in the architecture [41].

The study's authors presented a new paradigm for data security and integrity by focusing on encryption and decryption technologies to secure cloud users' data. One strategy advocated emphasized enhanced security while also enhancing speed. Detection of malware and real-time monitoring of the system were also part of their approach. [42]. This study's authors suggested a system for storing data across several clouds. Three-DES and one-way AES are used to encrypt the data. This approach, on the other hand, is inefficient, breaches user privacy, and loads middleware with unnecessary functionality [43]. This article's authors looked at several types of cloud penetration data preservation licensing framework approval. Both common and sensitive cloud data are secure with the three-cover architecture. Constraints imposed by the security architecture of the three films include security and privacy safeguards, as well as safety and approval processes [19].

Using quality indicators, the researchers examine instance cloud service broker frameworks in depth. When cloud service providers are leveraging these streak measurements to enforce standards, the quality-based cloud service broker architecture is employed (QCSB). QCSB's method and implementation are described in full in a new study. Conclusion: To assist cloud computing select the right CSP (cloud service provider), QCSB suggests creating a relationship between possible CSPs and customer quality preferences [44]. QCSB does both of these things. The difficulty was discovered as a result of the Mix Column conversion of AES having illogical objectives. An updated version of AES does away with these logical responsibilities altogether. Using the enhanced AES, it was possible to reduce LUTs by 13.6%, share discounts by 10.93%, and interruption eating by 1.19% all at the same time. Similarly, the conservative AES's low dispersion rate and large agenda sequences are described in [45], where it was accomplished at the first nonentity.

Visual examination, file size, radiance histogram, pixel-level assessment and distance from the display were all factors considered by these researchers. The average fraction value changed by 23.85% when comparing the unique file to the encrypt duplicate file, whereas it changed by 1.45% when comparing the innovative file to the decrypt duplicate file [46]. Fog computing and the Internet of Things integration research needs and suggestions were also mentioned in this study. It provided an overview of current studies on fog computing, the Internet of Things, and their applications (Internet of things). A framework for fog computing was presented [29].

In addition, it explains how to determine estimated presentation limitations such as the regular reversal time, the quantity and period of implementation as well as the pan of kinds and the complete conclusion duration [47]. A solution for different security services such as verification was presented for cloud computing, which addressed several difficulties with disparate data security and privacy. Using cloud computing, real-world users will have easier access to cloud data. For privacy, authenticity, and contact management, 128-bit AES encryption is repeated [48]. For workload distribution, this article looks about Round-Robin and Supper Present Implementation Freight (also known as Active Monitoring Load Balancer), which are two of the most often used approaches. Cloud analyst toolkit makes advantage of all of these Java-based virtual approaches. To demonstrate the comparison analysis, graph approaches have been recycled [49]. Cryptography is a process that comprises two primary steps: encryption and decryption. The encryption approach converts a standard document into an inventive text that no one else can deliver or understand except the receiver. A hybrid method to cryptography makes use of the Blowfish and AES algorithms. Thus, the only person who can decode the cryptograph text is the recipient [50].

We demonstrate how to design a low-control AES architecture with decreased trip magnitude and consumption using shift catalogs and variation for key/data storage. Controlling exchangeable on S-boxes is done using a low-power technology called clock gating. Research projects in these areas have as their main goal the identification of ways for improving cloud computing security. In the end, this research offers an AES-encrypted architecture for safeguarding confidential tasks stored in cloud platforms. Comparing findings obtained with this proposed framework to prior framework work shows that cloud computing benefits greatly from adopting the proposed framework. Our modified AES varies from other previously produced or modified AES presented in the study in terms of the JAVA cipher-based security architecture. Keep in mind that our trust-based strategy places suspects in a queue to protect the network's trustworthiness and bans them from using it.

The aforementioned literature study detailed the findings of many academics. As can be seen, security is a critical necessity, and numerous techniques have been created to ensure cloud security. According to the literature, a more robust encryption technique is required for cloud computing. The algorithm should be responsive. The parts that follow will detail the implementation of the proposed encryption techniques.

3. Cloud Computing Threats

Cloud service security concerns will be examined in this section. On the basis of our experience moving to the cloud, we address some of the risks and mitigations that may be connected with it. [7].

S.no.	Type of Cloud Computing Threats	Description
1	Modifications to the Business Model	Companies must weigh the dangers of losing control of infrastructure when relying on external service providers for servers, storage, and applications.
2	Cloud Computing Abuse	service providers give a free trial period. It is possible that malevolent users or spammers may utilize the trials to their advantage if the security measures are not taken
3	Insecure APIs and Interfaces	Violations of the current API may be transmitted to the Cloud through these interfaces.
4	Insiders with a Bad Motive	A trusted insider, on the other hand, may turn sour. If malicious insiders manage to access and control Cloud services without being detected, it might have a substantial impact on the company's offerings. When it comes to software as a service, this risk level may apply.
5	Issues with Shared Technology/Multi-tenancy	Multiple users of the virtual machine may all use the same program at the same time. Because of these hypervisor vulnerabilities, a malicious user may take control of a legitimate user's virtual machine and exploit it for his or her own purposes.
6	Loss and Leaking of Data	Insufficient disaster recovery, unstable data centers; inadequate encryption techniques; weak keys; and association risk. This is a danger that SaaS, PaaS, and IaaS are all exposed to.
7	Service Espionage	Phishing efforts, fraud, and exploiting software vulnerabilities all represent a danger to service or account hijacking.
8	Profiling of Potential Risks	lack of knowledge of internal security procedures and security compliance as well as the need for further hardening, patching, and audits.
9	Identity Theft	identity theft, the victim may bear the brunt of the harm and financial loss that the offender has caused. Among the security risks to be aware of include phishing efforts,

Cloud Computing Attacks

The following attacks may be carried out by an adversary by taking advantage of Cloud vulnerabilities.

S.no.	Types of attack	Description
1	Zombie Assault	Denial of Service (DoS) attacks on servers may occur. attackers flood the cloud with malicious queries, the services go down.
2	Injection of a Service	Attacker develops and integrates malicious SaaS, PaaS, or Cloud-based IaaS services on your network. If an attacker is successful, legitimate requests will be automatically routed to the fraudulent services
3	Virtualization-Related Attacks	Bypassing the isolation layer, attacker access to any virtual machine running on the host and the ability to change the system's behavior.
4	Man-in-the Middle Attack	Attacker could be able to intercept data being sent between cloud data centers.
5	Attempted Spoofing of Metadata	The attacker successfully interrupts the Web Services Description Language (WSDL) files file's service invocation code during delivery.
6	Phishing Attack	Phishing attacks work by modifying web links and redirecting visitors to a fake site in order to acquire sensitive data.
7	Invasion of a Hidden Backdoor	Hackers may remotely manipulate the compromised machine via a passive attack

4. Proposed Secure Framework for Cloud Computing (SFCC) Architecture

The architecture of the SFCC (Secure Framework for Cloud Computing) is shown in Figure 2. The security architecture provides the information required for secure technologies to work across cloud computing components and serves as a basis for secure cloud computing. Figure 1: Security Architecture Specifically, this framework looks for the following requirements: security, privacy, load balancing, and trust. Framework gateways are used to communicate with cloud beneficiaries, who reply to requests from users and provide the data back to them. The framework that is being suggested is comprised of the following components:

As part of the construction process, the Cloud Service Provider (CSP) layer manages critical resources and abilities while also calculating and directing cloud storage servers' operations and an obscure work out approach that are scattered throughout a network. SaaS (Software as a Service) is a business idea in which software programs are made accessible to end consumers on a subscription basis (as a service). There is a method of submitting requests known as PaaS (platform as a service, or software as a service). This strategy incorporates all of the development tools needed to create more complex apps. Described as an infrastructure service, infrastructure as a service includes necessary components including real computers, virtual machines, and virtual storage. Controlling the security service's relationship with its clients Gateways for trust management are in charge of service configuration as well as all other components, including security management. The sections that follow provide more in-depth information on each of the units.

In addition to implementing functionality, the security management layer also offers data on security and privacy. Modules and data related with the security service are listed below

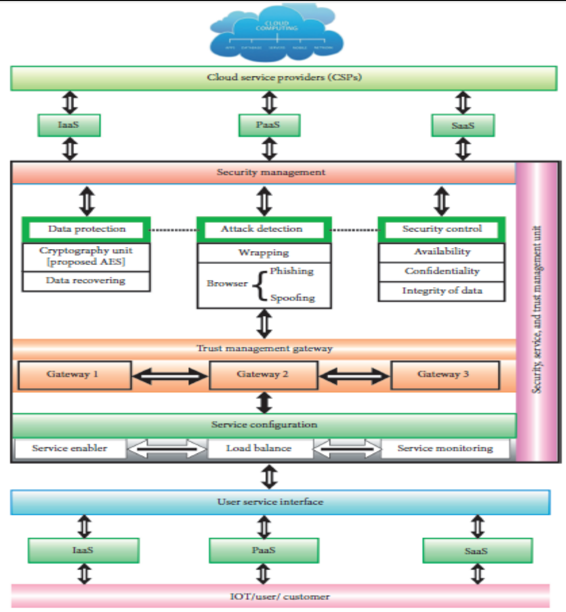


Fig 2: Secure Framework for Clod Computing (SFCC)

The proportion of time that a service is available is referred to as its availability rate. Security relies heavily on confidentiality (authentication, authorisation, and identity). It protects cloud-based data against unauthorized or accidental access. After signing in using a web browser, the average user is usually very good at remembering usernames and passwords. The correctness of data calculations generated from the combination of multiple files and their delivery are both the responsibility of the integrity of the data security control.

Finally, occurrences are defined as acts that occur on a semi-regular basis that violate cloud security standards (e.g., integrity, confidentiality, and availability). By encapsulating communications between two individuals, an attacker may take advantage of consumers' ignorance and continue to think that data is coming from the real root. Illegal behaviour, such as phishing, spoofing and altering browser certificates, may be detected by using unethical surfing to look for it.

