International Journal of Research in Economics and Social Sciences(IJRESS)
Available online at: http://euroasiapub.org
Vol. 9 Issue 5, May- 2019
ISSN(o): 2249-7382 | Impact Factor: 6.939 |

A CRITICAL ANALYSIS OF CLOUD COMPUTING TECHNOLOGY AND SECURITY SYSTEM

Shakeb Khan, Research Scholar, Department of Computer Science, Himalayan Garhwal University
Dr. Harsh Kumar, Professor, Department of Computer Science, Himalayan Garhwal University, Uttarakhand

ABSTRACT

Distributed computing is characterized by the United States' National Institute of Standards and Technology (NIST) as "a model for empowering advantageous, on-request network admittance to a common pool of configurable figuring assets (e.g., networks, servers, stockpiling, applications, and administrations) that can be quickly provisioned and delivered with insignificant administration exertion or specialist organization communication".Organization security alludes to the assurance of information and data that is utilized as a feature of any framework, regardless of whether it is put away on the host, server, or communicated across the organization, etc. Mystery, validation, non-disavowal, and respectability the board are altogether parts of organization security. Framework security has become more imperative to PC clients, organizations, and the military. With the appearance of the web, security has turned into a significant concern, and understanding the recorded setting of safety considers a superior comprehension of the development of safety advancement. The web's construction made it feasible for an assortment of safety dangers to emerge. At the point when the web's primary arranging is changed, it can decrease the probability of attacks being sent through the framework. The expression "distributed computing" alludes to a subset of the expression "organization" or "web." The web fills in as the working mechanism for distributed computing. The security of the cloud is like the security of an organization. The endeavors to foster wellbeing identified with the cloud organization, then again, are as an unmistakable difference.

KEY WORDS: Cloud Computing Technology, data storage, Networking, Information.

International Journal of Research in Economics and Social Sciences(IJRESS)
Available online at: http://euroasiapub.org
Vol. 9 Issue 5, May- 2019
ISSN(o): 2249-7382 | Impact Factor: 6.939 |

INTRODUCTION

Evolution of cloud computing

The advancement of Cloud figuring, which included systems administration, network sharing, data sharing, asset sharing, and administration sharing [Mohamed Magdy Mosbah et al., 2013]. The Cloud's first stage was like systems administration, with a few PCs connected together. These are alluded to as provincial organizations. Public labs and colleges are quick to utilize it. Then, at that point, utilizing TCP/IP to associate these organizations, the Internet was conceived, and it immediately spread over the world. The World Wide Web was made because of the utilization of the HTML design and the HTTP convention for trading data by means of a program. Then, at that point, came framework figuring, which was made to deal with the asset sharing cycle. It provided programming and conventions for far off asset sharing. It was endorsed for use in High Performance Computing (HPC) projects. Distributed computing, the latest phase of the cloud, permits clients to share administrations by means of the web by abstracting the infrastructural intricacies of servers, different stages, figuring limit, or entire programming programs, in addition to other things [Balinder Singh,2013].

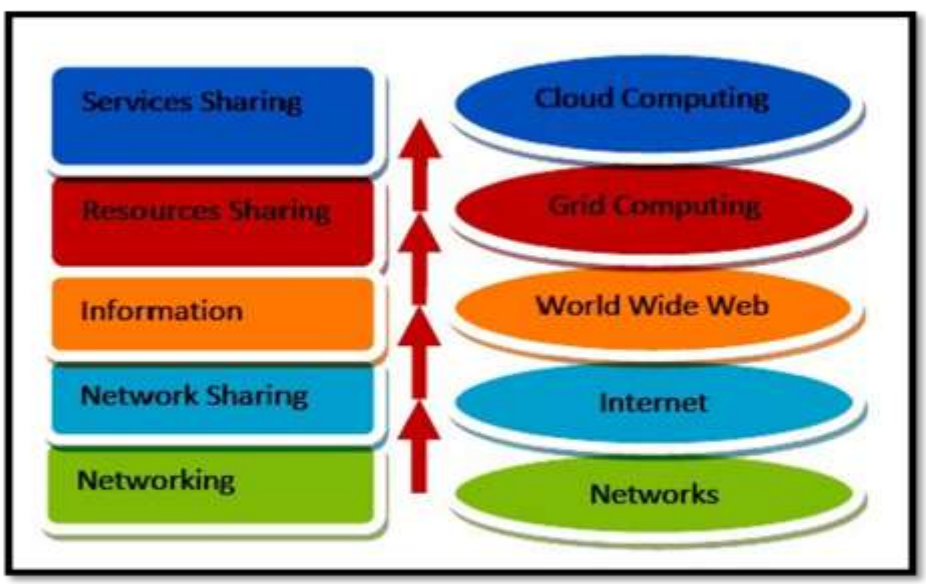

Figure-1: Cloud computing evolution

International Journal of Research in Economics and Social Sciences(IJRESS)
Available online at: http://euroasiapub.org
Vol. 9 Issue 5, May- 2019
ISSN(o): 2249-7382 | Impact Factor: 6.939 |

