EAI Endorsed Transactions
on Scalable Information Systems

Research Article EAI.EU

Analytical Method to Compute the Cloud Computing Data Security Issues by Using Encryption Algorithms

Abdul Hannan Khan[1, 2*], Syed Anwer Hasnain[1], Shahan Yamin Siddiqui[1, 2], Muhammad Sohail Irshad[2], Muhammad Sajid[2], Shahid Iqbal[3]

[1]School of Computer Science, National College of Business Administration & Economics, Lahore, Pakistan.
[2]Department of Computer Science, Minhaj University, Lahore, Pakistan.
[3]Department of Computer Science & IT, Virtual University of Pakistan, Lahore, Pakistan.

Abstract

All the associations are genuine thoughts to receive the cloud computing administrations, seeing its advantages as far as cost, openness, accessibility, adaptability and profoundly computerized procedure of upgrading. Cloud computing upgrade the present capacities progressively without further speculation. Cloud computing is a band of assets, applications, and administrations. With the execution of cloud computing, associations have solid worries about the security of their information. The research focuses on the security issues of cloud services. The AES and RSA algorithms will be verified on five parameters key generation time, encryption execution time, memory usage, file uploading time and file downloading time. The CloudSim simulator will be used to find results that the RSA is performing much better than AES in terms of encryption execution time.

Keywords: Advanced Encryption Standard (AES), Rivest-Shamir-Adleman Algorithm (RSA), CloudSim, IAAS, PAAS, SAAS, Key generation time, encryption execution time, and memory usage, file uploading time, and file downloading time.

Received on 03 March 2020, accepted on 04 May 2020, published on 13 May 2020

doi: 10.4108/eai.13-7-2018.164555

1. Introduction

Today is the era of Cloud Computing Technology in IT Industries. Cloud computing, which is based on the Internet has the most powerful architecture of computation. It reckons in a compilation of integrated and networked hardware, software and internet infrastructure. Cloud computing is the delivery of on-demand computing services from applications to storage and processing power, typically over the internet. Rather than owning their computing infrastructure or data centers, companies can rent access to anything from applications to storage from a cloud service provider. One benefit of using cloud computing services is that firms can avoid the upfront cost and complexity of owning and maintaining their own IT infrastructure, and instead simply pay for what they use when they use it. In turn, providers of cloud computing services can benefit from significant economies of scale by delivering the same services to a wide range of customers [1].

Cloud computing is a new rising field of preparing in which resources are available at the versatile environment and obliging practically no exertion. On account of its element and overhauled highlights individuals and affiliations are going to switch towards the cloud. Cloud organization supplier gives the cloud administrations at the economy of scale, compelling and gainful access. Its improvement is from scattered enrolling and the term circulated registering is used as a piece of different extents of translations [2].
The cloud organization suppliers give three particular organizations in the perspective of different capacities, for instance, IaaS (Infrastructure as a Service), SaaS (Software as a Service) as well as PaaS (Platform as a Service) [3].
SaaS: contains programming running on the provider's cloud base, passed on various clients (on enthusiasm) by method for a slight client (e.g. Program) over the Internet. Common representations are Google Docs and Salesforce.com. **PaaS:** These give a designer the versatility to make applications on the supplier's stage. A virtualized stage that consolidates one or more servers, working structures, and specific applications. Major

*Corresponding author. Hannankhan.cs@gmail.com organizations gave are limited, database, and adaptability. Ordinary cases are Google App Engine, Mosso, and AWS: S3. **IaaS:** The organization supplier has the equipment and is responsible for the cabin, pausing and looking at it. The client routinely pays on a for every usage premise. IaaS offers customers adaptable on interest access to resources (frameworks organization, servers, and limit), which could be gotten to by method for an organization API. Typical representations are Flexi scale, AWS: EC2 (Amazon Web Services) [4].

Figure 1 demonstrates the disseminated registering environment in which various cloud customers are getting to the organizations of the cloud while cloud organization's suppliers are moreover giving unmistakable application, stage and structure organizations [5, 6].

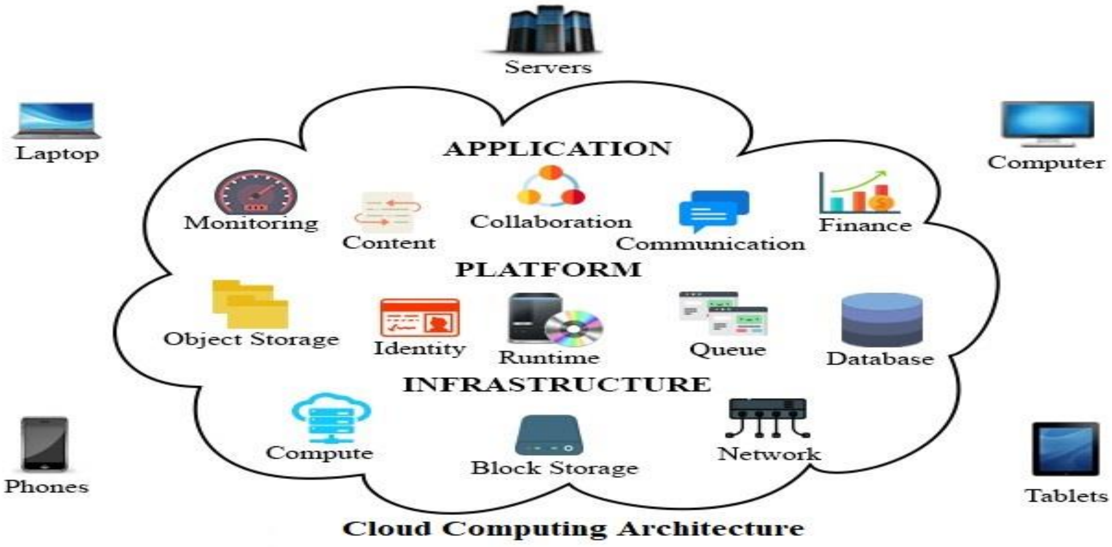


Figure 1. Architecture of Cloud Computing

Cloud computing Deployment models define the type of access of cloud computing that is Private, Public, Community and Hybrid Cloud. **Private Cloud**: is delivered for a singular affiliation. It may be controlled by that affiliation or by the organization's supplier. Each one of the benefits is held for that affiliation. **Public Cloud**: is available to everyone who needs to get the organizations of dispersed figuring and the affiliation who is giving this server is the proprietor of the cloud. Google is one of the instances of the open cloud. **Community Cloud**: Thus suggests a cloud establishment shared by a couple of relationships inside a specific gathering. It might be managed by any of the affiliations or a pariah. A normal case is the open cirrus cloud computing testbed, which is a gathering of federated servers, cultivates transversely more than six districts crossing from North America to Asia. **Hybrid Cloud**: The hybrid circulated registering to join the components of other game plan models as well. It includes a blend of any two (or all) of the three models discussed previously. Systematization of APIs has to lead to less requesting transport of usages across different cloud models [7].

There is a layered framework is available that ensures a security inappropriate processing environment. It includes four layers as showed up in Figure 2. It is the elucidation of the vital issue of cloud computing, which is security. We will realize virtual private networks and firewalls to get the opportunity to secure data from the cloud so that we cloud customer contact data solid.

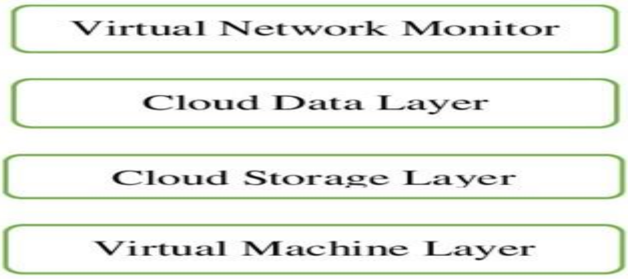


Figure 2. Layer System of Cloud Security

In the first place layer is a secure VM layer. The second layer is passed to the stockpiling layer. This layer has a point of confinement base which merges assets from different cloud association suppliers to accumulate a colossal virtual stockpiling framework. The fourth layer is a virtual system screen layer, this layer joining both equipment and programming approaches in virtual machines to handle issues. Regardless, a few social events are working and awakened by making models and safety for hazes. The cloud standards site is gathering and masterminding data about cloud-related gages being taken a shot at by different social events. CSA is one of them. CSA hoards arrangement suppliers, non-preferences and people to go into talk about the present and future best practices for data accreditation in the cloud [8].