For better data security, the data protection unit suggests employing AES ciphers, which can encrypt 128-bit data blocks at 1000 blocks per second with the double round key feature while consuming less power and balancing load. We employed symmetric identification to identify data streams by encrypting and decrypting using the same encryption key. As a result, both software and hardware benefit from it. Symmetric keys have the benefit of allowing for the secure storage of vast amounts of data without concern about its exploitation. It must be feasible to recover or restore lost data if a catastrophe destroys it.

The fourth layer of security is comprised of trustworthy gateways. To decrypt the data, these gateways must be linked to an authentic internet protocol address for the relevant domain. These entryways are designed to deal with problems associated with trust. Two of the three gateways are configured differently. Secure gateways will be used instead of the default one if the default one is attacked or misused.

The enabler creates a tailored cloud service based on the user's profile in order to facilitate integration and interoperability. Load balancing may be accomplished by the use of hardware, software, or a combination of the two. This setup necessitates using a single directory service for all instances of identity server. Automated facility inspections guarantee an extremely high level of facility presentation and accessibility via service monitoring. As a result of this layer, customers may access a wide range of services via the internet, including software services such as Software-As-A-Service and platform services like PaaS. (IaaS). When it comes to transmitting and receiving data, the service configuration layer is the last point of contact for users, IoT, and customers.

Under this part, we will talk about cloud computing's security paradigm and how it compares to the threats described before. Following are the security units that make up the model shown in Figure 3.

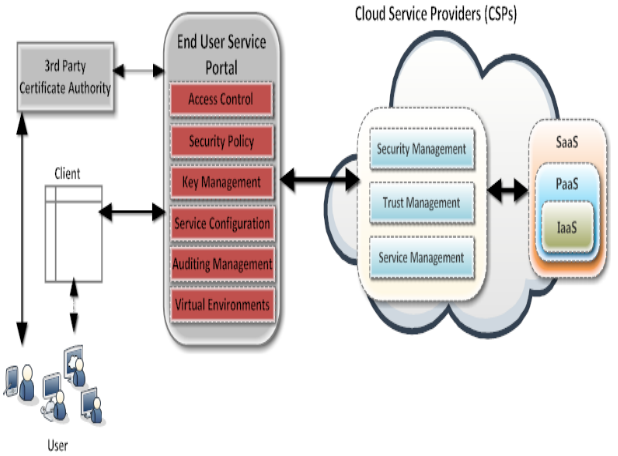


Fig 3: Cloud Computing Secure Model

A third-party certificate authority may certify the user, and the End User Service Portal can subsequently issue a service token. Users may use a single service provider's cloud services after registering with the portal. With the End User Service Portal, which includes VPN and cloud service administration and setup for secure remote access control, access control is made possible via the use of virtual private networks (VPNs) and security policy management, key management, and service configuration.

5. SFCC Experimentation and Implementation

Figure 4 depicts a secure cloud computing framework that is based on a security model that describes each component and applies the necessary security technologies for Cloud Computing implementation between components. The following is a description of the procedure for delivering flexible service to each component:

Client: The End-User Service Portal's multifactor authentication enables users to access the client side (i.e., web browser or host-installed application) from a variety of devices, such as a PDA, laptop, or mobile ph

one, without requiring a second factor of authentication. User cloud access is made possible via a client-side application. Use of third-party certification provided by a Certification Authority to authenticate using several factors.

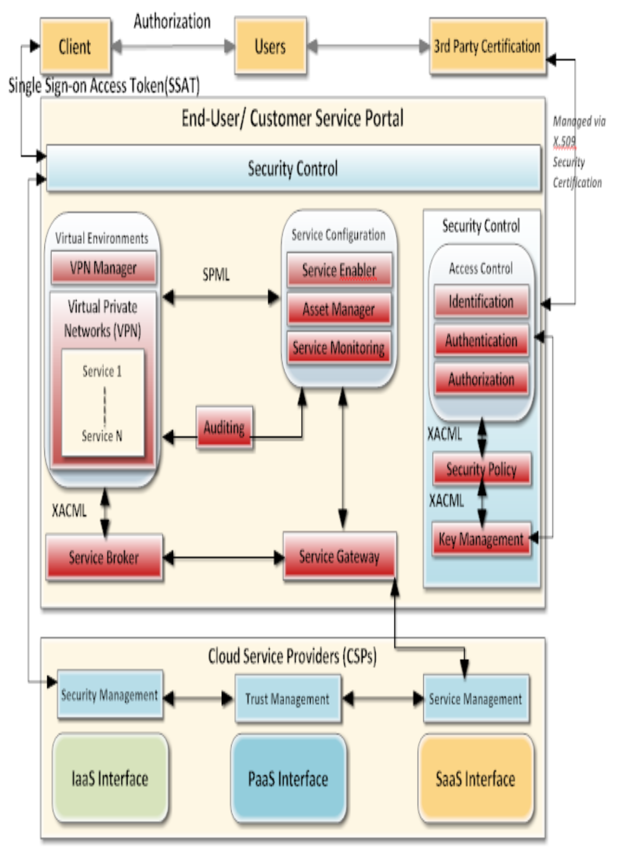


Fig 4: Secure Cloud Computing Framework

Singular Sign-on Access Tokens, in return for clearance, are available (SSAT). To share security policy and verification information with other portal components and cloud service providers, the access control component uses XACML and KIMP to connect with them. Regardless of service provider limits, the user has access to services.

A user's login and password may change depending on which service provider they are using. Single Sign-On (SSO): This leads to widespread usage of the same password throughout the network, creating new security risks. Inconvenient for users, multiple authentications lead to higher administrative expenses as a result. While Single Sign On (SSO) technology promises to decrease the number of network and application passwords, businesses are actively looking into using it [55]. This problem can be solved by implementing Single Sign-On for cloud users to make security administration easier while also implementing robust authentication in the cloud itself. This provides robust authentication at the user level while allowing users to connect into many cloud computing applications and services with a single login.

Configuration of the service: In response to the user input, the service enabler creates a personalized cloud service. In order to integrate and cooperate with the user's service provisioning requests, the cloud service provider's service management gets this user profile. The profile of a person may be shared using SPML [56]. The asset manager requests customized resources from the cloud service provider using the user's SPML profile, and then configures the service over a VPN on the cloud provider's end.

A service gateway maintains network resources, including virtual private networks, as part of a service broker's information lifecycle (VPNs). Protection from external threats is provided by the security component for all of these components. This module is in charge of meeting service providers' requirements for access control. There are several access control methods to choose from, each with its own set of benefits and drawbacks. Because of its simplicity, flexibility in capturing dynamic demands, and support for the idea of least privilege with efficient privilege management, most security professionals believe role-based access control to be the most promising solution [57]. Due to its ability to take in a wide variety of policy requirements, it is neutral in terms of policy and best suited for the previously mentioned need for policy integration. This may be used to govern the way resources are utilized by inserting requirements and conditions in authorizations. A need is defined as a precondition for obtaining anything else, such as access to the data. Conditions are non-topical, non-objective environmental requirements that must be fulfilled before access may be granted. It is important to consider responsibilities and conditions when implementing more stringent limits on cloud resource usage because of the cloud's fluid nature.

Policy Development and Enforcement: The policy development and enforcement function is the responsibility of the security management component. User and service credentials and characteristics are checked by the authentication and identity management module to make sure they are valid.

When working in the cloud, it may be challenging to integrate trust negotiation methods driven by needs with fine-grained access control mechanisms. For this reason, the trust level should be a service-oriented design feature of the cloud as well. The idea is that as a cloud service provider increases the range of services it offers, customers will have more faith in the company. Developing cloud bidirection trust is an extra hurdle to overcome. Clients must trust the service providers they choose, and suppliers must have faith in the clients to whom they release their service. A second alternative is to develop a trust management strategy that incorporates a wide range of trust negotiation criteria, is related to the service, and is bidirectional. Due to the cloud's intricate service composition dynamics, systems for trust and access control should contain delegation primitives. When it comes to previous research on access control delegation, researchers have concentrated on privilege delegation and different levels of control on privilege propagation and revocation. This is particularly true for role-based delegation.

Using effective cryptographic systems for delegation of trust presents major key management challenges owing to their inherent complexity [58].

Using automated techniques such as service monitoring, make sure that high standards of service performance and availability are always maintained. Users will have simple access to cloud services thanks to the suggested security architecture. We look at cloud orchestration setups to make sure users have a good experience. Tokens for a Single Sign-on. Besides that, we talk about potential cloud-based collaboration tools.

The SFCC is a real-time tool. The outcomes of the simulations match the actual world very well. These outcomes are in line with one another, at least in theory. It is everything done correctly this time. Real-time systems benefit from strong code consistency. In order to build the SFCC, the Eclipse integrated development environment is being used together with the CloudSim and iFogSim simulators. One of the most prominent cloud-based application simulators is CloudSim. Modeling of the cloud and managing events are responsibilities of this department.

Library resources may be put to many different uses. Common math, Json, and JFreeChart are all included into this program. The created simulation incorporates SFCC. Logic or concepts may be included into the simulation by anybody using the framework and getting the required outcomes. It allows the user to put the proposed strategy to the test in a variety of settings. A simulation makes it feasible to store and produce enormous amounts of data. Users may be able to better manage their networks and services if they can quantify things like encryption, description, power consumption, and network utilization.

Singular Sign-on Access Tokens, in return for clearance, are available (SSAT). To share security policy and verification information with other portal components and cloud service providers, the access control component uses XACML and KIMP to connect with them. Regardless of service provider limits, the user has access to services.