Cloud Computing Technology

Distributed computing is an Internet-based development that empowers a scope of organizations like programming, equipment, information stockpiling, and system to be conveyed over the web. As Cloud registering joins a few developments like organizations, virtualization, working frameworks, asset booking, exchange the executives, load adjusting, simultaneousness control, and memory the board, a large number of safety challenges emerge. It likewise incorporates information support planning and secure stockpiling of the support media. Distributed computing is turning into a well known objective for cybercriminals. To forestall digital wrongdoing, cloud suppliers should guarantee that sufficient safety efforts are set up. Getting to these cloud administrators raises a huge number of safety concerns.

Characteristics of cloud computing

Distributed computing administrations have five key qualities that show how they identify with and vary from customary figuring strategies.

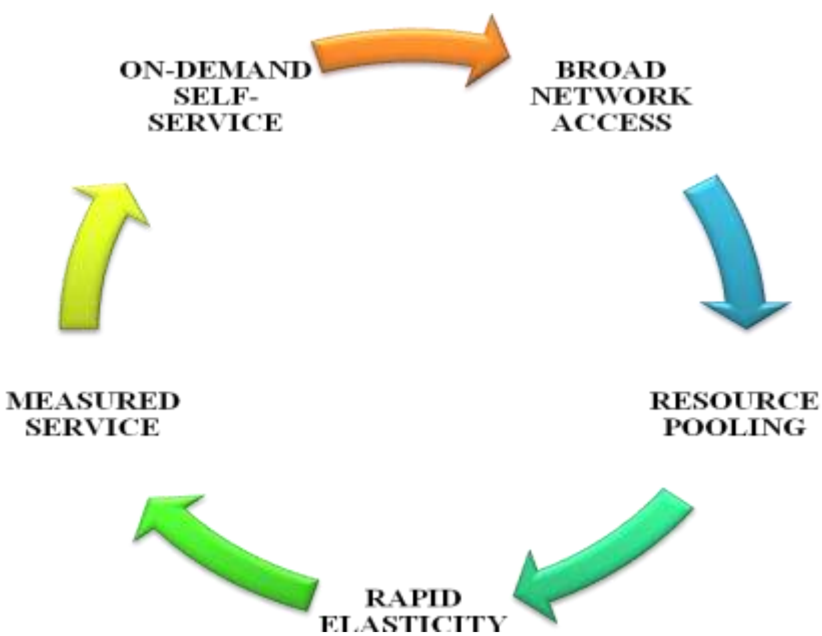

FIGURE-2: Characteristics of cloud computing

- **On-demand self-service**

A purchaser can naturally put together PC abilities, for example, server time and framework stockpiling, depending on the situation without the requirement for human joint effort or master help.

- **Broad network access**

Capacities are gotten to through the framework and got by standard instruments that are used by an assortment of flimsy and thick shopper gadgets, including mobile phones, tablets, versatile PCs, and workstations.

- **Resource pooling**

The PC assets of the supplier are pooled to serve the clients through a multi-occupant show, with different physical and virtual assets being given and reassigned depending on the situation by the clients.

- **Rapid elasticity**

"Flexible figuring" alludes to the unique variation of limit, for example, through changing the usage of registering assets to coordinate with a changed responsibility. Quick Elasticity is portrayed as the ability to increase assets and down depending on the situation in the most limited time conceivable. The cloud seems to be vast to the customer, and the purchaser can buy so a lot or as little PC power as they require.

- **Measured service**

Asset usage may be followed, controlled, and announced, giving both the supplier and the buyer more straightforwardness. Metering limit is utilized by distributed computing administrations to screen and update asset utilization. Pay-per-use gauges are utilized to charge for data innovation (IT) administrations.

Types of cloud services

Distributed computing has been separated into three classifications dependent on the administrations it gives. Coming up next is a speedy summary of each assistance model.

- **Software as a Service (SaaS)**

Programming as a Service (SaaS) permits clients to associate with and use cloud-based projects, for example, email or a program interface over the Internet. With the conceivable exemption of restricting client explicit application plan decisions, the client has no oversight or authority over the cloud structure, which incorporates the framework, servers, working frameworks, stockpiling, or even individual application capacities.