There are distinctive safety issues for Cloud Computing that are showing in figure 3 as it fuses various advances counting virtualization, data security, identity Privacy, location Privacy, Data Privacy, Mobile Device Security, Mobile Cloud Applications Security, Partitioning and Offloading Security. For example, security in the cloud creates that interconnects the frameworks in a cloud must be secure. Load conforming computations must be executed securely. The virtualization perspective dispersed registering results in a couple of safety concerns [9]. For example, ion control incorporates encoding the data and also ensuring that fitting methodologies are approved for data sharing. Resource conveyance and memory organization computations must be secure. Finally, data mining techniques may be important to malware acknowledgment in fogs.

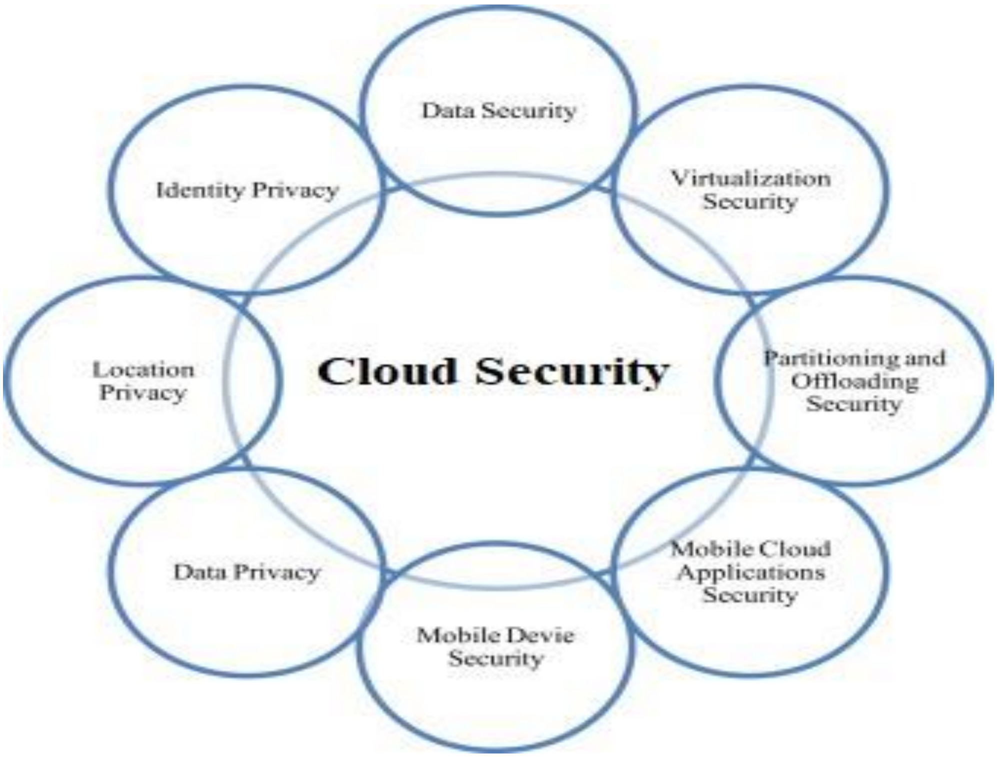


Figure 3. Parts Affecting Cloud Security

Cloud grants customers to accomplish the force of enlisting which beats their own specific physical space. It prompts various safety issues. The cloud organization supplier for cloud guarantees that the client does not go up against any issue, for instance, loss of data or data burglary. Appropriated figuring systems use new advances and organizations, most of which haven't been surveyed with completely studied concerning safety. There is similarly believability where a threatening customer can invade the cloud by emulating a true blue customer, thereby spoiling the whole cloud. This prompts sways different clients who are sharing the dirtied cloud. The safety issues stood up to by conveyed processing are discussed underneath [10].

A two-stage methodology can be utilized to secure the information in distributed computing. To begin with, the stage is identified with transmitting and putting away information while the second is identified with the recovery of information from the cloud. In the first place, stage incorporates putting away information, grouping, list building, and encryption and message verification code [11, 12].

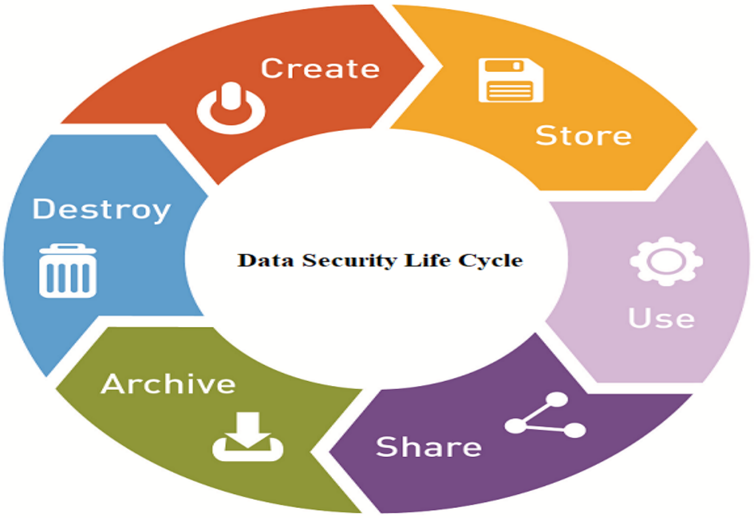


Figure 4. Life Cycle of Data Security

2. Literature Review

Krogstie explored cloud compute is accomplishing increasingly agreeableness step by step. That contains expected be utilizing the cloud for a few existence sat this time, with so many things as Google-applications, MSN Envoy, and Skype what's more, Flick. The thought began in the 1960s when McCarthy considered calculation Open utility [13]. Murugesan compared VPN is extra safe than straightforward dialup, yet network to the external world requires extra safety dealings. Then again, Web 2.0 moved the Web to a more intuitive and community way, guaranteed associates' social connection, and aggregate insight, and presented new Open doors for affecting the Web and pulling in its clients all the more effectively. Undertakings were quickly embracing Web 2.0, which is the next stage in Web development [14]. Smolinski explored that according to him among the well-known names that are connected to cloud registering are Salesforce by supplying endeavor applications during a site, Amazon with its AWS and Amazon's Versatile Figuring Cloud, Microsoft and its famous Windows Sky blue, Google with its a small number of administrations, for example, Google Docs which gave cloud computing an incredible pull and Open deceivability. Eucalyptus, Open Nebula and Aura be presented as the main Open basis stages for sending private, and also crossbreed, mists [15].

Takagi improved comprehend cloud computing, the US NIST characterize it like: "Cloud computing is a representation used for empowering pervasive, helpful, on insist system entrance to a common team of configurable figuring assets (e.g., systems, servers, applications, stockpiling, and administrations) that can be quickly provisioned and discharged through insignificant administration exertion or customer and administration supplier collaboration. This model advances accessibility, also, to be made out of 5 crucial attributes, 3 administration models, and 4 arrangement models" [16]. Krutz described the client control information and application though picking the working framework with an advancement atmosphere facilitated while on interest VMs. The supplier conveys the obligation regarding system, capacity, and server situations. The principle focuses are directors. Safety concerns are taken care of by the client; the cloud supplier gives the slightest safety obligation. It gives computational assets like a stage where applications and administrations can be produced and facilitated. In this layer, the client pedals information while application and administrations are VMs with contact to introduced application. He demonstrated this layer as having common safety procurements among suppliers and clients [17].

Mell explored the NIST description of Cloud Computing characterizes 4 arrangement models for cloud computing: Private/personal, Community/group, Public/open and Hybrid/crossbreed [18].

Winkler used private frameworks inside encouraged, regularly dedicated to one affiliation. Additional data isolation might be required among different workplaces to shield data security. Personal cloud may fuse contact by business accessories, corporate work environments, associates, intranet clients/vendors. Ordinarily, a personal cloud utilizes virtualization development inside the adjacent server ranch. Mutual cloud frameworks between associations are group cloud. It can oversee by a few associations otherwise an outsider and housed location. Clients might associate more than a common personal system or over the Internet utilizing a VPN [19]. Zissis crossbreed cloud consolidates inner as well as outside mists (Open, personal or group). NIST characterizes a crossbreed cloud while "an arrangement of more than one particular cloud frameworks that stay narrative elements, however, are bound together by standardized or selective advancement that enables data and application convey ability (e.g., cloud impacting for weight changing between fogs)" [20].