A user's login and password may change depending on which service provider they are using. Single Sign-On (SSO): This leads to widespread usage of the same password throughout the network, creating new security risks. Inconvenient for users, multiple authentications lead to higher administrative expenses as a result. While Single Sign On (SSO) technology promises to decrease the number of network and application passwords, businesses are actively looking into using it [55]. This problem can be solved by implementing Single Sign-On for cloud users to make security administration easier while also implementing robust authentication in the cloud itself. This provides robust authentication at the user level while allowing users to connect into many cloud computing applications and services with a single login.

Configuration of the service: In response to the user input, the service enabler creates a personalized cloud service. In order to integrate and cooperate with the user's service provisioning requests, the cloud service provider's service management gets this user profile. The profile of a person may be shared using SPML [56]. The asset manager requests customized resources from the cloud service provider using the user's SPML profile, and then configures the service over a VPN on the cloud provider's end.

A service gateway maintains network resources, including virtual private networks, as part of a service broker's information life cycle (VPNs). Protection from external threats is provided by the security component for all of these components. This module is in charge of meeting service providers' requirements for access control. There are several access control methods to choose from, each with its own set of benefits and drawbacks. Because of its simplicity, flexibility in capturing dynamic demands, and support for the idea of least privilege with efficient privilege management, most security professionals believe role-based access control to be the most promising solution [57]. Due to its ability to take in a wide variety of policy requirements, it is neutral in terms of policy and best suited for the previously mentioned need for policy integration. This may be used to govern the way resources are utilized by inserting requirements and conditions in authorizations. A need is defined as a precondition for obtaining anything else, such as access to the data. Conditions are non-topical, non-objective environmental requirements that must be fulfilled before access may be granted. It is important to consider responsibilities and conditions when implementing more stringent limits on cloud resource usage because of the cloud's fluid nature.

6.1 Components

Data protection encryption and decryption utilize the advanced encryption standard. Subsequent sections compare the method with previously reported unmodified algorithms. Tables 1–11 outline the various layers and devices. Components are the building blocks of a system. On-premise hardware is referred to as a "data center," whereas cloud computing is used to describe cloud computing as a whole. Your data is kept on a public cloud when you use the cloud, but in a data center, it is saved on your hardware. Table 1 depicts the data center's set-up.

Physical computers, virtual machines, and virtual storage are all available via an infrastructure as a service (IaaS) platform. Table 2 shows how infrastructure-as-a-service is set up. It is a business concept in which software applications are made available as a service to end customers (as a service). To see how software as a service is set up, look at

Table 3. In order to submit requests, a system called PaaS is used (platform as a service, or software as a service). As a consequence, complex applications may be designed and deployed as needed. Table 4 shows how the platform-as-a-service model is implemented in this scenario.

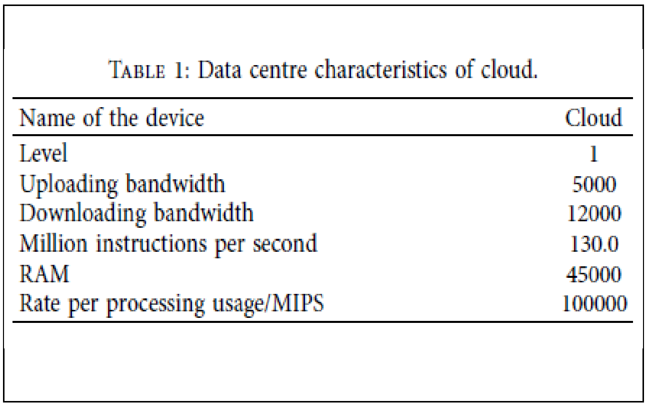


Table 1: Data centre characteristics of cloud.

Name of the device	Cloud
Level	1
Uploading bandwidth	5000
Downloading bandwidth	12000
Million instructions per second	130.0
RAM	45000
Rate per processing usage/MIPS	100000

The second-to-last rung of the hierarchy is comprised of gateway devices. Proxy servers and cloud-based devices interact with these gateway devices through the communication layer. The features of gateway devices are shown in the table below. Tables 6–8 demonstrate how to set up the gateway device.

Security management: the security management factor provides the security and privacy information as well as a table of implementation functions. Security and privacy details. Table 5 shows the setup for security management.

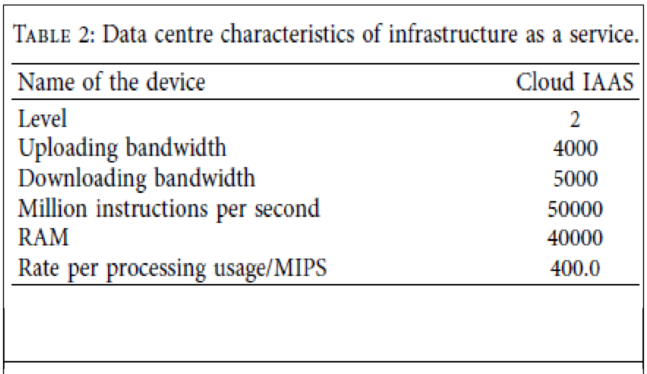


Table 2: Data centre characteristics of infrastructure as a service.

Name of the device	Cloud IAAS
Level	2
Uploading bandwidth	4000
Downloading bandwidth	5000
Million instructions per second	50000
RAM	40000
Rate per processing usage/MIPS	400.0

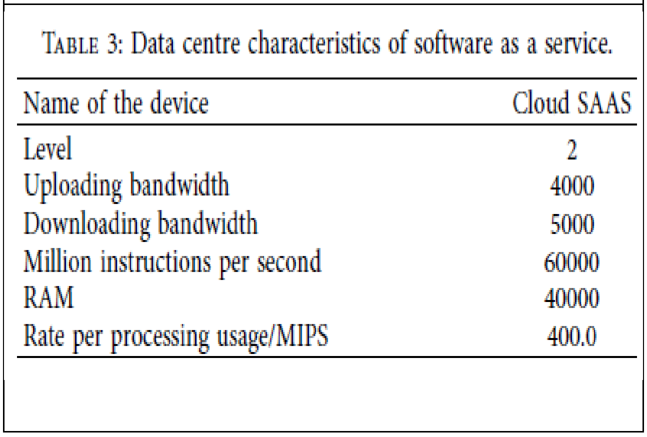


Table 3: Data centre characteristics of software as a service.

Name of the device	Cloud SAAS
Level	2
Uploading bandwidth	4000
Downloading bandwidth	5000
Million instructions per second	60000
RAM	40000
Rate per processing usage/MIPS	400.0

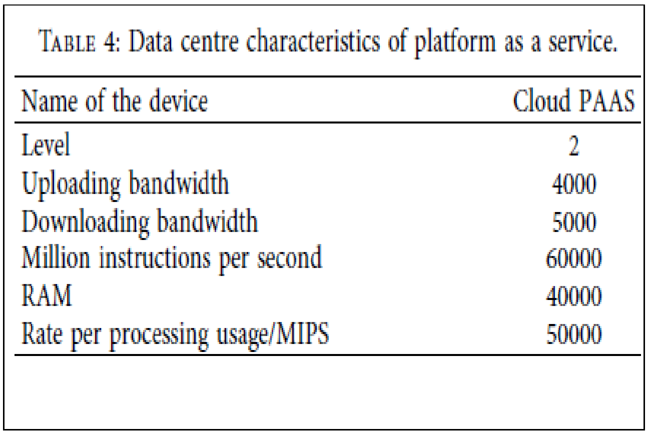


Table 4: Data centre characteristics of platform as a service.

Name of the device	Cloud PAAS
Level	2
Uploading bandwidth	4000
Downloading bandwidth	5000
Million instructions per second	60000
RAM	40000
Rate per processing usage/MIPS	50000

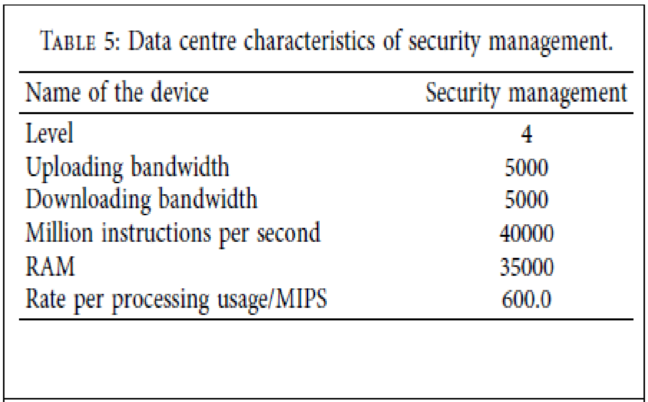


Table 5: Data centre characteristics of security management.

Name of the device	Security management
Level	4
Uploading bandwidth	5000
Downloading bandwidth	5000
Million instructions per second	40000
RAM	35000
Rate per processing usage/MIPS	600.0

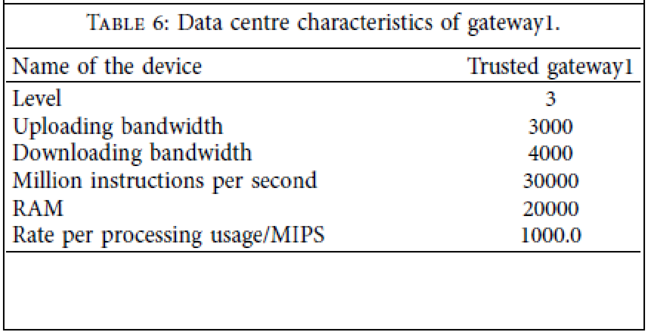


Table 6: Data centre characteristics of gateway1.

