Evaluation of Multifactor User Security Through Multi Authentication Verifiable Hybrid Revert Encryption for Cloud Computing Environment

J. Mohammed Ubada[1] and Dr. M. Mohamed Surputheen[2]

Jamal Mohamed College (Affiliated to Bharathidasan University), Tiruchirappalli, Tamil Nadu, India

Abstract

Cloud computing, distributed computing, and computing module with the following data, and instead of storing the data centers. The advanced cloud technology has changed is sent from the remote server to access the target data. It is used to send those programs, to calculate the cloud service provider, to run parallel processors and to run large data centers. Cloud users enjoy the environment where cloud computing provides services on demand without maintaining data in their local systems. Many security methods operate on data from the cloud, although there are some issues with reducing cloud performance. They take a long time approaching the third party system to grant permission in multi security authentication. To handle this issue, an efficient multi-factor authentication access restriction scheme has been proposed. The Multifactor Authentication Verifiable Hybrid Revert Encryption (MAVHRE) is strong authentication, the legality of providing multi-factor access to the cloud before. The proposed method is used multifactor authentication there are used OTUP, Graphical user authentication and cloud access key validation. Fist to verify the user OTUP verification before enter the cloud request. The OTUP password is verified then to authenticate user verification with help of the Graphical user authentication. This mechanism's primary key work achievement is the guarantee for both the data's privacy and security depending on OTUP and Graphical user authentication. Similarly, it also needs a user cloud for each service provider to verify anonymously to avoid malicious communication service providers. The above analysis shows that the proposed scheme is highly efficient and reduces the constitution's complexity in Cloud Computing.

Keywords:

cloud computing, authentication scheme, data's privacy and security, Multi- factor Authentication Verifiable Hybrid Revert Encryption (MAVHRE), OTUP (One Time User Password), Graphical user authentication.

1. Introduction

Authentication is the process of verifying a person's identity. Data stored in the cloud can be accessed by anyone who is not authorized to do so third-party cloud service providers, to maintain on a remote server, the form of the high risk of unauthorized access to sensitive data, has been encrypted owned and operated. When users send information or data, compromised safety to destroy data privacy and confidentiality is an important issue in a cloud computing environment. Cloud computing attracts cloud users running their scientific and complex applications, and these applications may require parallel processing to do their job effectively. If the user submitting the job unscheduled correct resources, these conditions can cause performance degradation. Scheduled completion time, completion time, processing time, scope, cost, safety, job migration, resource utilization, expected, quality of service and performance considerations very basic scheduling parameters should be Generation and performance of cloud services consistently raised the performance of the user's challenge to the cloud environment. Cloud computing provides an economical and effective solution for sharing data between cloud users at low maintenance costs. Security and confidentiality of identity data, so it is impossible to use it, and in many cases, cloud service providers are the main road of shared data protection. With no trusted cloud recurring members, Cloud service providers are aware of the interest in the change.

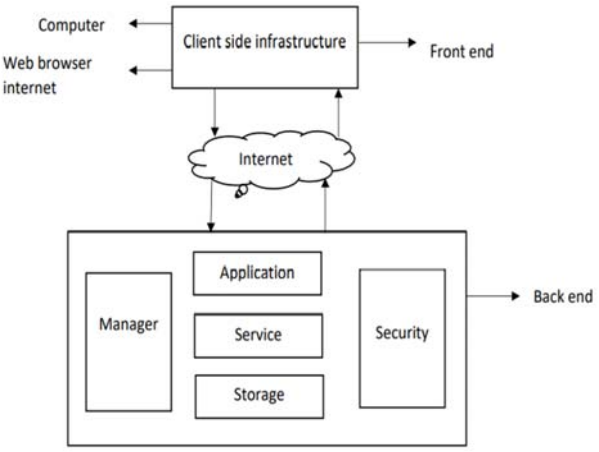

Figure 1 Cloud computing Architecture

1.1 Secret sharing and data management

Shared confidentiality is a confidential spread of technology between group participants or team members. Each role is useless; the original secret defines the secrets and is the individual role's role. If do not show the original secret, can only redeem the original secret, along with a clear number of shares in the individual shares. Increasing the amount of data on the network, sensor output storage,

Manuscript received September 5, 2022
Manuscript revised September 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.9.62

and fast fixed bandwidth and similar applications. Therefore, data availability in particular cloud storage, to maintain the quality requirements address, must meet such a device.