Modi represented, a secret key sniff is utilized as a part of User to source Attacks to contact honest to goodness client's records. As an outcome, the assailant can abuse shortcomings with a specific end goal to accomplish source-level entrance to the framework, also material or implicit. Source missiles can be created from cushion floods utilizing forms operation as the source. This can occur once the still cradle is overloaded among application agenda policy. In this way, a continuous focus to assailants is the verification procedure and the components worn to save it. Additionally, key loggers, phishing assaults, frail secret key recuperation work processes, and so on don't have widespread benchmarks. Double client confirmation and biometrics may make this less of an issue as this innovation develops. Along these lines in cloud picking up the source-level entrance to VMs or owner be able to gain by assailants who know how to get entrance to legitimate client cases. Public ports separated ports, and shut ports records can remove from port filtering. Assailants discover Open/Public ports and assault the management administrations. Firewall rules, portal sifting, switch, IP address, MAC addresses, and further system linked subtle elements be able to acquire [21].

Distributed computing proposes three organization models by which unmistakable sorts of organizations are passed on to the end customer [22]. The differing models have unmistakable qualities and are suitable for different customers and business objectives. The three models are the SaaS, PaaS, and IaaS. The three models are the SaaS, PaaS, and IaaS, IaaS is the foundation of all Cloud organizations, with PaaS based upon it and SaaS consequently based upon it [23].

Before separating security challenges in Cloud Computing, we need to appreciate the associations and conditions between these cloud organization models [24]. PaaS and what's more SaaS are encouraged on top of IaaS; thusly, any crack in IaaS will influence the security of both PaaS and SaaS organizations, furthermore, it may be legitimate on the alternate way. Regardless, we have to consider that PaaS offers a phase to produce and send SaaS applications, which grows the security dependence between them. As an aftereffect of these significant conditions, any attack on any cloud organization layer can exchange off the upper layers. Each cloud organization model incorporates its particular trademark security deformities; regardless, they in like manner share a few troubles that impact each one of them. These associations and conditions between cloud models may moreover be a wellspring of security risks. A SaaS supplier may rent a change circumstance from a PaaS supplier, which may moreover rent an establishment from an IaaS supplier. Each supplier is accountable for securing his specific organizations, which may achieve a clashing mix of security models. It moreover makes chaos over which organization supplier is careful once an attack happens.

Kumar presented an examination containing fog as well as cloud computing this may support the variations among researchers. Cloud computing technology instantly maturate as well as many development tools come in as design and implement cloud infrastructure [25]. Laghari presented the solution to enhance the standard of experience framework for cloud computing (QoC) as the observance of the standard of experience (QoE) of the end-user using video content services within the cloud computing environment [26, 27, and 28].

It presented a revaluation containing user’s visual perception that they suffered from the general video quality warping because of image compression of social clouds and final visible quality is remittent under fair for twitter, which is specified in scale containing MOS [29]. Laghari presented towards agreement a mobile user's QoE once registering cloud services through mobile apps and mobile device has no sufficiently internal storage. Multiple-way for assembling biased QoE of consumers for having access to WeChat cloud services. If a user didn't accept the quality of service from the cloud service supplier then he did not instantly blame the service supplier about the service level agreement (SLA) violation. It concluded that it is extremely difficult to increase QoE for users if cloud service suppliers aren't aware of the end user's device performance once they getting access to cloud features [30, 31]. It explored the overall cloud computing in several parameters to verify and regulate the end user's quality of experience (QoE) concerning storage, speed, performance with limited resources [32, 33 and 34].

It focused on the problem of supporting k-NN query over cryptographically secure cloud data furthermore data owner can't share his key along with query consumers and recommended another resolution with multiple keys to resolve the key sharing issues in detail [35].

It offered and pointed out the key areas of study with distinctive elements viz architecture, data encryption techniques, access control mechanisms and also detected some extraordinary analysis problems and future analysis recommendations to bring consider action as making sure foolproof confidentiality in smart health solutions [36]. It recommended a non-interactive PPTR strategy without relying on any middleware. PPTR exploited the polynomial procedure to express task requirements and worker interests, taking out the specified keyword dictionary as well as reducing the computing unit cost. It also validated the practicality of PPTR by accomplishing comprehensive comparisons with MSDE, MuED, and MRSE. Through theoretical qualitative analysis and experimental study, the recommended PPTR system outperforms the overall other three strategies in lots of points [37, 38].

Khan presented the solution to enhance the internet of things security with limited resources than focusing on the security of information correspondence of totally obliged devices and the web and their middle of the road devices. Exceptionally obliged devices serve unconfident of assets furthermore don't be able to help the general TLS/DTLS conventions for safe correspondence [39].

3. Proposed Methodology

Simulation technology has become a powerful tool for determining the best start conditions on the "pay-you-go" programs. In some cases, public cloud, which telephone number provided virtual machine infrastructure type is instantiated, at a specified time, which is reflected in the final cost. For example, To develop a new proposal for a variety of related (cloud computing topics purposes, Provide resources or data center management), as well as a lot of work and money shall be invested to establish the appropriate size of the test sets, including data center, which is independent of the various public cloud provider or organization. It may be present in an automated tool. To do this, resulting in yet another performance evaluation will be very difficult. How reproducibility because of the inherent variability in the cloud is controlled. Thus, a tool for the study of complex scenes, it is best to use a simple simulation.

Cloud computing network simulator CloudSim is used in the evaluation of different scenarios using three parameters (resource utilization, power consumption, and cost) to judge the performance of cloud computing services provided by Cloud Service Provider (CSP).

3.1 CloudSim Cloud Computing Simulator

CloudSim simulator interface is as under which contains the major components: the cloud services provider, Cloud User, and Datacenters.

CloudSim is invented at the University of Melbourne, Australia; where researchers work on a project named Cloud Bus. CloudSim aids in the system and behaviour of cloud computing environments like resource sharing techniques, virtual machines, cloud data canter’s, cloud computing services cost models, etc. CloudSim is a powerful tool that assists the researchers to work with it without knowing inner details. CloudSim launches preconfigured configurations to execute the applications and its open-source feature is its main competitive advantage comparing with other commercial network simulators.

CloudSim consists of four components which are shown in figure 5.

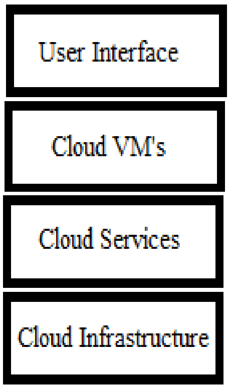


Figure 5. CloudSim Components

A security system can be characterized as a procedure, or a gadget, which intended to distinguish, or keep, or recuperate from a security assault. Security systems like steganography, encryption, hashing and so on are regularly utilized as a part of giving security to a framework. A Security Service can be distinguished as a handling or correspondence administration planned to improve the security of information and the data exchanges of a substance. These administrations help in countering security assaults. Security benefits, as a rule, utilize one or more security system to accomplish its objectives.

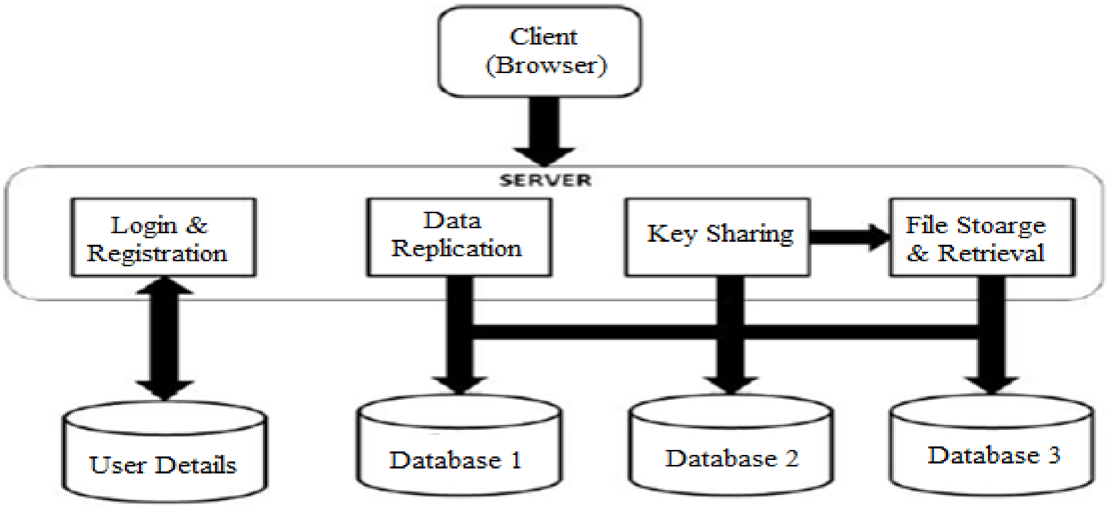


Figure 6. Security Mechanism Architecture

The Security Mechanism consists of the following:-

- Client browser - It's an interface from which the client can access the Cloud services.
- Server - It is responsible for processes including data replication, key storage, file retrieval, file storage. The security mechanism will be implemented at the server-side. User details will be managed and controlled by the Cloud administrator.
- User-Detail - It is a Database that consists of details of Registered Users.
- Databases - These are the individual Clouds in which the data get splits into multiple parts so it is not readable (i.e. in encrypted form). Once the information is encrypted by the Server, the information is divided into multiple parts according to the number of clouds and stores them in these individual Data Stores.