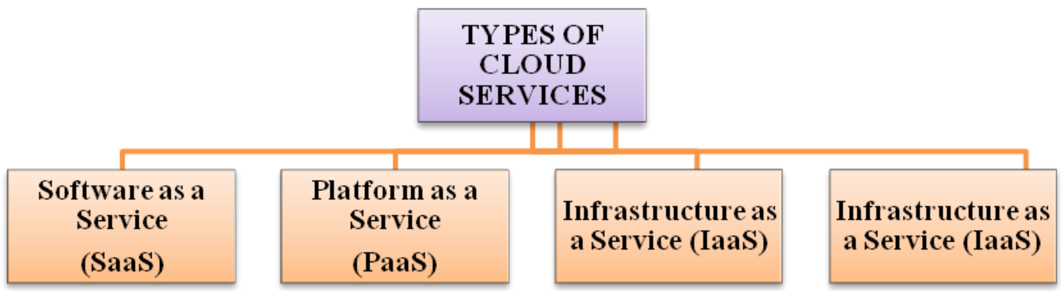

Figure-3: Types of cloud service

- **Platform as a Service (PaaS)**

Stage as a Service (PaaS) is a sort of web based help that permits clients to create and convey applications and administrations. The client doesn't have power over or oversight of the fundamental cloud foundation, like the framework, servers, working frameworks, or capacity, yet has authority over the conveyed applications and perhaps design settings for the application-facilitating state. PaaS administrations are facilitated in the cloud and can be gotten to straightforwardly through an internet browser by clients.

- **Infrastructure as a Service (IaaS)**

Foundation as a Service (IaaS) gives customers virtualized PC assets for orchestrating, planning, putting away, networks, and other basic processing assets through the web. The client can send and work self-decisive programming that incorporates working frameworks and applications. The client doesn't have command over the secret cloud engineering, however has authority over working frameworks, stockpiling, and conveyed applications, just as the capacity to restrict the force of some framework the board parts (e.g., have firewalls).

Cloud computing architecture

The overall construction of distributed computing is portrayed in Figure. The cloud can be gotten to through Cloud Service Providers utilizing any gadget like a PDA (Personal Digital Assistant), cell phone, etc (CSP). Google Apps is the best illustration of distributed computing since it permits any program to be open through a program and sent across large number of PCs by means of the Internet [Srinivasa Rao V et al., 2009].The front-end stage, back-end stage, and organization parts make up the distributed computing engineering. The host, like a PDA or a cell phone, is the front-end stage or customer, while the numerous PCs, servers, and administrations contain the back finish of the framework. Frameworks for putting away information in the "cloud" of PC administrations. The framework is overseen by a focal server, which monitors information transmission and customer solicitations to guarantee that everything works well. It sticks to a bunch of conventions and utilizes middleware, which is a kind of programming. Middleware permits machines on an organization to speak with each other. The server doesn't run at greatest limit constantly. This shows that there is unused preparing power that is being wasted. It's attainable to segment an actual server into numerous servers, each with its own working framework. Server virtualization is the name of the methodology. Server virtualization disposes of the necessity for more actual PCs by upgrading the yield of every server [Sareen et al., 2013]. There are two additional names utilized related to virtualization: hypervisor or Virtual Machine Monitor (VMM) and Virtual Machine (VM). VMM is a piece of programming that permits diverse working frameworks to run on a similar machine. A virtual machine (VM) is a product execution of a registering climate that can be utilized to introduce and run a working framework or program. VMs oversee two working frameworks: the host working framework and the visitor working framework.