1.2 Privacy & security in cloud computing

Concerns about the potential other potential security vulnerabilities to be shared among resources are the potential tenant of data security and resources that are not aware of the strong legal and relational data dissemination of the problem. High data can be outsourced to this issue of security, which is especially important in sensitive applications.

In cloud computing, security, file encryption, and uploading of cloud data. By propagating the data owner, the authorization to decrypt the file and delete the user who provides access to the user. Initial encryption mode allows the user to dynamically add, delete keynote or dynamic broadcast station authentication users can access the encryption broadcast file, followed by the main broadcast. Increase the number of users and the same number of users, which will increase the cost of reducing technology.

Highly controlled, it focuses on scalable key management due to some shortcomings of encryption technology. HASBE6 (Hierarchical Attribute-Set-Based Encryption-6) user's private key encryption password-based only on text attributes, flexibility cipher text property control, and scalability-related is to provide safe access for the file-centric model to peer file sharing system.

The files are organized in groups, and the file-sharing system that has been disseminated has been studied. As the number of team members increases regularly and updates are made, it is necessary to revoke the list when dealing with key issues. Access control is difficult: these methods have many disadvantages.

1.3 Security analysis

Many issues such as privacy, data protection, privacy, authentication, and computation security are in the cloud. These are because it is not under a trusted environment control, as well as the cloud server's user data, highlights shared confidentiality, data security, and access control cloud. External access to this environment is being stored in various ways, such as enabling files to be accessed, and the dealer contents between private and cloud services are not compromised. Therefore, the secure use of cloud, encryption, and access control confidential data included in contract-based liability provides various combinations of minimal benefits; it must be a cloud service provider.

The type of secure data structure refers to outsourcing decryption keys that are allowed, cloud sharing of the basic method of the user's previous problem, and encryption of data to the owner of the data. To share data between user groups, they are at all levels (data consumers), and need fine-grained data access control in terms of user data access. Therefore, to improve the transmission of data in each user's request, the automatic attendant ensures the confidentiality of user data is to disable CSP re-encryption.

2. Related work

Cloud-Net-ready cross-country resources for task-oriented mechanisms is a cloud of fine particles that make all known send-offs possible. Cloud and Cloud Green Cloud Central Workflow Planning The distance between the joint and offload processing submissions. The Show's power, Sense model, can be effectively loaded off-road mobile device performance, and the planning program can be upgraded to a regular remote cloud protocol class [1].
Vendors unload algorithm was first proposed as a multi-factor computing uninstall decision problem, such as non-cooperative games. After the exact analysis of the game development's potential structural features, there will be at least a pure Nash equilibrium strategy. Fully distributed network equipment vendors unload algorithm fully distributed computing environment based on machine learning techniques [2].

An analysis of the game's structural characteristics and the game appears to allow Nash equilibrium and improved limited property rights. And design the unloading of distributed computing algorithms, Nash equilibrium can be achieved, deriving the upper bound convergence time, two important aspects of the performance metric, and the centralized quantum efficiency [3].
Jointly decided to optimize the computing for all users and allocate communication resources and unloads, they minimize the energy for all users and calculate the overall cost of latency. The optimization problem, in general, will be specified as a non-convex quadratic constraint secondary program, which is an NP problem. Effectively used access points are determined to optimize binary communication resources and no-load settings in the case of semi-transparent slack, which is inseparable from the calculation [4].

Typical optimization, energy consumption, and the total cost of reducing the maximum waiting time between computing users, allocating computing and communication resources together are offloading all users. The joint optimization problem is formulated as a mixed-integer design. This problem can be restarted within a second. Usually, NP-hard constrained quadratic programming [5].
Given the proximity of many users to the same computing task, which is likely to require a reasonable allocation of task strategies, response delay tasks can be significantly reduced. Encourages the adoption of personal design, effective missions, strategies, future calculations, time, tasks, calculation requests, preservation and same-source money [6].