Cryptography can be divided into two categories. SYMMETRIC Cryptography (Encryption) and ASYMMETRIC Cryptography (Encryption). There are many asymmetric encryption algorithms for data protection and security which might be actualized to the cloud such as DES, Triple-DES, AES, as well as Blowfish, etc. DES and AES are mostly used symmetric algorithms.

Figure 7 described the Encryption for cloud computing is the responsibility of CSP which deploys data storage. User data must be encrypted before storing it in the cloud due to the confidentiality problem of the corporate user.

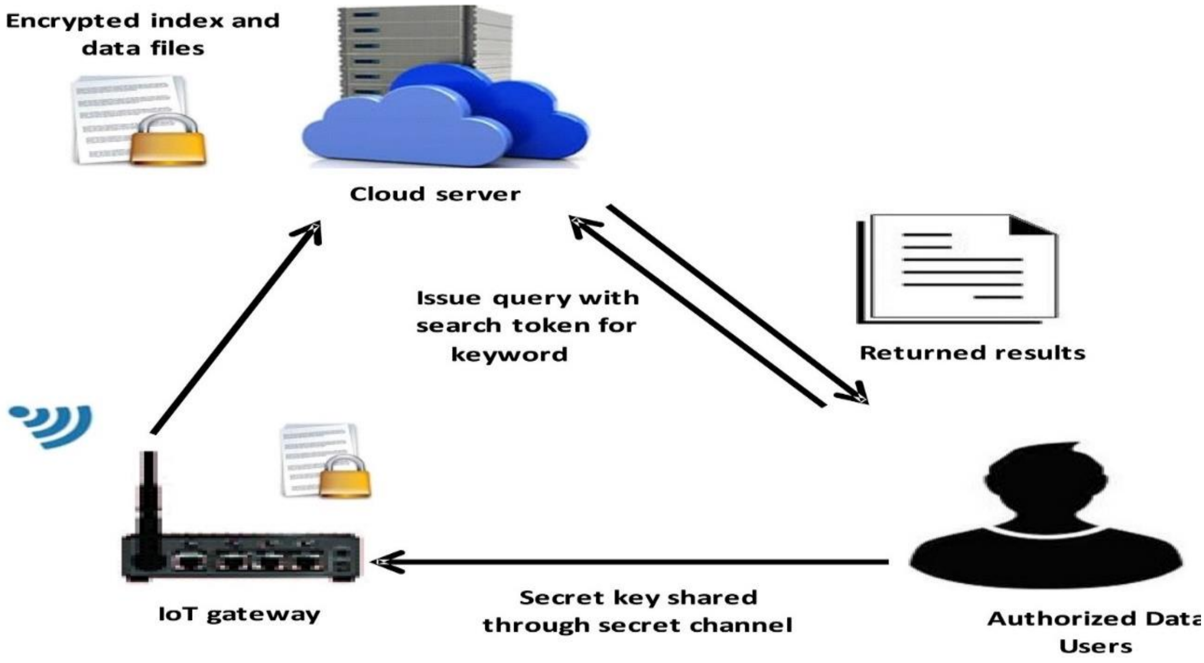

Encrypted index and data files
Cloud server
Issue query with search token for keyword
Returned results
IoT gateway
Secret key shared through secret channel
Authorized Data Users

Figure 7. Encryption for Cloud Computing

3.2 Cryptography Algorithms for Data Security Mechanism

3.2.1 Rivest–Shamir–Adleman Algorithm

The RSA encryption calculation for information security in the cloud computing environment has the greatest vital open key cryptosystem. It is well known as well as broadly utilized open key cryptography mechanism. It applies a huge number of integers and its size in 1,024 bits. It is block cipher due to asymmetric nature. It works with only one round of encryption. Today modern computers use the RSA encryption data security algorithm for the cloud to encrypt and decrypt data. Due to the asymmetric encryption algorithm, it is also called a public key cryptography mechanism. Its mechanism is one of them can be exchanged with everyone and another key must be reserved privately.

3.2.2 AES (Advanced Encryption Standard) Algorithm

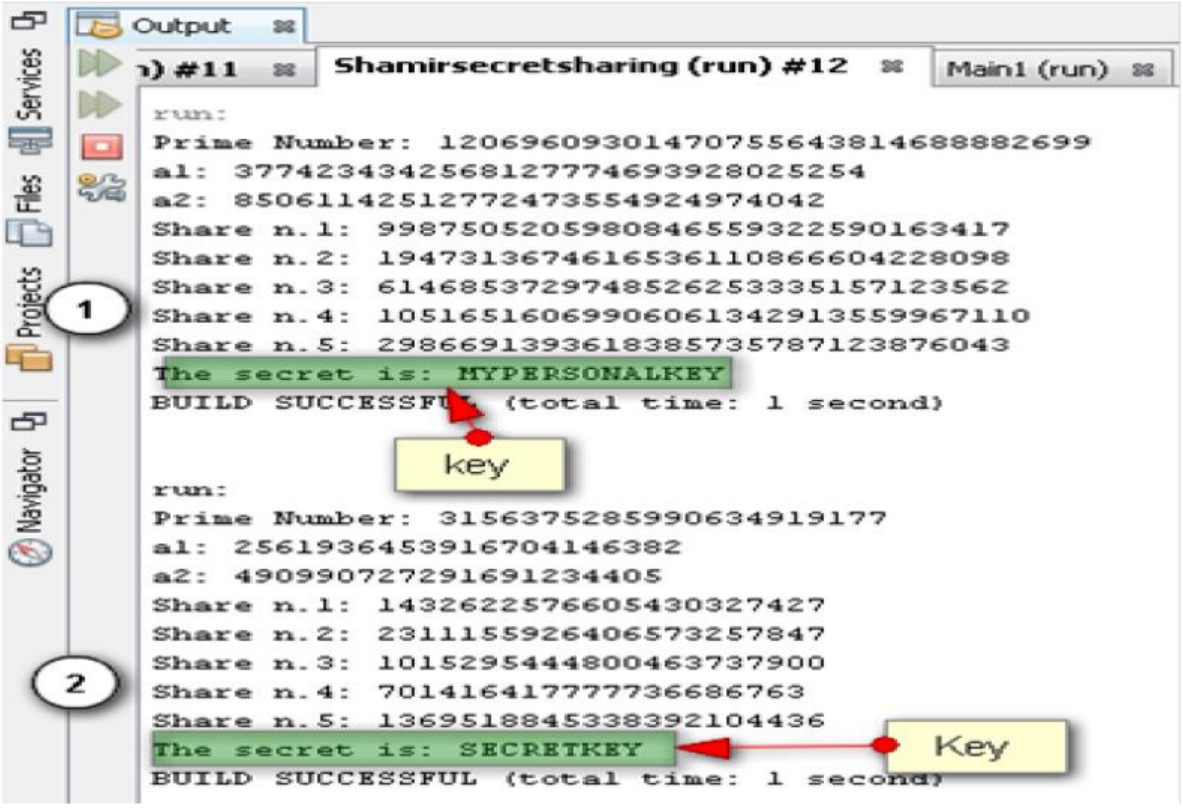
In 2001, the NIST took a step after the successful development of DES (1997); it had chosen the AES as the replacement of DES and 3DES. AES was developed by Vincent Rijmen, Joan Daemen. US Govt. used it due to it is a symmetric block cipher for protecting as well as securing sensitive information. It can be implemented both software and hardware as well. AES uses three-block cipher or rounds depends upon its key versions such as AES-128 bits key, AES-192 bits key and AES-256 bits key. Each version of AES works for encrypting and decrypting information message in pieces of 128 bits utilizing cryptographic keys of 128 bits, 192 bits as well as 256 bits, separately.