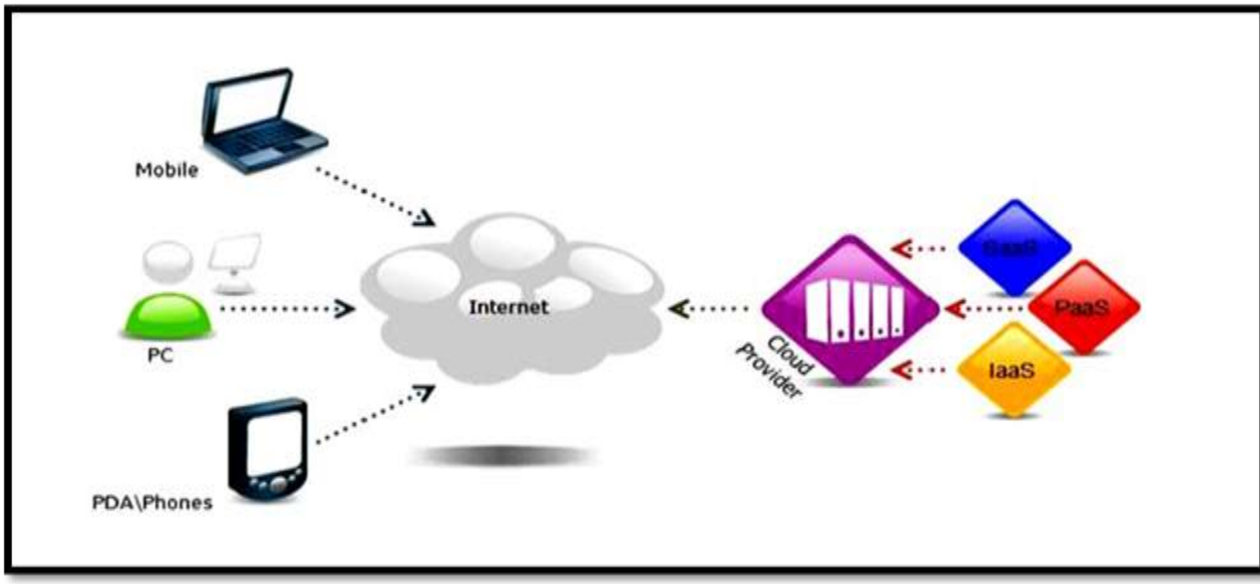

Figure-4: Cloud Computing Organization

Advantages of cloud computing

Distributed computing includes a few advantages; these advantages can be used by an individual, associations, government foundations and so on Figure 1.7 portrays the benefits of distributed computing.

Distributed computing is without a doubt the most financially savvy way of utilizing, keep up with, and redesign innovation. Utilizing distributed computing to oversee and keep up with IT frameworks could set aside cash. Maybe than buying exorbitant frameworks and hardware for the firm, it can set aside cash by using distributed computing specialist co-op abilities. It will be feasible to bring down functional expenses on account of the accompanying variables:

- System refreshes, new equipment, and programming might be covered by the agreement.
- There is at this point not a need to pay master laborers compensation.
- Costs of energy use might be diminished.
- There are diminished stand by times.

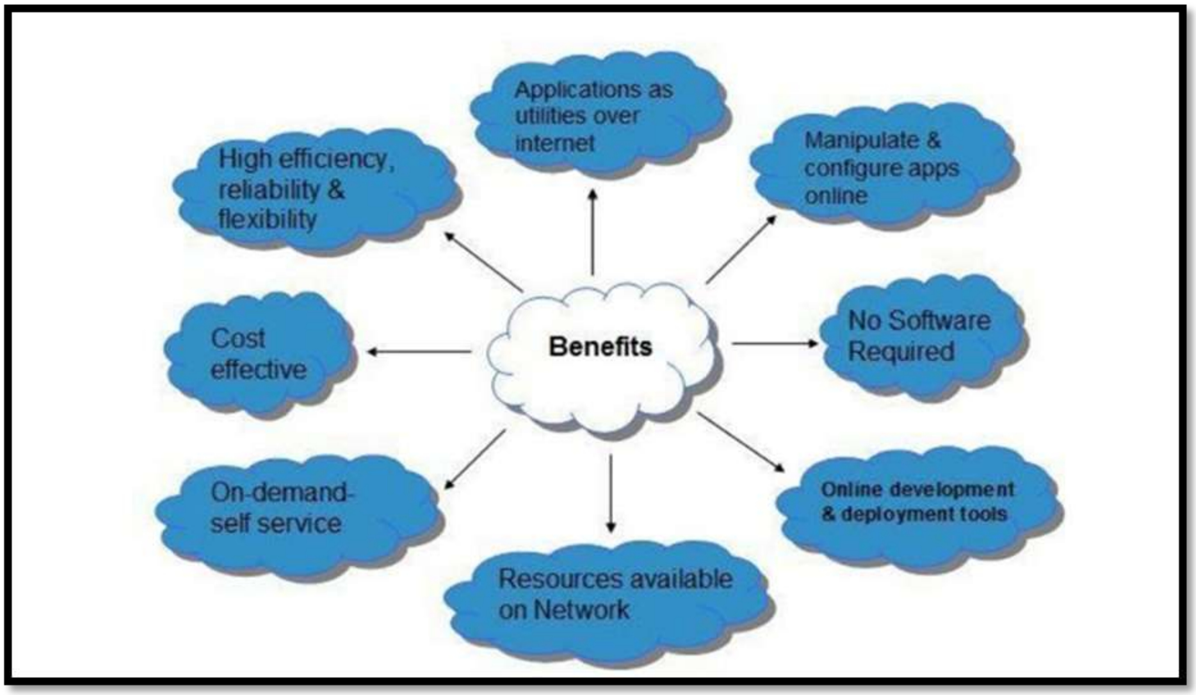

Figure-5: Cloud Computing Advantages

Virtual Storage Provides Nearly Infinite Storage Capacity: The cloud gives almost limitless capacity limit by using virtual capacity. Accordingly, there's no should be worried about running out of extra room or boosting current stockpiling limit.