Name of the device	Trusted gateway1
Level	3
Uploading bandwidth	3000
Downloading bandwidth	4000
Million instructions per second	30000
RAM	20000
Rate per processing usage/MIPS	1000.0

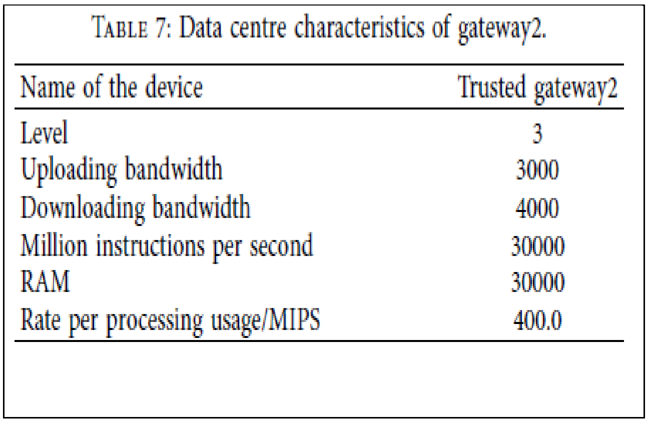


Table 7: Data centre characteristics of gateway2.

Name of the device	Trusted gateway2
Level	3
Uploading bandwidth	3000
Downloading bandwidth	4000
Million instructions per second	30000
RAM	30000
Rate per processing usage/MIPS	400.0

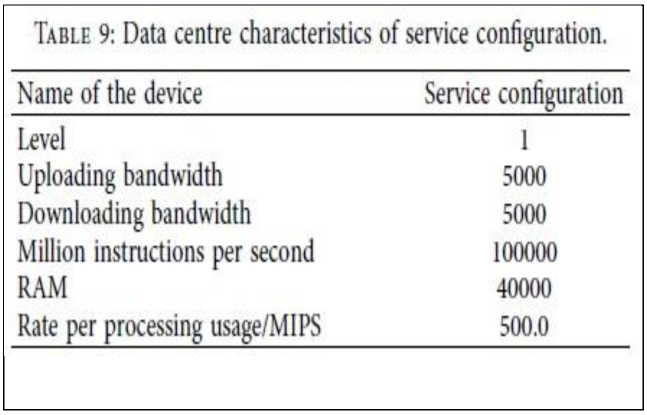


Table 9: Data centre characteristics of service configuration.

Name of the device	Service configuration
Level	1
Uploading bandwidth	5000
Downloading bandwidth	5000
Million instructions per second	100000
RAM	40000
Rate per processing usage/MIPS	500.0

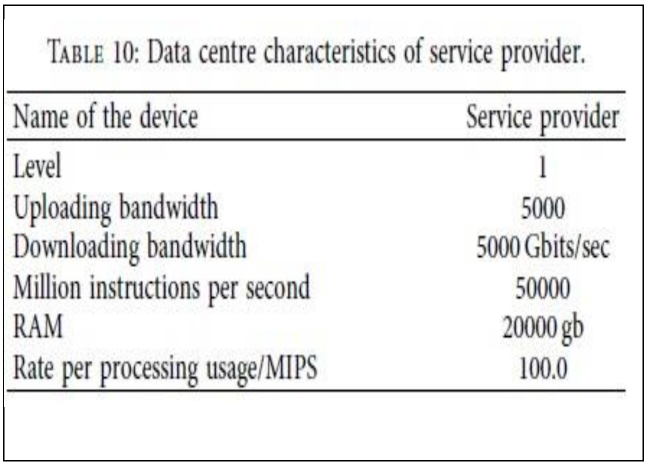


Table 10: Data centre characteristics of service provider.

Name of the device	Service provider
Level	1
Uploading bandwidth	5000
Downloading bandwidth	5000 Gbits/sec
Million instructions per second	50000
RAM	20000 gb
Rate per processing usage/MIPS	100.0

Assigning virtual machines to hosts allows the processing and unloading of modules to be more efficient, which helps the load balancing mechanism.

Strong encryption is used in these virtual machines to provide the security and trust features. Table 11 depicts the virtual computer's settings. In order to ensure that all operations are reproducible, the materials and techniques section should provide sufficient information to enable this. If there are a lot of steps to follow, they may be broken down into subsections using headings.

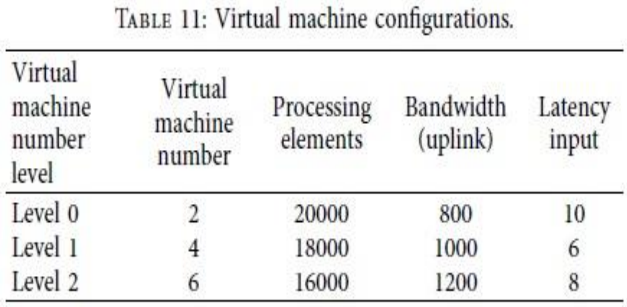


Table 11: Virtual machine configurations.

Virtual machine number level	Virtual machine number	Processing elements	Bandwidth (uplink)	Latency input
Level 0	2	20000	800	10
Level 1	4	18000	1000	6
Level 2	6	16000	1200	8

The Physical Topology of the SFCC shows how the network's nodes and devices are organized. The construction of physical objects and the definition of their properties such as competency, capacity, and settings. Some examples of these cloud-based devices include sensors and actuators (virtual machines). All of these things and settings are connected in some way as well. It is necessary to understand the topology of physical networks in order to comprehend how networks are set out, how various network devices are arranged, and how they connect with one another. It is possible to achieve the greatest load and data transmission rate possible on a network by using these network designs and capabilities. Figure 5 shows the topology in terms of physical properties.

When it comes to cloud computing, the top-down approach is always used. To manage the lower-level architecture, the cloud must stay at the very top of the pyramid [59]. CSPs [38] may be categorized based on their function as one of three different cloud kinds that lie underneath the surface. The virtual machine allocation policy method is utilized in the third layer of the proposed system to enable data offloading and privacy for security [60]. In addition to enhancing load balancing, offloading modules also adds an additional layer of protection to the hosts, addressing concerns about the cloud's security. Module processing and offloading are made easier by creating and assigning virtual machines to hosts, which helps with the load balancing mechanism. In order for the security and trust functions to work, these virtual machines have a strong encryption method installed. As with a host H, a virtual machine needs some storage and processing power. Prerequisites for setting up a virtual computer are listed. When running several virtual machines, the Vm size must be less than the total amount of host H and storage S available.

VMs may be generated under a variety of circumstances. Fourth-layer implementation includes trusted gateways. A trustworthy source must be connected to a legitimate Internet protocol address for these gateways to acquire encrypted data and decode it. These gateways are designed to solve issues with trust [61]. All three portals have alternative paths, with the second one being a shortcut. Other safe gateways will be found to guarantee data transmission in the case of an attack or misuse of a conventional gateway, as shown in Figure 3.

To preserve trusted users' privacy and security, reliable gateways move those on the blacklist to a separate category called prohibited users. Three tasks will be assigned to the fifth layer, which will be accountable for all of them. Also In contrast to direct and disparity cryptanalysis, each current encryption method needs a nonlinear revolution and has been shown to be a solid cryptographic original.

included are features such as service monitoring and load balancing. The bottom-most cloud user layer represents the Internet-of-Thing layer in the proposed system. This is how each of the frameworks listed above works. There will be no change in the status of the trusted customer as long as there is a mediator (trustee). A middleman is not necessary as long as the cloud service providers are dependable. The trust chain is shown graphically in Figure 6.

In this comparison, we will examine the cloud computing confidentiality paradigm in more depth vs traditional AES algorithm modifications. Data integrity mechanisms are utilized in this framework to increase the security of the data by employing cryptographic techniques such as modified AES ciphers that can encrypt 128-bit data blocks in 1000 cycles with little power, time, and network delay. Frameworks are in charge of things like load balancing, trust management, and effective resource management.

Strict encryption and decryption requirements necessitated symmetric identification, in which the same key was used for both operations. It differs from earlier versions of AES in that we use the double round key functionality to encrypt 1000 blocks per second. When it was first created, AES used a square key and ran at a speed of 800 blocks per second (BPS). One of the most significant benefits of employing symmetric keys is that a vast amount of data may be securely kept without worry of being exploited, which is a significant advantage.

AES Substitution Box, Section 4.5 (S-Box). A lookup table known as a substitution box, or simply an S-box, is used to arrange a byte-by-byte replacement to get around. In 16 16 arrays, the S-Boxes perform one-to-one graphing for all byte values ranging from 0 to 255. Bit misunderstanding occurs when bits are replaced in a nonlinear conversion.

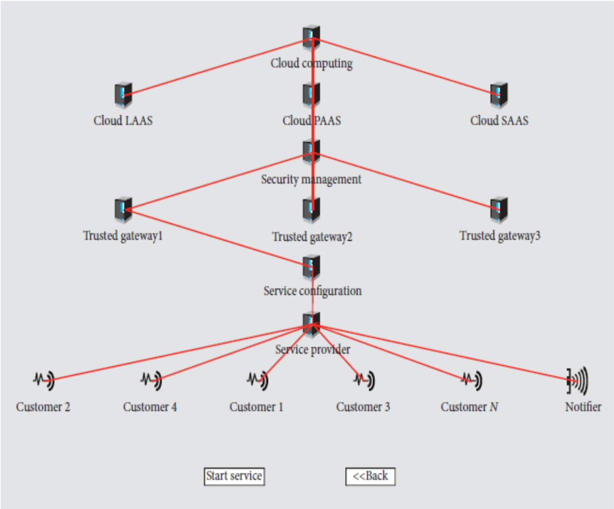


Fig 5: Topology of Physical Network

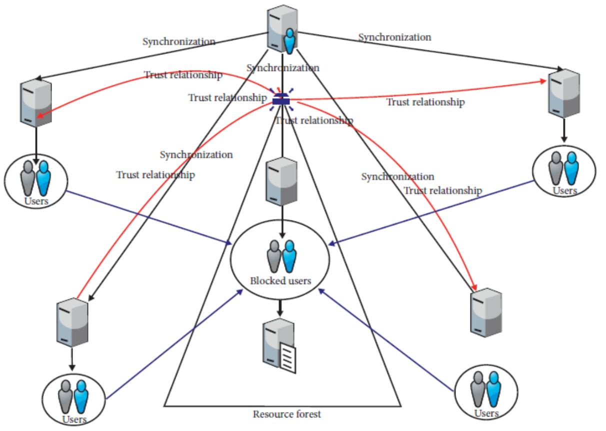


Fig 6: Chain of Trusted Gateways

In contrast to direct and disparity cryptanalysis, each current encryption method needs a nonlinear revolution and has been shown to be a solid cryptographic original.