In this article, Compared and analyzed the two cryptographic techniques and investigate which one is better in performance than others. Our comparisons based on parameters are encryption execution time, memory usage, key generation time, file uploading time and file downloading time.

Finally, we list the performance comparison of AES and RSA data encryption algorithms by some principles for cloud environments.

4. Results Discussion

Different size of files ranging from 10 KB to 200 KB is used to conduct the simulations. We try to compare the presentation of two presented encryption algorithms AES as well as RSA. CloudSim tool is used to conduct experiments. The key generator from AWS is used that is allowed by CloudSim. CloudSim can access AWS. The figure shows the snapshot of the key generator for implementation 128 bits key is used for simulations.



```
run:
Prime Number: 12069609301470755643814688882699
a1: 3774234342568127774693928025254
a2: 85061142512772473554924974042
Share n.1: 9987505205980846559322590163417
Share n.2: 19473136746165361108666604228098
Share n.3: 6146853729748526253335157123562
Share n.4: 10516516069906061342913559967110
Share n.5: 2986691393618385735787123876043
The secret is: MYPERSONALKEY
BUILD SUCCESSFUL (total time: 1 second)

run:
Prime Number: 3156375285990634919177
a1: 2561936453916704146382
a2: 490990727291691234405
Share n.1: 1432622576605430327427
Share n.2: 2311155926406573257847
Share n.3: 1015295444800463737900
Share n.4: 701416417777736686763
Share n.5: 1369518845338392104436
The secret is: SECRETKEY
BUILD SUCCESSFUL (total time: 1 second)
```

Figure 8. Key Generator for Implementation 128 Bits Key

Performance comparison and analysis of the data encryption algorithms in cloud computing are assessed by considering the following parameters.

4.1 Key Generation Time

The Key Generation Time is called that the key generation software takes to generate the number of keys for encryption.

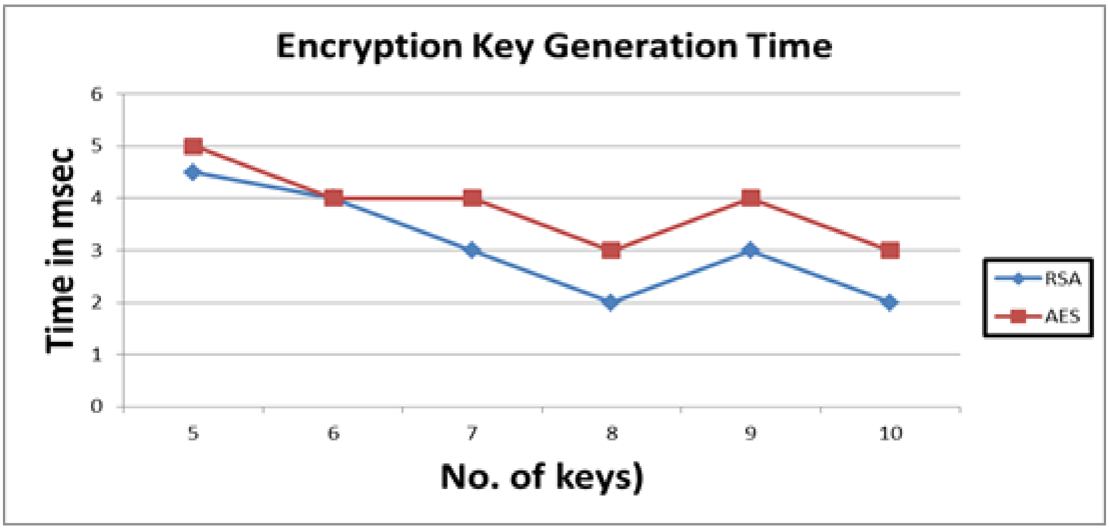


Figure 9. Encryption Key Generation Time

In figure 9 given above horizontally No. of keys is given in ascending order from 5 to 10 while

Vertically Time is also in ascending form from 0sec to 6sec.

- A small parallelogram line represents an RSA algorithm.
- Square line showing the AES algorithm.

Encryption key generation time is measured in sec. and keys are in members. At the start of AES, there are 0 key and 0 times. At 5 keys there is exactly the time taken is 5sec. At key 6 & 7, the time taken is the same 4sec. At key 8 it goes down at 3sec but the time rises again 4sec at key 9. It goes down again 3sec at key 10.

At the start of RSA, there are 0 key and 0 times. At 5 keys there is exactly the time taken is 4.5sec. At key 6 the time taken is 4sec. At key 7 it goes down at 3sec and key 8 is 2sec. But the time rise again 3sec at key 9. It goes down again 2sec at key 10.

4.1.1 Comparison of Key Generation Time

Key generation time of AES and RSA No. of keys w.r.t time.

Table 1. Encryption Key Generation Time of AES and RSA

AES		RSA	
No. of keys	**Time in Msec**	**No. of keys**	**Time in Msec**
5	5	5	4.5
6	4	6	4
7	4	7	3
8	3	8	2
9	4	9	3
10	3	10	2

4.2 Encryption Execution Time

The Encryption Execution Time is called that the encryption algorithm takes to encrypt plain text to cipher text. This time calculates the throughput of the encryption algorithm.

In figure 10 given below horizontally file sizes are given in ascending order from 50 kb to 200 kb

While vertically Time is also in ascending form from 0 Msec to 70 Msec.

Encryption execution time is measured in kb/sec. At the start of AES, the file size is 50 kb the execution time 25 Msec. When the file size 60 kb the file execution time goes up 45 Msec. The file execution time changes extremely high or extremely low in the AES accordingly file size. Or sometimes increase slightly from 30 Msec to 33 Msec.

At the start of RSA, the file size is 50 kb and file execution time is 7 msec. When the file size 60 kb the execution time goes a little high 8 Msec. All the variations in the RSA is increased slightly from 7 Msec to 11 Msec.

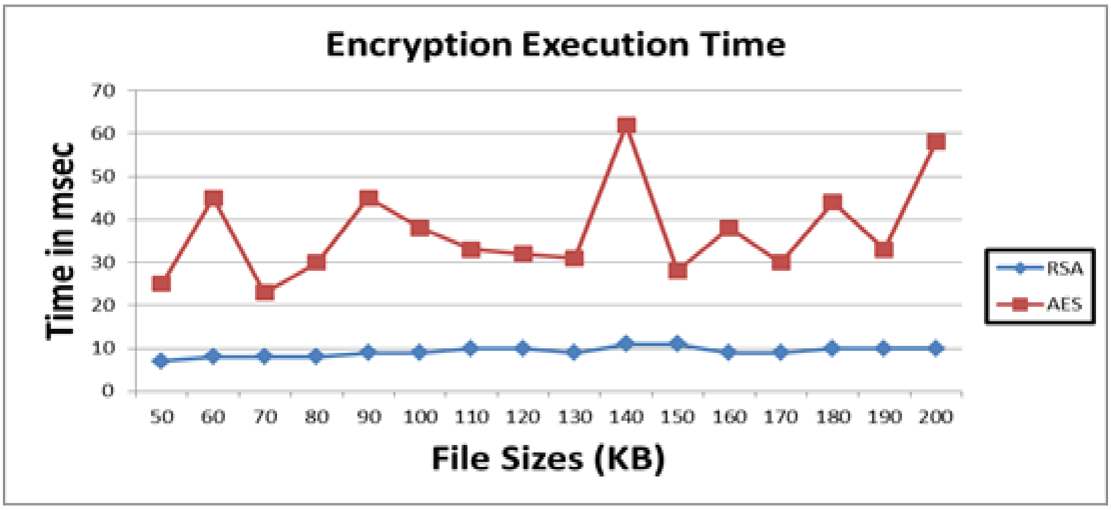


Figure 10. Encryption Execution Time

4.2.1 Comparison of Encryption Execution Time

Encryption Execution time of AES and RSA file size in kb w.r.t time in Msec.

Table 2. Encryption Execution Time of AES and RSA

AES		RSA	
File Size (kb)	**Time in Msec**	**File Size (kb)**	**Time in Msec**
50	25	50	7
60	45	60	8
70	22	70	8
80	30	80	8
90	45	90	9
100	38	100	9
160	39	160	10
170	30	170	9
180	45	180	10
190	38	190	10
200	59	200	10

4.3 Memory Usage (Encrypted File Size)

Space is used to store the encrypted file on the server.