Reinforcement and recuperation: Because all information is saved in the cloud, backing up and reestablishing it is more straightforward than putting away it on an actual gadget.

Programming Integration in the Cloud: In the cloud, programming combination is generally done consequently.

Simple Information Access: Once the enlistment has been finished in the cloud, it could be gotten to from any area with a web association.
At long last, and most basically, distributed computing gives the advantage of fast arrangement. Subsequent to picking this method of activity, the whole framework can be completely

functional very quickly.

RESEARCH METHODOLOGY

Research Methodology is a science that methodically conducts research or solves research problems. We can apply several applicable approaches or techniques to reach the required research objective. We have investigated and built cloud security tools and processes for the survey results solution. In this work the users, the users and the servers are developed and carried out on different levels.

Survey

We have included government interviews, cloud news, IT business news and IT companies, military companies, universities, colleges and IDCs with various IT professionals. We took into account our key aims in the questionnaire.

Data Collection

We study books, newspaper publications, direct questions, indirect questions from IT personnel, and ancient software and data bases for companies.

Framework for Design

In order to fulfill our goals, we have developed a questionnaire based on the literature study findings. In order to conclude our study questions accurately, we produced a questionnaire. We talked with our coworkers and our supervisors a lot before we finalized our questionnaire.

Targeted population

We targeted IT personnel, network administrators, system assistants, network consultants, software developers, developers, students, penetration testing personnel, network safety analysts, network and system officers, etc for this survey, following literature reviews and discussions with our colleagues.

RESULTS AND DISCUSSION

In many small, medium-sized and large organizations, cloud computing is the main driving factor. It provides an environment of development, resource allocation and restructuring when necessary, virtually for storage and networking. It meets the user's demands on demand. It facilitates "as a service" paradigm for sharable resources. The cloud provides data centres for the firm to transfer its data worldwide. It removes responsibility for maintaining your data from local nodes, and cloud also offers customizable online resources. Cloud Service Providers automatically maintain software computing resources and data. However, information is no longer controlled when it is produced quickly and is disseminated across new, agile channels of cooperation. Hence Data security has become an important issue. The key factors for cloud computing are data security issues.

Secure Dynamic Bit Standard (SDBS)

The 3-bit Secure Dynamic Bit Standard (SDBS) is 128-bit, 256-bit and 512-bit. Whenever the data provider wants to upload a data file to the cloud, a bit level is randomly selected and transformed into bytes. The master key and the session key can be generated using a random generator based on the Cloud Service Provider (CSP) byte value. The master key is encoded with the session key and it is sent to the data provider by the encoded master key and the session key. Session key is used to decrypt the main key, and to encrypt the data file the master key is utilised. In addition to the proof of ownership (PoW) provided by CSP, the encrypted data file will be sent to the Big data cloud server.When a data user wishes to download an array of data from the cloud server, after One Time Password (OTP) authentication, the CSP sends the encrypted master key and session key together with the encrypted data file to the data user. The master key is then decoded using this session key and the data file is decoded and placed in the system of the data user using the master key. SDBS is a new algorithm that contains three different standards, 8 rounds with 128-bit keys, 10 rounds with 256-bit keys, and 12 rounds with 512-bit keys. Round includes different operations such as input plain text replacement, modification and transformation into output text.

The simple text named 'S' is a four-line byte array. Each row includes Nb byte numbers, where Nb differs for the three standards. Nb is set to 4 in the Standard 128-biter, Nb is set to 8 in the

International Journal of Research in Economics and Social Sciences(IJRESS)
Available online at: http://euroasiapub.org
Vol. 9 Issue 5, May- 2019
ISSN(o): 2249-7382 | Impact Factor: 6.939 |

Standard 256-bit, and Nb is set to 16 in the Standard 512-bit.The array of input bytes shown as i_0, i_1, ⋯, i_{15} and the array of output bytes is represented by o_0, o_1, ⋯, o_{15} as shown in figure.

INPUT BYTES

i_0	i_4	i_8	i_{12}
i_1	i_5	i_9	i_{13}
i_2	i_6	i_{10}	i_{14}
i_3	i_7	i_{11}	i_{15}

STATE ARRAY

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

OUTPUT BYTES

o_0	o_4	o_8	o_{12}
o_1	o_5	o_9	o_{13}
o_2	o_6	o_{10}	o_{14}
o_3	o_7	o_{11}	o_{15}

Encryption Process

International Journal of Research in Economics and Social Sciences(IJRESS)
Available online at: http://euroasiapub.org
Vol. 9 Issue 5, May- 2019
ISSN(o): 2249-7382 | Impact Factor: 6.939 |