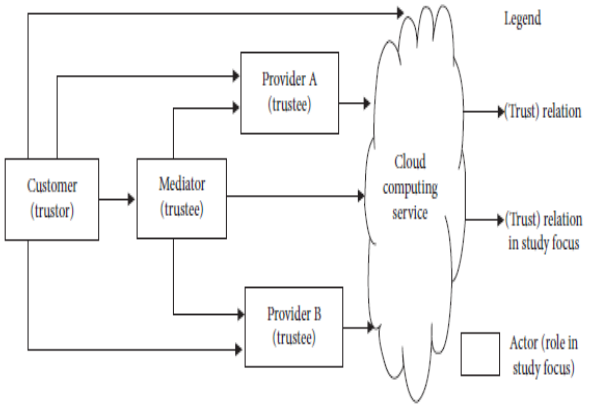


Fig 7: Cloud Service Provider Trusted Chain Mediator

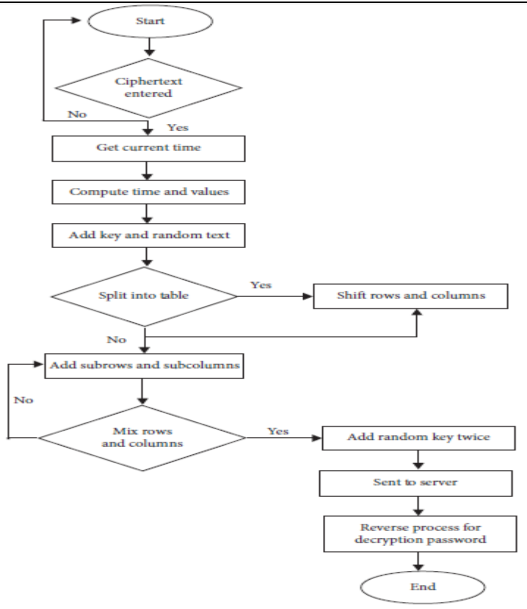
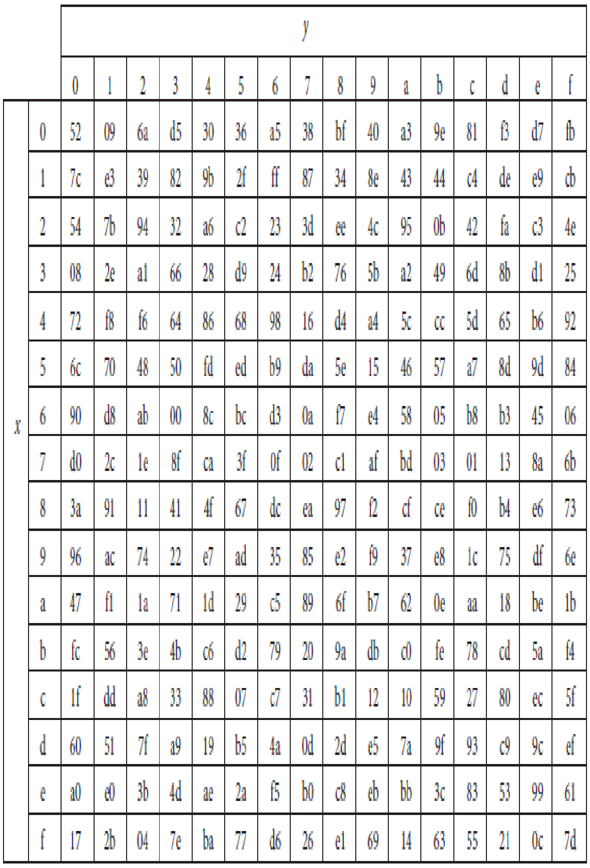


Fig 8: Flowchart of Proposed Work

The S-box is shown graphically in Figure 9. The hexadecimal character [62] is used to represent all values. Figure 6 shows the round key substitution general substitution box.



		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Fig 9: Substitution Box

6. Proposed Algorithm

The preceding section emphasized the importance of developing a new algorithm for cloud data security. This section details the proposed algorithm's steps. The technique is meant to operate on plaintext and encrypted text with a combined length of 1024 bits. To increase data security, the algorithm is controlled by a 1024-bit key. Decryption is equal to encryption.

The algorithm's first phase is key generation. The technique will generate a 1024-bit random key. Following that, it will be separated into 128-bit blocks. These eight blocks will be utilized to initiate the generation of additional keys. The following keys were produced using a random kay AES (RK-AES) sequence [63].

Encryption:

Stage 1: A 1024-bit plaintext is obtained in the first step.

Phase 2: In the second step, the 1024-bit plaintext is separated into eight 128-bit sub-blocks.

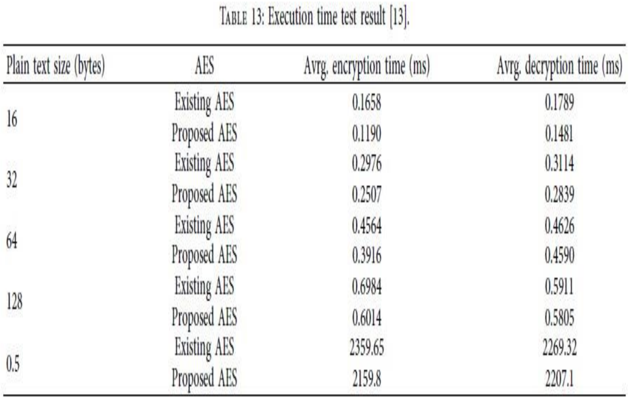
Phase 3: In the third step, each 128-bit sub-block is added to a key block created using the Random kay AES (RK-AES) procedure.

Step 4: Using a replacement table, each bit will be replaced with another bit in the fourth step.

Step 5: The fourth step's output will be organized in two-dimensional matrices.

Step 6: In the sixth step, a mirror image of the matrices organized in the fifth step will be created.

Table 13: Execution time test result [13].



Plain text size (bytes)	AES	Avrg. encryption time (ms)	Avrg. decryption time (ms)
16	Existing AES	0.1658	0.1789
	Proposed AES	0.1190	0.1481
32	Existing AES	0.2976	0.3114
	Proposed AES	0.2507	0.2839
64	Existing AES	0.4564	0.4626
	Proposed AES	0.3916	0.4590
128	Existing AES	0.6984	0.5911
	Proposed AES	0.6014	0.5805
0.5	Existing AES	2359.65	2269.32
	Proposed AES	2159.8	2207.1

Step 7: N times, each bit will be relocated to the right. This N can be computed using the formula N=(number of steps) mod (size of block)

Step 8: Using the formula starting key/previous step-key, a step-key will be generated in the eighth step.

Step 9: The step-key will be appended to the previous step's output.

Iteration will be the tenth phase. Ten repetitions should be required to obtain encrypted text.

7.1 Implementation of proposed algorithm:

A cloud-based environment is created for the purpose of implementing the proposed algorithm. The method must be validated in a real-world cloud setting before it can be used by cloud users. The cloud environment was configured as follows.

160 GB SSD 8 GB RAM

4vCPU Processor (Intel Xeon Processor)

Digital Ocean [64] provides this configuration as a droplet. The proposed approach was implemented using angular js, mysql, and java after configuring the environment. The file and keys are encrypted and stored in a mysql database. Apart from the proposed algorithm, the same infrastructure supports RSA, AES, and Blowfish. Thus, a comparison can be made.

7. Result and Discussion

The effectiveness of the proposed technique is confirmed and validated using a simple piece of code. With the help of this test, we were able to demonstrate that the suggested AES algorithm is better than any previous AES algorithm and that execution time would be reduced after the deployment of AES and upgraded AES code on hardware. In this case, both the acquisition of the SFCC results and the deployment of the cloud computing security architecture were successful. During the peer-to-peer key generation, encryption, and decryption procedures, the time is used as a dynamic character. The work framework continues to get a high volume of enquiries about Intel(R) Core(TM)-i3 processors and 4GB RAM when running the CloudSim and iFogSim simulators on Eclipse's integrated development environment (IDE). CloudSim is one of the most well-known cloud-based application simulators available.

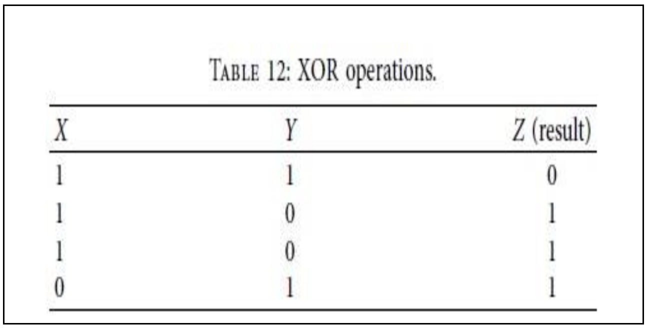


TABLE 12: XOR operations.

X	Y	Z (result)
1	1	0
1	0	1
1	0	1
0	1	1

number of variables are compared, such as encryption, decryption and energy usage. Other variables include network use and latency. In real-time applications, the same methods are employed to deal with the aforementioned problems. The outcomes of the simulations match the actual world very well. Real-time systems benefit from strong code consistency.