In figure 11 given below horizontally file size s is given in ascending order from 50 kb to 200 kb

While vertically Bytes is also in ascending form 0 to 35000.

At the start of AES, the file size is 50kb the memory usage is 0 byte. When the file size 70kb the memory usage goes up to 4000 bytes. The memory usage increase accordingly increasing the file size. The memory usage is 1 byte. When the file size 70kb the memory usage increase to 4100. All the variations in the RSA are increasing from 0bytes to 35000bytes.

The memory usage in AES is less than RSA.

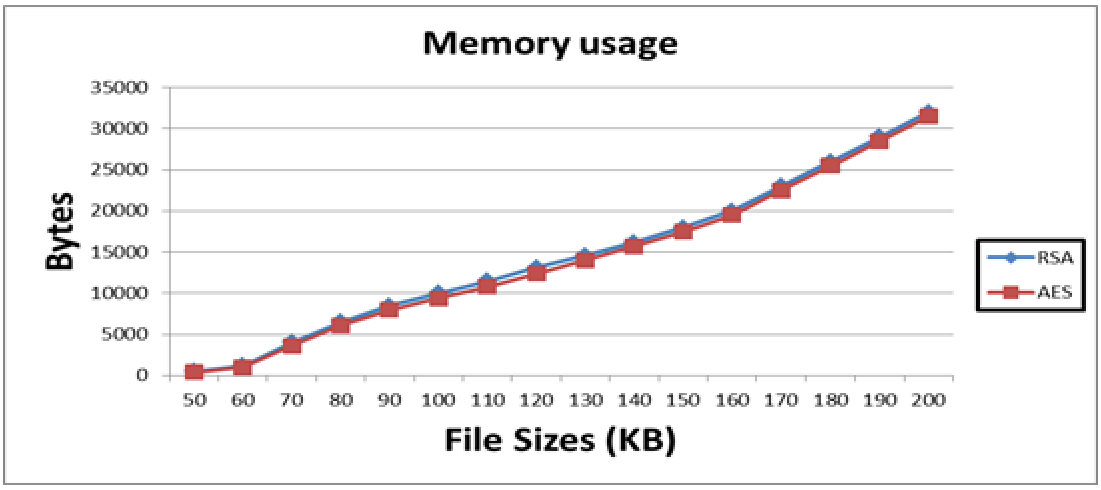


Figure 11. Memory Usage

4.3.1 Comparison of Memory Usage (Encrypted File Size)

Memory Usage of AES and RSA file size in kb w.r.t bytes.

Table 3. Memory Usage of AES and RSA

AES		RSA	
File Size (kb)	**Bytes**	**File Size (kb)**	**Bytes**
50	0	50	0
60	1000	60	1000
70	4000	70	4000
80	5000	80	6000
90	7000	90	8000
100	8000	100	9000
110	9000	110	10000
120	12000	120	13000
130	13000	130	14000
140	14000	140	15000
150	16000	150	17000
160	18000	160	19000
170	23000	170	24000
180	25000	180	26000
190	28000	190	29000
200	30000	200	31000

4.4 File Uploading Time

The File Uploading Time is called that the sever takes to receive files from the client.

In figure 12 given below horizontally file sizes are given in ascending order from 50 kb to 200 kb

While vertically time is also in ascending from 0 Msec to 70 Msec.

At the start of AES, the file size is 50 kb the file uploading time is 10 msec. When the file size 60 kb the file uploading time increase 12 Msec. The file uploading time increase accordingly increasing the file size. The file size is 200 kb than the file uploading time is 59 msec.

At the start of RSA, the file size is 50 kb the file uploading time is 9 msec. When the file size 60 kb the file uploading time increase 10 sec. The file uploading time increase accordingly increasing the file size. The file size is 200 kb than the file uploading time is 35 msec.

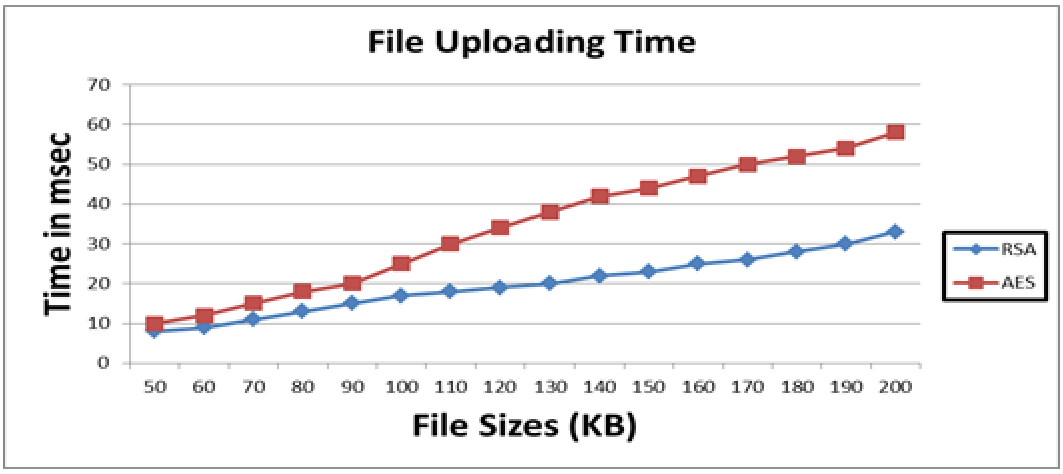


Figure 12. File Uploading Time

4.4.1 Comparison of File Uploading Time

File Uploading Time of AES and RSA file size in kb w.r.t time in Msec.

Table 4. File Uploading Time of AES and RSA

AES		RSA	
File Size (kb)	**Time in Msec**	**File Size (kb)**	**Time in Msec**
50	10	50	8
60	13	60	9
70	15	70	10
80	19	80	13
90	20	90	15
100	25	100	17
110	30	110	18
120	34	120	19
130	38	130	20
140	41	140	21
150	43	150	23
160	48	160	25
170	50	170	27
180	51	180	28
190	54	190	30
200	59	200	32

4.5 File Downloading Time

The File Downloading Time is called that the server takes to send the file to the client.

In figure 13 given below horizontally file sizes are given in ascending order from 50 kb to 200 kb while vertically time is also in ascending from 0 Msec to 70 Msec

At the start of AES, the file size is 50 kb the file downloading time is 8 msec. When the file size 60kb the file downloading time increase 10 Msec. The file uploading time increase accordingly increasing the file size. The file size is 200 kb than the file uploading time is 52 msec.

At the start of RSA, the file size is 50 kb the file uploading time is 5 msec. When the file size 60 kb the file uploading time increase 9 Msec. The file downloading time increase accordingly increasing the file size. The file size is 200 kb than the file uploading time is 28 msec.

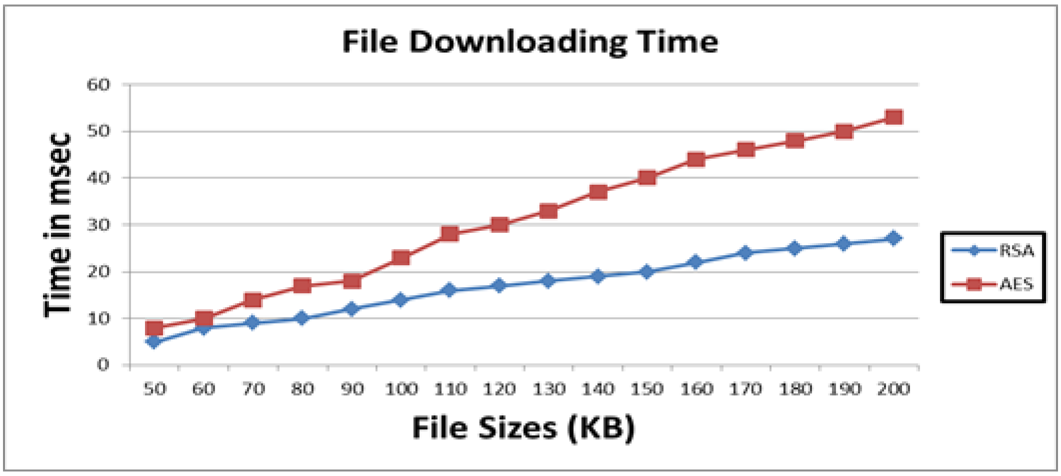


Figure 13. File Downloading Time

4.5.1 Comparison of File Downloading Time

File downloading time of AES and RSA file size in kb w.r.t time in Msec.