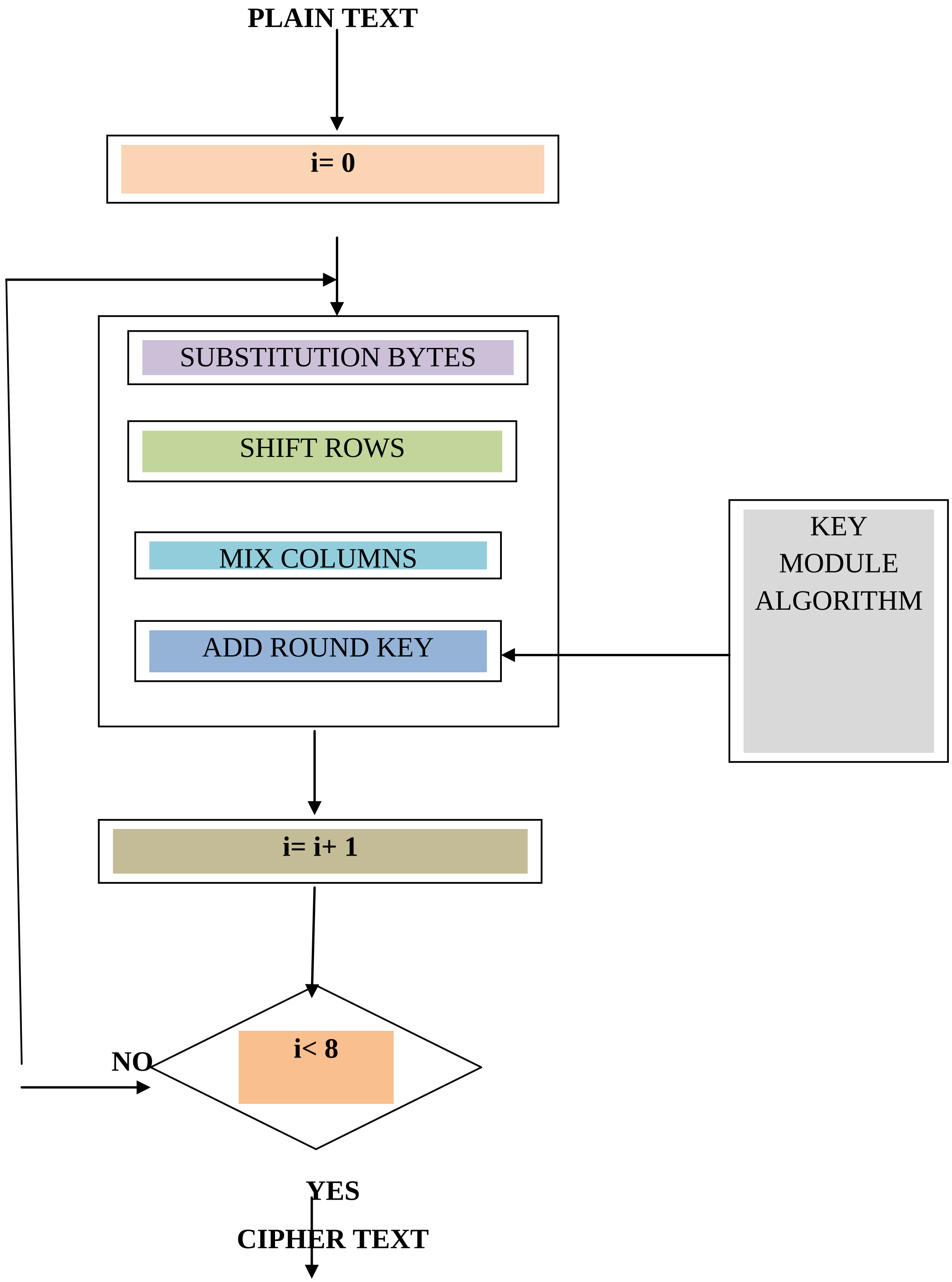

Figure-6: 128-Bit standard SDBS encryption process

Substitution bytes transformation

Byte substitution is a non-linear byte interchange that acts automatically with a substitution table called S-box on every byte of the state. The 128-bit standard replacement table is seen in Figure.