The encryption is based on an attribute encryption method and a subset of the access strategy for general content data sets. Therefore, the gateway matches and verifies that it only keeps the attributes of a sufficient number of partial cipher texts; it is maintained. So the digest data that can be obtained can be decoded. The construction has several advantages. To encrypt the digest data's content by multiple encryptions by different entities and provide fine-grained access [7]. Therefore, challenges remain to be addressed to maximize the number of multi-factor energysaving device uninstall scenarios. All devices that can offload the task to gain a favorable radical realize the maximum energy savings and unloading equipment useful for the number of groups [8].

In data access, collaboration and sharing of data by different users can thus achieve remarkable production efficiency. Security solutions focus on identity verification, and the implementation of user's data cannot be deprived of unauthorized access. Still, they challenge cloud servers and ignore users' sensitive privacy issues to other request users [9]. However, from access points/base stations, radio resources limit the data stream MCC (Mobile Cloud Computing) suffers from the poor quality multi-factor Quality of Service (QoS) in multi-service situations such as long buffer times and intermittent interruptions. Back off-based Wireless Resource scheduling (BWR) program, which is higher than non-real-time real-time business service priority. BWR can improve the mobile cloud's overall performance with real-time streaming and network QoS [10].

To generate a dynamic search and dynamic search, save on the cloud server token query encrypted file, find the data owner and encryption. Once the token is received, the server can retain the encrypted data while performing a privacy search. Different, single-user mode, multifactor secret cryptography dynamic search cloud search, concentrated on many previous works [11].

A Heuristic Offloading Decision Algorithm (HODA) decides jointly optimized semidistributed and unload and communication, computing resources to maximize the system's utility. The contribution to the sub problem is to reduce the proof NP-modular and maximization problems whose hardness is decomposed into two sub problems: the computing and communication resource optimization solution quasi-convex determined by (1) Solved by and convex optimization, and (2) a subset of unimodular optimized functions [12].

A system environment developed using three main entities allows to trust third parties, data owners, and users. The sharing power concept is developed for the system's authentication protocol privacy protection shared access to multiple users. Not only for security and privacy issues, for example, to achieve authentication of shared access, has the user's privacy allowed the user only to access their data fields using the access request matching mechanism [13].

Local Cloud Resources there are many user situations, some sharing devices. Centralization and decentralization: A new clustering algorithm, with the management function divided into two layers. Strategic compromise with distributed intelligence distribution is faster, more focused, and optimal for more complex decisions [14].

Characterized designed to optimize the tradeoff between latency problems cloud across multiple nodes and communications operations. This question has a pair of NP-hard concepts that choose to drive while nodes and delay collaboration, proper resource allocation heterogeneous multi-user services, and service computation algorithms [15].

Distributed computing provides multiple choices is a local non-cooperative game model for multi-user computing. The goal of the game is that the best configuration of profits is to achieve each user. Incorporate the profit of the media delivery time for users, the cost of development, and the impact of energy costs for cost accounting. After that, analyze the calculation offload decision problem that shows that the game theory in the game, reach the Nash equilibrium [16].

The data owners are encrypted before they left the final last again. Deduplication technology is mainly used by several cloud backup suppliers and various cloud services such as transceiver boxes. However, the encrypted data cannot be de-duplicated; it is a pseudo-random. Deduplication is a technique for de-duplicating data within a specific set of data. Other copies of the same data left by copying them in memory will be deleted [17].

However, most of the existing homomorphic encryption schemes are single-user, which means that they can only be performed by ciphertext evaluation of public-key cryptography. Binders can be evaluated as homomorphic encryption, re-encryption, and ciphertext can be evaluated by multi-user BGN users by homomorphic encryption method. This program is a bit homomorphic, bilinear pairing, and can perform infinite multiplication and addition grouping based on decision problems [18].