Table 5. File Downloading Time of AES and RSA

AES		RSA	
File Size (kb)	**Time in Msec**	**File Size (kb)**	**Time in Msec**
50	8	50	5
60	10	60	7
70	14	70	9
80	17	80	10
90	19	90	12
100	22	100	15
110	28	110	17
120	30	120	18
130	32	130	19
140	37	140	20
150	40	150	22
160	44	160	24
170	46	170	25
180	48	180	26
190	50	190	27
200	53	200	28

4.6 Resource Utilization Time

In figure 14 given below horizontally time in an hour is given in ascending order from 1hour to 5 hour while vertically resource utilization (CPU in MPS) is also in ascending form 1.3 to 1.6

The resource utilization first increases in the AES with time, but after some time the resource utilization decreases.

The resource utilization first increases in RSA with time, but after some time it will decrease. The difference between AES and RSA is that the AES decreases and also decreases but in RSA it will increase than decrease and then again increase.

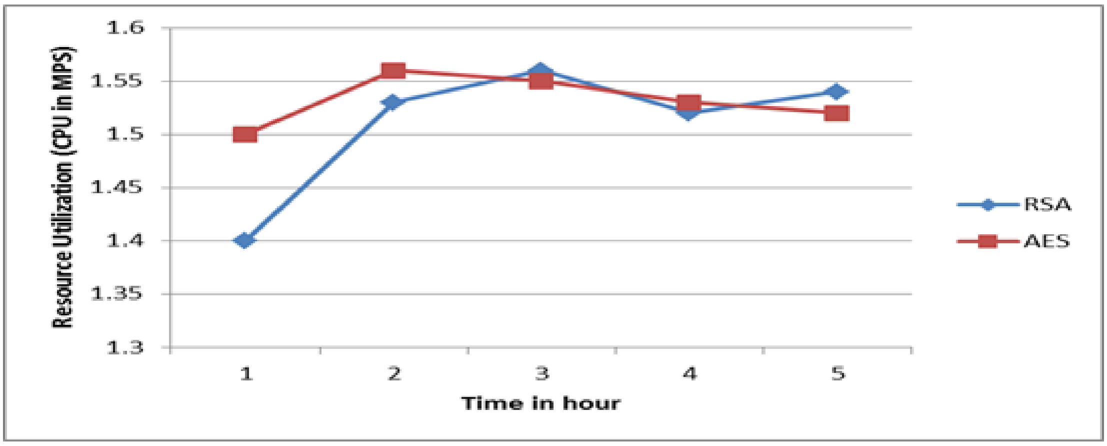


Figure 14. Resource Utilization Time

4.6.1 Comparison of Resource Utilization (CPU in MPS)

Resource utilization of AES and RSA time in hour's w.r.t resource utilization.

Table 6. Resource Utilization

AES		RSA	
Resource utilization	**Time in Msec**	**Resource utilization**	**Time in Msec**
1.5	1	1.4	1
1.56	2	1.53	2
1.55	3	1.56	3
1.53	4	1.52	4
1.52	5	1.54	5

4.7 Resource Utilization Threshold

In figure 15 given below horizontal threshold is given in ascending order from 0.1 to 0.9 while vertically resource utilization (CPU in MPS) is also in ascending form 1.46 to 1.6.

The resource utilization in the 0.1 to 0.2 threshold decrease from 1.54 to 1.5 in the AES. In 0.2 to 0.3 thresholds the resource utilization increases from 1.5 to 1.55. But in 0.3 to 0.4 threshold resource utilization also increase from 1.55 to 1.56. Then it will decrease again from 1.56 to 1.52.

The resource utilization in the 0.1 to 0.2 threshold decrease from 1.54 to 1.5 in the RSA. In 0.2 to 0.3 thresholds the resource utilization increases from 1.5 to 1.58. But in 0.3 to 0.4 threshold resource utilization decreases again from 1.58 to 1.54. Then it will increase again from 1.54 to 1.55.

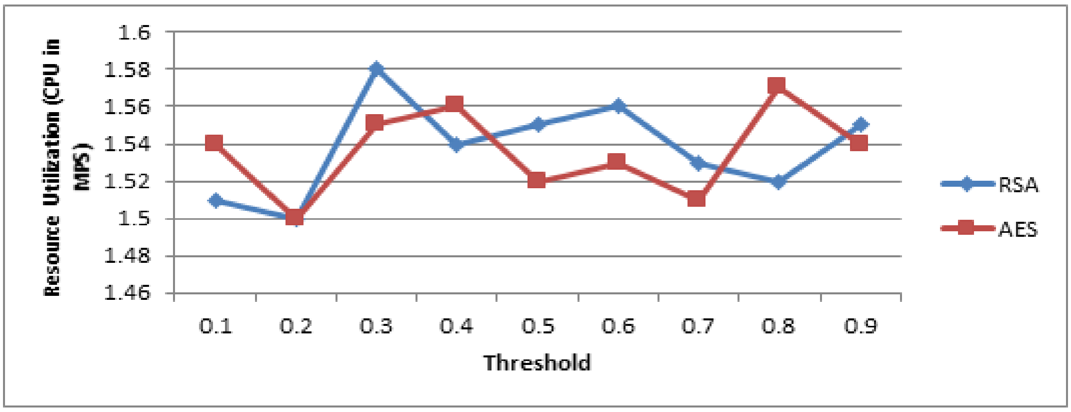


Figure 15. Resource Utilization Threshold

4.7.1 Comparison of Resource Utilization Threshold

Threshold of AES and RSA time in threshold w.r.t. resource utilization.

Table 7. Resource Utilization Threshold

AES		RSA	
Resource utilization	Threshold	Resource utilization	Threshold
1.54	0.1	1.51	0.1
1.5	0.2	1.5	0.2
1.55	0.3	1.58	0.3
1.56	0.4	1.54	0.4
1.52	0.5	1.55	0.5
1.53	0.6	1.56	0.6
1.51	0.7	1.57	0.7
1.57	0.8	1.52	0.8
1.54	0.9	1.55	0.9

4.8 Energy consumption Time

In figure 16 given below horizontally time in an hour is given in ascending order from 1hour to 5hour while vertically energy consumption (in KWh) is also in ascending form 0 to 1.6

The energy consumption in the 1 to 2-hour decrease from 1.2 to 1.1 in the AES. In 2 to 3 hours, energy consumption increases from 1.1 to 1.5. But in 3 to 4-hour energy consumption decrease again from 1.5 to1.4. Then it will increase again from 1.4 to 1.5.

The energy consumption in the 1 to 2-hour increase from 1 to 1.2 in the RSA. In 2 to 3 hour v the energy consumption also increases from 1.2 to 1.3. But from 3 to 4-hour energy consumption decrease from 1.3 to 0.9. Then it will increase again from 0.9 to 1.3.

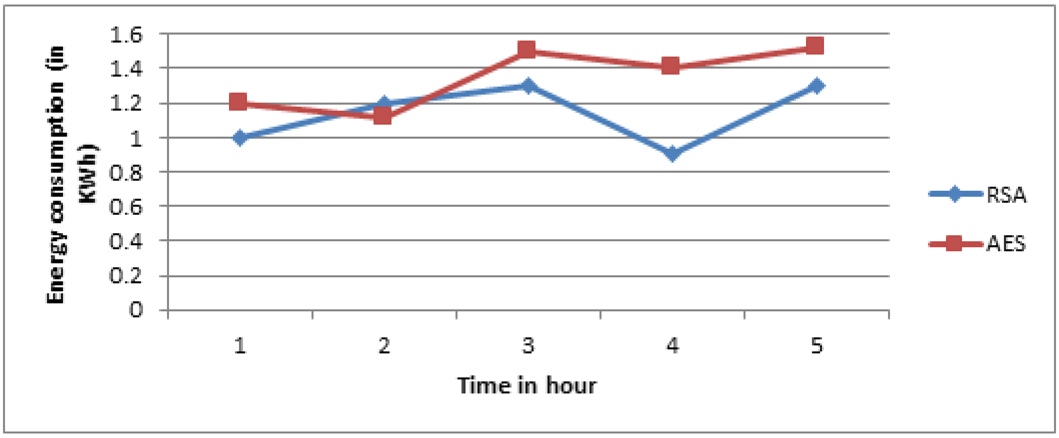


Figure 16. Energy Consumption Time

4.8.1 Comparison of Energy Consumption (in KWh)

Energy consumption of AES and RSA time in an hour's w.r.t. energy consumption (in KWh).