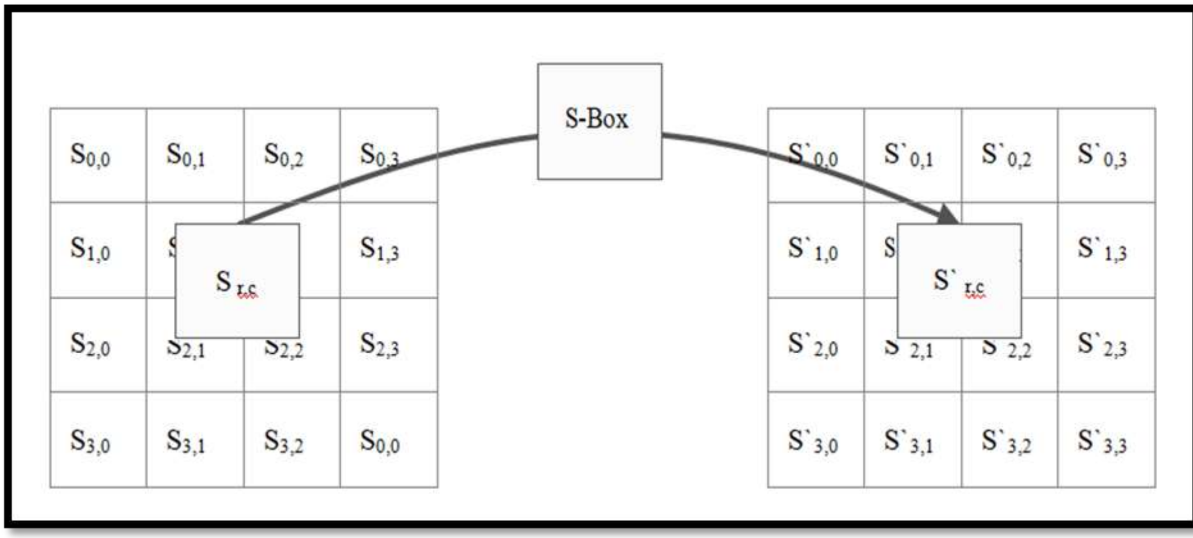

Figure-7: 128-Bit Standard Substitution Bytes

SDBS PERFORMANCE ANALYSIS

Two kinds of parameters, the encryption time and time of decryption, can examine the performance of the Secure Dynamic Bit Standard Algorithm (SDBS). Cryption time shall be the time necessary to complete a file-size encryption process and the decryption time shall be as long as required to finish the file size decryption process. Below is the current SDBS 128-bit representation of standard file-based encryption time and decryption time.

This figure illustrates how time and decryption time of the Vs file in scheme 4 is performed. The chart is made between file size and encryption time. In comparison to the other techniques scheme 1, scheme 2 and scheme 3, the time of encryption or decryption of the suggested Scheme 4 is reduced. In that technique 2.56ms were used to encrypt 1 GB of data, the 24GB data file was used to encrypt 12.1ms as well. From figure 4.15, one GB of data was decrypted with a set of 2.35ms; the 24GB data file was decrypted also with a set of 11.72ms.