Simulators are modified to suit the application's needs. As part of a quick and approachable system, it is expected that both the implementation period, which refers to the time required to convert a plain text into an encryption manuscript and back again, as well as the decryption period, which refers to the time required to convert a cipher text into a plain text, will be brief; this is because a quick and approachable system will be quick and approachable. The execution time is also influenced by the system's design. There are four different key sizes used to determine the execution time: 16, 32, 64, and 128 bytes. This results in a milliseconds (ms) execution time.

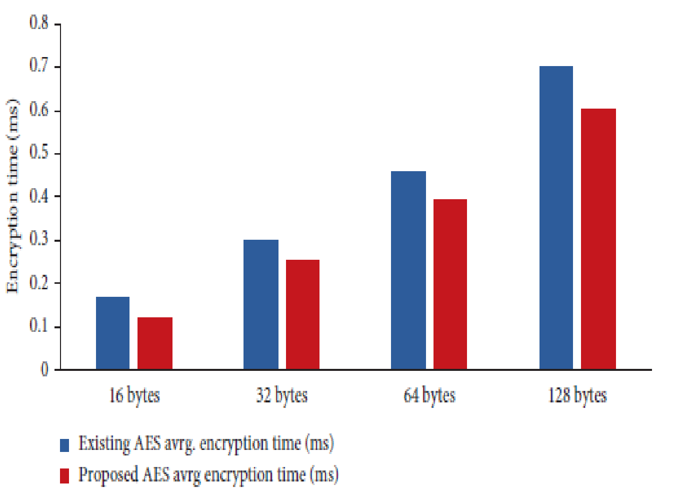


Fig 10: Encrypting time: proposed vs. AES existing AES

The results in milliseconds are produced by calculating the average time for encryption and decryption after the input text has been encrypted and decrypted in 0.5MB chunks using the same key and after the input text has been encrypted and decrypted in 0.5MB chunks using the same key.

FIGURES 10–13 demonstrate that the prior AES technique has a little increase in encrypting and decrypting time when compared to the current AES approach. FIGURE 10–13: Table 13 examines the performance of numerous existing AES algorithms as well as several novel AES ideas based on a string key.

Avalanche Effect: In cryptography, a concept called dispersal is used to replicate an algorithm's cryptographic asset. A little change in the input results in a large change in the outcome. The flooding effect is the technical term for this. The effects of an avalanche are managed slowly by feigning reserve. Material philosophy's hammering reserve is the amount of variance. Bit-by-bit XOR using ASCII is used in the informal growth of programmable design. To put it another way, we are bracing ourselves for a major avalanche impact. With Avalanche is completion, the cryptographic technique is brought full circle. Table 14 provides comprehensive information on the avalanche impact. Avalanche phenomenon is seen in Figure 13. (simulation results from Table 14)

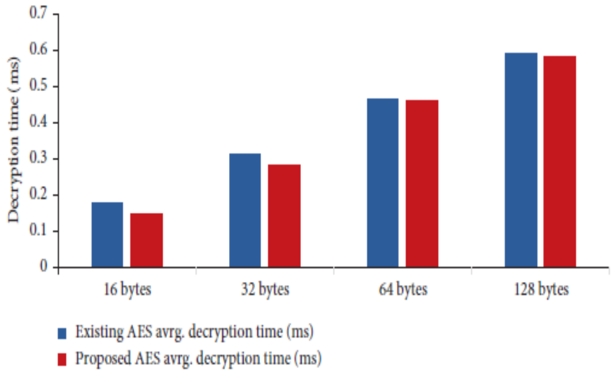


Fig 11: Decrypting time: proposed AES vs. existing AES

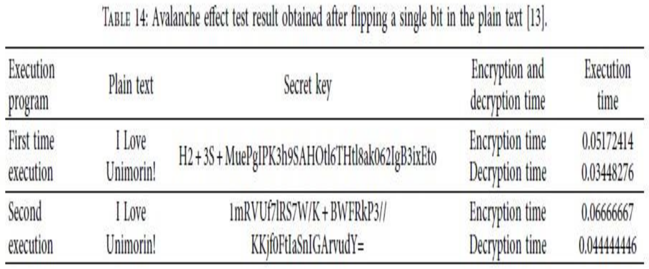


Table 14: Avalanche effect test result obtained after flipping a single bit in the plain text [13].

Execution program	Plain text	Secret key	Encryption and decryption time	Execution time
First time execution	I Love Unimorin!	H2 + 3S + MuePgIPK3h9SAHOtl6THtl8ak062IgB3ixEto	Encryption time Decryption time	0.05172414 0.03448276
Second execution	I Love Unimorin!	1mRVUf7lRS7W/K + BWFRkP3// KKjf0FtIaSnIGArvudY=	Encryption time Decryption time	0.06666667 0.04444446

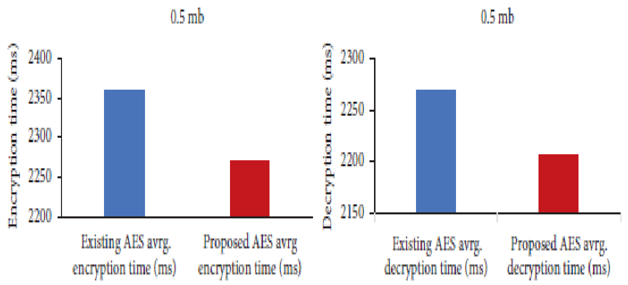


Figure 12: Encrypting and decrypting time: proposed AES vs. existing AES

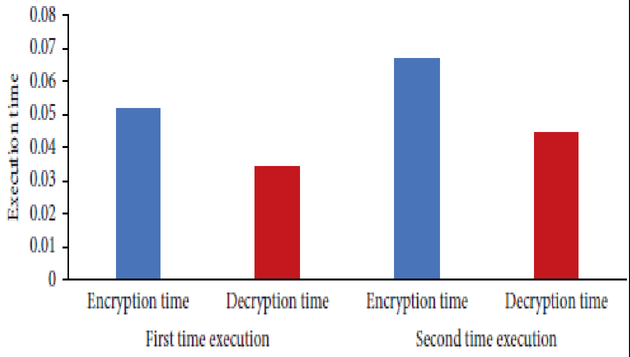


Fig 13: Avalanche effect test result

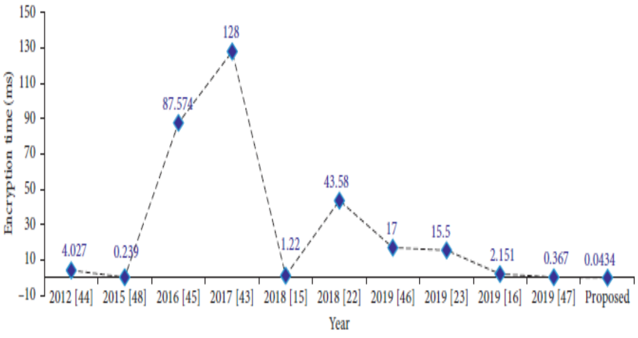


Fig 14: Time factor for encryption processing in various AES.

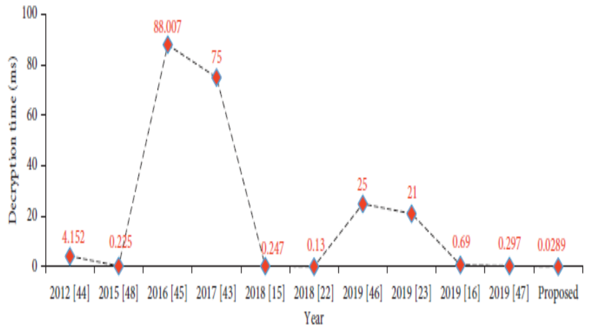


Fig 15: Time factor for decryption processing in various AES

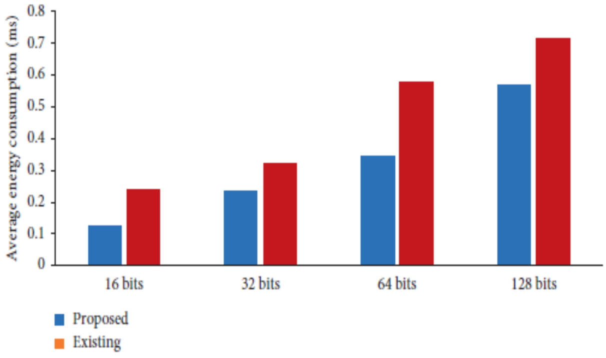


Fig 16: Energy usage for various key AES encrypting and decrypting algorithms

8.1 The Average Networking Delay

The delay is included in the cost of testing and determining whether or not the data is safe. In a local host cloud scenario with a large number of clients, data traffic would rapidly grow, impacting the scheme. Real-world factors such as key size and network speed might result in delays, suspensions, and congestion. The more keys you have, the longer it will take to encrypt your data, and hence the greater the delays will be. Before encryption, the key is produced and then divided into blocks. There is a possibility that the scope of one block will affect the total scope. When comparing the latency of the proposed framework to that of the previous technique [13], it is 15% faster. Bits B must travel for a specific latency L from an end device to a processing device before the delay D is reflected, and the observed delay T is determined using the formula.

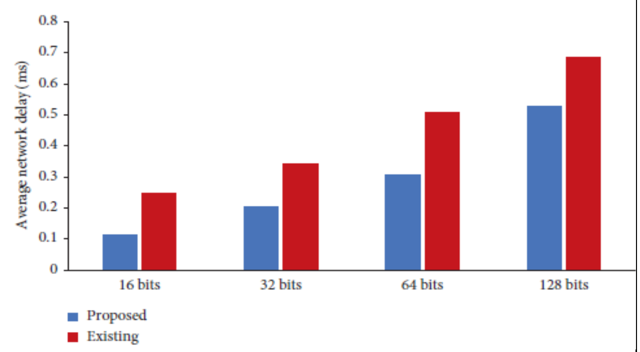


Fig 17: Delay in network for various key AES encrypting and decrypting

The delay is expressed mathematically in the next section, and the simulation result is shown in the picture. The delay calculation is shown in Figure 17.