Table 8. Energy Consumption Time of AES and RSA

AES		RSA	
Energy Consumption	**Time in Msec**	**Energy Consumption**	**Time in Msec**
1.2	1	1	1
1.1	2	1.2	2
1.5	3	1.3	3
1.4	4	0.9	4
1.5	5	1.3	5

5. Conclusion

Information technology brought a revolution in form of cloud computing, a lot of researchers had made a lot of effort to resolve cloud computing issues and also they had addressed different data security issues but still, there are various problems related to data security. Twenty different sizes of files are used for simulations of two data/information encryption techniques AES and RSA. These files are used for evaluating the performance of both algorithms to test their performance comparison. The comparative analysis results of these files ranging from 10KB to 200KB on AES and RSA are simulated. The AES and RSA algorithms are verified on five parameters key generation time, encryption execution time, memory usage, file uploading time and file downloading time i.e. We analyzed that the encryption execution time consumed by RSA is less as compared to the time consumed by AES but RSA has occupied more memory space then AES. It is clear from simulation results that the RSA is performing much better than AES in terms of encryption execution time.

The objective of the simulation is to compare and analyze the performance and effectiveness of both encryption algorithms that are providing data security for files transmission between server to client (downloading) or client to the server (uploading). In short, keeping data to the cloud is carefully stored for long-term at large-scale data storage places; it does not instantaneously provide any assurance on data availability and data consistency. From simulation results, the RSA encryption technique can be useful for data/information security in the cloud environment. Our present objective is to secure text documents which may include confidential data like credit card details, bank customer's records, etc.

Conflicts of Interest:

The authors declare that there are no conflicts of interest regarding the publication of this article.

References

[1] Venters, W., & Whitley, E. A. (2012). A critical review of cloud computing: researching desires and realities. Journal of Information Technology, 27(3), 179-197.

[2] Fowler, G. A., & Worthen, B. (2009). The internet industry is on a cloud–whatever that may mean. The Wall Street Journal, 26.

[3] Sharif, F., & Hafeez, A. (2012). The analysis of cloud computing major security concerns & their solutions. J. Inf. Commun. Technol, 6(2), 48-53.

[4] Sowmya, S. K., Deepika, P., & Naren, J. (2014). Layers of cloud–iaas, paas, and saas: A survey. International Journal of Computer Science and Information Technologies, 5(3), 4477-4480.

[5] Mujahid, A., Mahmood, T., Iqbal, W. and Ali, M, N. (2013). Comparative Analysis Of Cloud Computing Security Issues. Lahore, Pakistan.: Lahore Printing press.

[6] Kulkarni, G. (2012). Security aspects in cloud computing. Pune, India. Printing Press

[7] Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering, 39(1), 47-54.

[8] Nelson Gonzaalez, Charles Miers, Fernando REdigolo.(2011). A quantitative analysis of current security concerns and solutions for cloud computing. So Paulo, Brazil.: Seo Paulo Printing Press.

[9] Behl, A., & Behl, K. (2012). An analysis of cloud computing security issues. New Delhi, India.: New Delhi Printing Press.

[10] Huaglory Tianfield. (2012). Security Issues in Cloud Computing.Glasgow Caledonian, UK.: Printing press.

[11] Sood, S. K. (2012). A combined approach to ensure data security in cloud computing. Shimla, India. Shimla Printing Press.

[12] Shaikh, R., & Sasikumar, M. (2012). Security issues in cloud computing. Mumbai, India. Mumbai Printing Press.

[13] Krogstie, J.(2012). Model-based development and evolution of information systems a quality approach. New York, USA.: New York Printing Press.

[14] Murugesan, S.(2007). Information Technology Professional. MITP, USA.: IEEE printing press.

[15] Sempolinski, P.(2010). A Comparison and Critique of Eucalyptus, OpenNebula, and Nimbus in Cloud Computing Technology and Science. Notre Dame, USA.: Notre Dame printing press.

[16] Takabi, H.(2010). Security and Privacy Challenges in Cloud Computing Environments Security Privacy. Pittsburgh, USA.: Pittsburgh Printing Press.

[17] Krutz, R, L.(2010). Cloud security: a comprehensive guide to secure cloud computing. Indianapolis, IN.: Wiley Printing Press.

[18] Mell, P.(2011). The NIST definition of cloud computing (draft). Nigeria, REMO.: Nigeria Printing Press.

[19] Winkler,V,R,T.(2011). Securing the Cloud: Cloud Computer Security Techniques and Tactics. Waltham, MA.: Syngress Printing Press.

[20] Zissis, D.(2012). Addressing cloud computing security issues. Lesvos, Greece.: Lesvos Printing Press.

[21] Modi, C.(2013). A survey of intrusion detection techniques in the Cloud. London, UK.: London Printing Press.

[22] Subashini, S. and Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. UK Printing Press.

[23] Bhadauria, R., Chaki, R., Chaki, N. and Sanyal, S. (2011). A Survey on Security Issues in Cloud Computing. Pune, india.: Pune Printing Press.

[24] Mell, P.(2011). The NIST definition of cloud computing (draft). Nigeria, REMO.: Nigeria Printing Press.

[25] Kumar, V., Laghari, A. A., Karim, S., Shakir, M., & Brohi, A. A. (2019). Comparison of fog computing & cloud computing. Int. J. Math. Sci. Comput, 1, 31-41.

[26] Laghari, A. A., He, H., Khan, A., Kumar, N., & Kharel, R. (2018). Quality of experience framework for cloud computing (QoC). IEEE Access, 6, 64876-64890.

[27] Laghari, A. A., He, H., Halepoto, I. A., Memon, M. S., & Parveen, S. (2017). Analysis of quality of experience frameworks for cloud computing. IJCSNS, 17(12), 228.

[28] Laghari, A. A., He, H., Shafiq, M., & Khan, A. (2018). Assessment of quality of experience (QoE) of image compression in social cloud computing. Multiagent and Grid Systems, 14(2), 125-143.

[29] Laghari, A. A., He, H., Karim, S., Shah, H. A., & Karn, N. K. (2017). Quality of experience assessment of video quality in social clouds. Wireless Communications and Mobile Computing, 2017.

[30] Laghari, A. A., He, H., Shafiq, M., & Khan, A. (2017, May). Impact of storage of mobile on quality of experience (QoE) at the user level accessing the cloud. In the 2017 IEEE 9th international conference on communication software and networks (ICCSN) (pp. 1402-1409). IEEE.

[31] Laghari, A. A., He, H., Memon, K. A., Laghari, R. A., Halepoto, I. A., & Khan, A. (2019). Quality of experience (QoE) in cloud gaming models: A review. Multiagent and Grid Systems, 15(3), 289-304.

[32] Laghari, A. A., He, H., Shafiq, M., & Khan, A. (2016, October). Assessing effect of Cloud distance on end user's Quality of Experience (QoE). In 2016 2nd IEEE international conference on computer and communications (ICCC) (pp. 500-505). IEEE.

[33] Laghari, A. A., He, H., Laghari, R. A., Khan, A. I., & Yadav, R. (2019). Cache Performance Optimization of QoC Framework.

[34] Laghari, A., Laghari, R., Wagan, A., & Umrani, A. (2020). Effect of Packet Loss and Reorder on Quality of Audio Streaming. EAI Endorsed Transactions on Scalable Information Systems, 7(24).

[35] Cheng, Ke, Liangmin Wang, Yulong Shen, Hua Wang, Yongzhi Wang, Xiaohong Jiang, and Hong Zhong. "Secure k-nn query on encrypted cloud data with multiple keys." IEEE Transactions on Big Data (2017).

[36] Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-Health solutions in cloud computing. IEEE Access, 7, 74361-74382.

[37] Wang, H., Wang, Y., Taleb, T., & Jiang, X. (2019). Special issue on security and privacy in network computing. World Wide Web, 1-7.

[38] Shu, J., Jia, X., Yang, K., & Wang, H. (2018). Privacy-preserving task recommendation services for crowdsourcing. IEEE Transactions on Services Computing.

[39] Khan, A. H., Siddiqui, S. Y., Irshad, M. S., Ali, S., Saleem, M. R., & Iqbal, S. Analytical Method to Improve the Security of Internet of Things with Limited Resources.