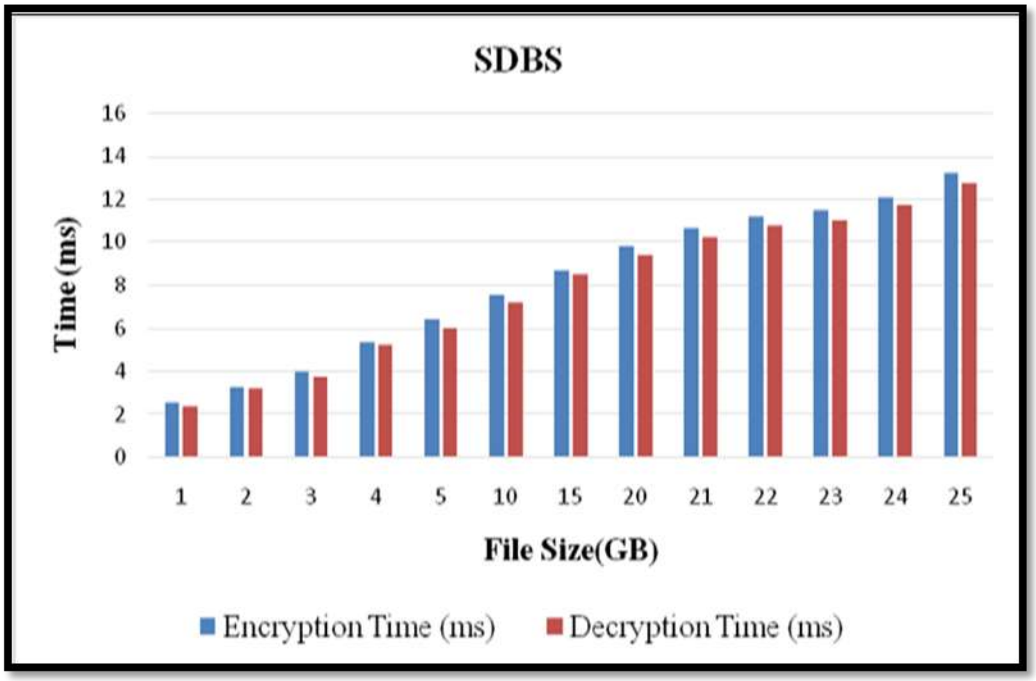

Figure-8: SDBS 128-bit performance standard scheme

Four-level security system security analysis

The proposed system of secure and safe four-level security system is explained in the security analysis. In order to secure the data file from unauthorized persons, the four tiers of security systems - authentication, authorization, encryption and decryption. Table further discusses further secrecy, integrity, efficiency and openness.The multiple security analyses performed by the proposed work are described in Table. During the registering of data access the Data Provider, Data User and CSP can be authenticated and authorized. Only the registration phase is possible when data access is not authenticated or illegitimate. No subsequent security phases can take place. Data Provider and CSP can be encrypted.

Data user and CSP can be decrypted. An unauthenticated person cannot access or download the data file, so the suggested work is treated with confidentiality. Integrity is possible because before uploading, the Data Provider can change the file.Nobody was able to alter the file after uploading the encrypted data file. Data Provider (DP), Data User (DU), and CSP are efficient in the upload and download of the suggested job. CSP's openness shows upload or downloading details. In order to prevent unauthorized users from logging into the system, CSP tries to log on unofficially. The SDBS technique provides complete security to encrypt a data file and to decrypt the Master and Session Key produced. Proposed work safety levelCompared to existing programmes such as Scheme 1, Scheme 2 and Scheme 3, the suggested Scheme 4 - SDBS algorithm provides security. Multilevel security measured in milliseconds is presented in figure, Authorization, Upload, and Download Time.

Table-1: Big data cloud security system security services

	Data Provider	**Data User**	**CSP**
Authentication	YES	YES	YES
Authorization	YES	YES	YES
Encryption	YES	NO	YES
Decryption	NO	YES	YES
PoW	YES	NO	YES
OTP	NO	YES	YES

CONCLUSION

This study proposed a secure technology for the user of huge data cloud. Only after authentication and authorization from the cloud service provider is the data file sent to the cloud (CSP). The data file is encrypted in a large data cloud environment. Only after the connection and One Time Password (OTP) submission can the authenticated and authorized user decipher data. The data provider must register in the first stage for the file to be uploaded to the big data cloud. A username, password, mail, address, telephone number and role type are required to register. After the process is completed, the data user must log in to submit the data files together with proof of ownership (PoW). The CSP gives the data user upload rights on the basis of the credentials. The data user needs to register and log in to ensure that the data file gets downloaded from the big data cloud. The data user then has to send a CSP download request and transmit the CSP OTP to the data user mail id or mobile number to accept that download request. The Data User must next offer OTP to download from big data cloud the decrypted data file if the OTP value provided is correct. The method proposed is confidential with a high level of data integrity.

REFERENCES

- Casola V, De Benedictis A, Modic J, Rak M and Villano U. "Per-administration Security SLA: a New Model for Security Management in Clouds", InEnabling Technologies: Infrastructure for Collaborative Enterprises, IEEE 25th International Conference on 2016, pp. 83-88, 2019.
- Center Of Protection Of National Infrastructure Information Security Briefing cloud-computingbriefing.pdf.
- Chaowei Yang, Qunying Huang, Zhenlong Li, Kai Liu and Fei Hu "Large Data and Cloud Computing: Innovation Opportunities and Challenges", International Journal of Digital Earth, Vol. 10, No.1, pp.15-53, 2019.

- Chase, J., Niyato, D., Wang, P., Chaisiri, S. furthermore, Ko, R. "A Scalable Approach to Joint Cyber Insurance and Security-as-a-Service Provisioning in Cloud Computing", IEEE Transactions on Dependable and Secure Computing, 2019.
- Chase, M. also, Chow, S. S. "Further developing protection and security in multi-authority characteristic based encryption", In Proceedings of the sixteenth ACM gathering on Computer and correspondences security, pp. 121-130, 2019.
- Chen, D. furthermore, Zhao, H. "Information Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering, IEEE, Vol. 1, pp. 647-651, 2019.
- Chhaya S Dule and Girijamma H. A. "Content an Insight to Security Paradigm for Big Data on Cloud: Current Trend and Research",International Journal of Electrical and Computer Engineering, ISSN: 2088-8708,Vol. 7, No. 5, pp. 2873-2882, 2019.
- Chorafas, D. N. "Distributed computing Strategies" CRC press, 2019.
- Chow, S. S. "Eliminating Escrow from Identity-Based Encryption in Public Key Cryptography–PKC", Springer Berlin Heidelberg, pp. 256-276, 2019.
- Cloud Computing Security,https://en.wikipedia.org/wiki/ Cloud_ computing_ security.
- Cloud Security Alliance "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", 2019.