To evaluate the algorithms, six alternative file formats were used. Each file format has a different file size, making it possible to evaluate each technique using a different set of parameters. Table 15 contains a list of the documents and the related data.

Table 15: File Format and File Size

S. No.	File Type	File Size
1.	JPG image file	0.1 MB
2.	PDF Document	5 MB
3	MP3 file	10 MB
4.	Text file	0.05 MB
5.	MP4 file	15 MB
6.	MS Word file	2 MB

The approach was assessed based on five different variables. Each of the five factors has an impact on the other two: encryption time, file size after decryption, the avalanche effect, and entropy. 0.05 MB, 0.1 MB, 2, 5-, 5-, 10- and 15-megabyte files were utilized in the technique evaluation. This flowchart compares the proposed encryption algorithm (prop. encry.) against the existing one. It was decided to compare the RSA, AES, and blowfish algorithms since they had all undergone extensive testing for encryption.

Figure 18 shows how long it takes to encrypt files of different sizes using this method. The proposed method beats RSA, AES, and Blowfish in terms of speed, as shown. In addition, as the file size grows, so does the encryption time.

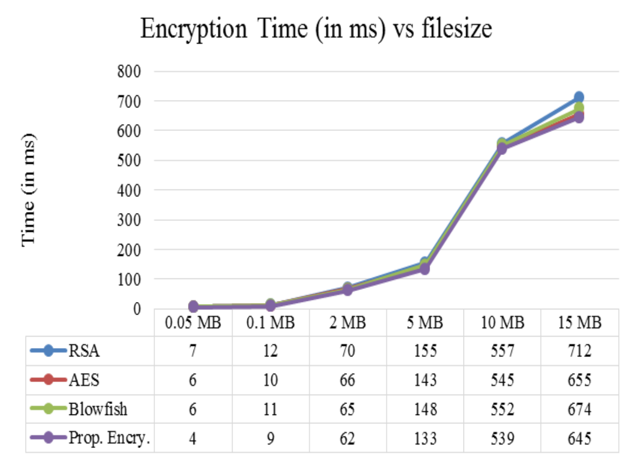


Fig 18: Comparison of encryption times for various file sizes

The time it takes to decode files of different sizes is shown in Figure 20. The decryption process made use of the same file that was encrypted using the method. As shown, the proposed encryption method decrypts data more quickly than RSA, AES, and Blowfish. In addition, as the file size grows, so does the decryption time.

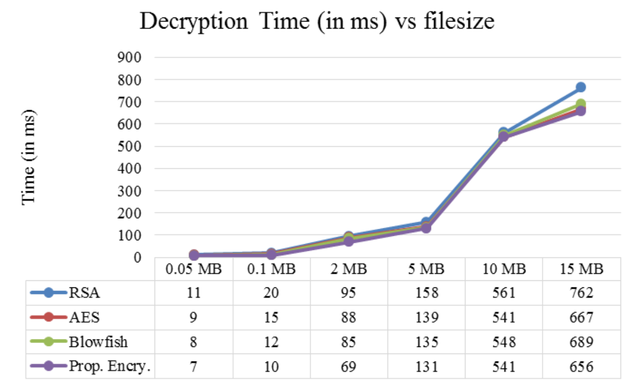


Fig 19: Comparison of decryption times for various file sizes

The file size after encryption is shown in Figure 20 for a variety of file formats. **The** exact same file was used in the comparison. As you can see, the decrypted files produced by each method are about the same size. In contrast to RSA, AES, and Blowfish, the proposed method produces smaller files than those of those three algorithms. The lower file size is helpful for storing more files since it allows for more space to be used. More decrypted data may be stored with less cloud storage capacity.

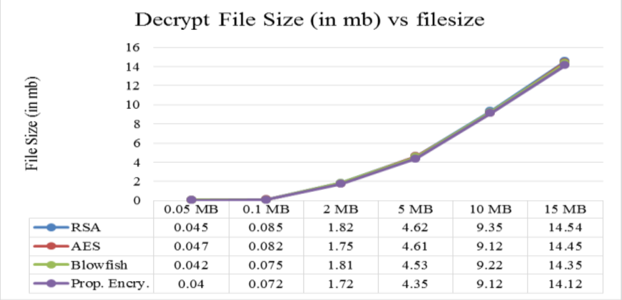


Fig 20: Comparison of decrypt file size for different file size

Figure 21 explains how to calculate the algorithm's entropy. The entropy measures how random the data is. Each key piece of information reveals a link between the various pieces of information. For effective encryption techniques, you will want a lot of entropy. To compare, the suggested encryption algorithm's entropy is better than that of both AES as well as Blowfish.

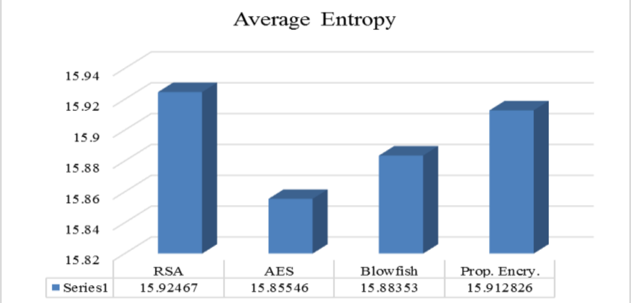


Fig 21: Comparison of average entropy for algorithms

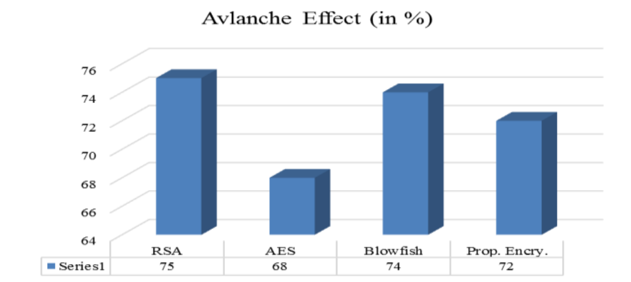


Fig 22: Comparison of avalanche effect for algorithm

Figure 22 depicts the avalanche effect. Small changes in the input data have huge effects on the output, as described by the avalanche effect. AES and Blowfish's avalanche effects are shown in Figure 5, where the suggested encryption algorithms avalanche impact is shown to be superior than AES. In comparison to other algorithms, that of RSA's avalanche has a higher security level.

8. Conclusion and Future Work

The cloud computing environment has a strong security architecture in place to protect user data and keep communications secure while also preventing unauthorized access. Cloud customers might feel more secure about controlling their data in the cloud if they adopt this privacy and integrity management approach. There is no need to worry about whether or not the cloud service is reliable while using cloud storage and networking. Only those who have verified and validated their identity may access cloud data secured using the AES technique. Actual delays are a result of several variables that are not taken into account in our simulation. Utilization of the network is decreased by 11.53%, as is latency, which is lowered by 15.67% using this framework. This design improves security while also making the most of resources while also speeding up the development of a computational cloud service.

Users are concerned about the safety and security of their cloud storage data. A lot of people are still getting their heads around cloud computing and do not know how to keep their data safe while using it. Current security algorithms and methods are discussed in this article. An encryption method for cloud-stored documents is presented in this article. The debate shows that the suggested method for encrypting data is safer. Furthermore, the findings show that the proposed method encrypts and decrypts data quicker than RSA, AES, and Blowfish. Measurements of avalanche effect and entropy show that the proposed computation generates cipher text that is comparable to industry standards. Because it is very tough to crack now, the suggested encryption technique has a lot of appeal. Additionally, when file size grows, the proposed method will become increasingly advantageous based on the trend of encryption time. However, executing code consistently leads in capacity and registration costs, which are negligible in exchange for better execution. It is still possible to undertake research on future key development and attack strategies, such as key expansion and key management.

Although cloud computing has grown quickly in recent years, security issues have emerged as a roadblock to its broad acceptance, which must be overcome if cloud computing is to become more widely used. For this research, we will review existing literature on cloud computing security issues and propose a security model and framework for a safe cloud computing environment that emphasizes security needs, as well as assaults and risks associated with cloud deployment. Security in the Cloud Computing environment, however, requires more than simply technology; it also includes standards, monitoring mode, rules and regulations, and a number of other elements as well. As the security problem is gradually addressed, cloud computing will increase and so will its applications. But we think future study should concentrate on cloud computing's risk management. Businesses can make an educated decision about whether cloud computing can help them achieve their business goals while presenting an acceptable level of risk, thanks to risk assessment. It is a challenging procedure to manage risk in cloud computing since it involves evaluating risks and making attempts to reduce them in addition to identifying them. For cloud computing, we plan to look at qualitative and quantitative methods to risk assessment.

References

[1] G.S. Mahmood, J. H. Dong, and B. A. rahman Jaleel, "Achieving an effective, confidentiality and integrity of data in cloud computing," *International Journal of Network Security*, vol. 21, no. 2, pp. 326–332, 2019.

[2] S. Othman and A. S. Riaz, "A user-based trust model for cloud computing environment," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, 2018.

[3] Firman, A. N. Hidayanto, and P. Harjanto, "Critical components of security framework for cloud computing community: a systematic literature review," *International Journal of Pure and Applied Mathematics*, vol. 118, no. 18, pp. 3345–3358, 2018.

[4] K. V. Pradeep, V. Vijayakumar, and V. Subramaniyaswamy, "An efficient framework for sharing a file in a secure manner using asymmetric key distribution management in cloud environment," *Journal of Computer Networks and Communications*, vol. 2019, Article ID 9852472, 8 pages, 2019.

[5] Dr. Ramalingam Sugumar and K. Arul Marie Joycee, "FEDSACE: a framework for enhanced user data security algorithms in cloud computing environment," *International Journal on Future Revolution in Computer Science & Communication Engineering*, vol. 4, no. 3, 2018.

[6] M. Kpelou and K. Kishore, "Lightweight security framework for data outsourcing and storage in mobile cloud computing," *International Journal of Recent Technology and Engineering*, vol. 8, no. 2, 2019.

[7] R. Ganga Sagar and N. Ashok Kumar, "Encryption based framework for cloud databases using AES algorithm," *International Journal of Research Studies in Computer Science and Engineering*, vol. 2, no. 6, 2015.

[8] J. R. Jain and A. Abu, "A novel data logging framework to enhance security of cloud computing," in *Proceedings of the SoutheastCon 2016*, IEEE, Norfolk, VA, USA, April 2016.

[9] J. Singh, "Framework for client side AES encryption technique in cloud computing," *IJIRMPS*, vol. 6, no. 5, 2018.

[10] J. Y. Gudapati Syam Prasad, S. sunil kumar, and A. Keerthi, "Integration of searching and AES encryption in cloud computing," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 8, no. 4, 2019.

[11] A. Elgendy, W.-Z. Zhang, C.-y. Liu, and C.-H. hsu, "An efficient and secured framework for mobile cloud computing," *IEEE Transactions on Cloud Computing*, 2018.

[12] R. Saha, G. Geetha, G. Kumar, and T.-h. Kim, "RK-AES: an improved version of AES using a new key generation process with random keys," *Security and Communication Networks*,

[13] vol. 2018, Article ID 9802475, 11 pages, 2018.

[14] O. C. Abikoye, A. D. Haruna, A. Abubakar, N. O. Akande, and E. O. Asani, "Modified advanced encryption standard algorithm for information security," *Symmetry*, vol. 11, no. 12, p. 1484, 2019.

[15] K.-L. Tsai, Y.-L. Huang, F.-Y. Leu, I. You, Y.-L. Huang, and C.-H. Tsai, "AES-128 based secure low power communication for LoRaWAN IoT environments," *IEEE Access*, vol. 6, pp. 45325–45334, 2018.

[16] M.V. C. Suana, A. M. Sison, C. Aragon, and R. P. Medina, "Enhancement of advanced encryption standard (AES) cryptographic strength via generation of cipher key-dependent S-box," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 6, no. 4, 2018.

[17] S. NurRachmat, "Performance analysis of 256-bit AES encryption algorithm on android smart phone," *IOP Conf. Series: Journal of Physics: Conf. Series*, vol. 1196, 2019.

[18] On technical security issues in cloud computing, Meiko Jensen etal, 2009

[19] Cloud computing security issues and challenges, Balachandran reddy et al, 2009

[20] Cloud Computing security issues and challenges Kresimir Popovic, et al, 2010

[21] Dikaiakos, M.D., Katsaros, D., Mehra, P., et al.: Cloud Computing: Distributed Internet Computing

[22] for IT and Scientific Research 13, 10–13 (2009)

[23] Amazon Web Services. Amazon Virtual private Cloud, http://aws.amazon.com/vpc/

[24] C. Băsescu, A. Carpen-Amarie, C.Leordeanu, A. Costan, and G. Antoniu, "Managing Data Access on

[25] Clouds: A Generic Framework for Enforcing Security Policies", In proceeding of IEEE International

[26] Conference on Advanced Information Networking and Applications (AINA), 2011

[27] R. Sravan Kumar and A. Saxena, "Data integrity proofs in cloud storage", Third International Conference on

Communication Systems and Networks (COMSNETS), 2011.

[28] Z. Wang, “Security and Privacy Issues Within Cloud Computing” IEEE Int. conference on

[29] computational and Finformation sciences, Chengdu, China, Oct. 2011.

[30] James B.D. Joshi, Elisa Bertino, Usman Latif, Arif Ghafoor, “A Generalized Temporal Role-Based Access Control Model”,IEEE Computer Society, 2005.

[31] Moonam Ko, Gail-joon Ahn, Mohamed Shehab, “Privacy enhanced User-Centric Identity Management”, IEEE International Conference on Communications,2009.

[32] Cong Wang, Qian Wang, Kui Ren, Wenjing Luo, “Privacy preserving public audting for data storage security in Cloud Computing”, IEEE Communication Society, 2010.

[33] Tripathi and A. Mishra, “Cloud computing security considerations” IEEE Int. conference on signal processing, communication and computing (ICSPCC), 14-16 Sept., Xi'an, Shaanxi, China, 2011.

[34] Vadym Mukhin, Artem Volokyta, “Security Risk Analysis for Cloud Computing Systems” The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Prague, Czech Republic, 15-17 September 2011.

[35] Mathisen, “Security Challenges and Solutions in Cloud Computing” 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST2011) , Daejeon, Korea, 31 May -3 June 2011.

[36] M. Oqail Ahmad and R. Z. Khan, “Cloud computing modelling and simulation using CloudSim environment,” *International Journal of Recent Technology and Engineering (IJRTE) ISSN*, vol. 8, no. 2, 2019.

[37] V. Surya, S. Ranichandra, and R. Ranjani, “Secure cloud storage using AES encryption,” *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 6, no. 6, 2018.

[38] Nair and S. S. SantoshAnand, “A performance booster for load balancing in cloud computing with my load balancer technique,” *International Journal of Recent Technology and Engineering*, vol. 8, no. 1, 2019.

[39] D. Salama and A. Elminaam, “Improving the security of cloud computing by building new hybrid cryptography algorithms,” *IJEIE*, vol. 8, no. 1, pp. 40–42, 2018.

[40] D.-H. Bui, D. Puschini, S. Bacles-Min, E. Beign´e, and X.-T. Tran, “Ultra low-power and low-energy 32-bit datapath AES architecture for IoT applications,” in *Proceedings of the 2016 International Conference on IC Design and Technology (ICICDT)*, pp. 1–4, Ho Chi Minh City, Vietnam, June 2016.

[41] H. Jia, X. Liu, X. Di et al., “Security strategy for virtual machine allocation in cloud computing,” *Procedia Computer Science*, vol. 147, pp. 140–144, 2019.

[42] B. T. Spiers, M. Halas, R. A. Schimmel, and D. P. Provencher, “Secure network cloud architecture,” U.S. Patent 8,984,610, United States Patent (Justia Patents), 2015.

[43] E. Bertino, F. Paci, R. Ferrini, and N. Shang, “Privacy-preserving digital identity management for cloud computing,” *IEEE Data Engineering Bulletin*, vol. 32, no. 1, pp. 21–27, 2009.

[44] S. Yi, Li Cheng, and Q. Li, “A survey of fog computing: concepts, applications and issues,” in *Proceedings of the 2015 Workshop on Mobile Big Data*, pp. 37–42, ACM, Hangzhou, China, June 2015.

[45] M. Aazam and E.-N. Huh, “Fog computing and smart gateway based communication for cloud of things,” in *Proceedings of the 2014 International Conference on Future Internet of Bings and Cloud*, pp. 464–470, IEEE, Barcelona, Spain, August 2014.

[46] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. De Rose, and R. &Buyya, “CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms,” *Software: Practice and Experience*, vol. 41, no. 1, pp. 23–50, 2011.

[47] G. N. Selimis, A. P. Kakarountas, A. P. Fournaris, A. Milidonis, and O. Koufopavlou, “A low power design for sbox cryptographic primitive of advanced encryption standard for mobile end-users,” *Journal of Low Power Electronics*, vol. 3, no. 3, pp. 327–336, 2007.

[48] M. A. FaiqaMaqsood, M. M. Ali, and M. Ali Shah, “Cryptography: a comparative analysis for modern techniques”, (IJACSA),” *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, 2017.

[49] R. Paul, S. Saha, S. Sau, and A. Chakrabarti, “Design and implementation of realtime AES-128 on real time operating system for multiple fpga communication,” 2012, http://arxiv.org/abs/1205.2153.

[50] D. Lohit Kumar, Dr.A. R. Reddy, and S. A. K. Jilani, “Implementation of 128-bit AES algorithm in

MATLAB," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 33, no. 3, 2016.

[51] Dr. N. Suba Rani, Dr. A. Noble Mary Juliet, and K. Renuka Devi, "An image encryption & decryption and comparison with text - AES algorithm," *International Journal of Scientific & Technology Research*, vol. 8, no. 7, 2019.

[52] O. I. Omotosho, "A review on cloud computing security," *International Journal of Computer Science and Mobile Computing, IJCSMC*, vol. 8, no. 9, pp. 245–257, 2019.

[53] L. R.1 and H. S.2 Mohan, "Implementation and performance analysis of modified AES algorithm with key-dependent dynamic S-box and key multiplication," *Computer Applications Research*, vol. 5, no. 3, 2015.

[54] Thomas Erl, Ricardo Puttini, Zaigham Mahmood "Cloud Computing: Concepts, Technology & Architecture" Prentice Hall, 2013

[55] Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan, A Comprehensive Survey on Security in Cloud Computing, Procedia Computer Science, Volume 110, Pages 465-472, 2017.

[56] Shende, P. ., Vishal Ashok, W. ., Limkar, S. ., D. Kokate, M. ., Lavate, S. ., & Khedkar, G. . (2023). Assessment of Seismic Hazards in Underground Mine Operations using Machine Learning. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 237–243. https://doi.org/10.17762/ijritcc.v11i2s.6142

[57] Thomas, C., Wright, S., Hernandez, M., Flores, A., & García, M. Enhancing Student Engagement in Engineering Education with Machine Learning. Kuwait Journal of Machine Learning, 1(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/123

[58] Thangamayan, S., Kumar, B., Umamaheswari, K., Arun Kumar, M., Dhabliya, D., Prabu, S., & Rajesh, N. (2022). Stock price prediction using hybrid deep learning technique for accurate performance. Paper presented at the IEEE International Conference on Knowledge Engineering and Communication Systems, ICKES 2022, doi:10.1109/ICKECS56523.2022.10060833 Retrieved from www.scopus.com