In cloud integration, computing, security issues, such as confidentiality and user rights data, and an important factor in mobile cloud computing development is displayed in mobile computing cloud computing systems. Cloud Computing system is based on a three-layer structure change encryption with a layered attribute correction layered access control method [19] to provide a secure and reliable operation. However, this assumption does not apply to large-scale mobile cloud applications. By computing, offload to execute applications competing by these cloud resources, a part of the cloud can be scheduled to be delayed for a large number of users. It does not consider user partition; it may be delayed when a cloud in the schedule has a decrease in significant performance. Rather, it is the minimum completion time tracking application for each user to achieve a minimum average completion time for all

users even more, based on the number of resources in the cloud [20]

3. Implementation of the proposed method

Multifactor authentication is using two or more measures to enhance the user authentication process in the cloud. Verify user identity Access the computer Authenticated. For entities authenticated by Multi-Factor Authentication Verifiable Hybrid Revert Encryption (MAVHRE) Method in the cloud computing environment, the multi-factor authentication method needs to be the fastest, light, and secure. Computing resource sharing and the availability cloud is a big revolution. Users need to access the service for identity verification in the cloud. As such, certificates are one of the key challenges in cloud computing environments. In many applications, multiple users participate in doing things. A proposed method to used multifactor authentication details based OTUP, Graphical user authentication and cloud access key validation to solve the security problem of maintaining cloud-based data storage authentication protocol without affecting the user's personal information. It is used for data sharing cloud servers, which cannot reveal the user's need to challenge the request itself. The algorithm's confidentiality is used to identify the new privacy challenge of cloud multi-factor data storage between challenging users. The privacy of the address, but it does not matter if it gets access.

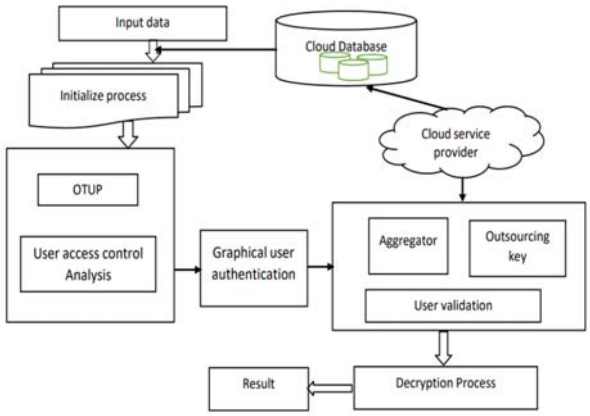

Figure 2 Proposed multi authentication Block diagram

Sharing permissions through the applicable mechanism and authentication protocols to enable privacy-related user access requests, make secret visits to the request. Policy-enabled ciphertext may allow the user to access the properties of temporary access control applications, shared data across multiple users, access to unique data fields, re-encryption, and adoption agents. This process of the proposed MAVHRE method, shown in figure 2.

3.1 Initialize process

The data can be verified by outsourcing pre-processing initialization data inspection data in the form of valid data. In this pre-processing stage, a cloud authentication request and response environment are provided to provide security. Further, at the initialization time, the Result Decryption Process Cloud Database Initialize process Cloud service provider Graphical user authentication User validation Outsourcing key Aggregator User access control Analysis OTUP Input data data check is made by originality without any noise and copied data. Instruct the huge data level to order pre-processing as a record and reduce the dimensionality of the original data.

Algorithm: Service level set up pre-processing
Input: user request
Output: Authentication of data using Multifactor security (OTP, Fingerprint or non-numeric
validation)
Step 1: input data Rd;
For each rd (recordset Rs)
Check is Empty==NULL
Fill attribute Ac==nill to Rd
End for
Step 2: check distinct data Dt
For each attribute Dti in the data set
While (mismatch attribute (Ac) == Rd)
Remove record set from rd
Do
End for
Step 3: check numeric and non-numeric validated attributes fields
If Rd is a numeric attribute
Then hold discretize or eliminate the attribute;
If Rd is a non-numeric attribute, then
Hold Values rd
Else
Remove the non-matched noise value
End if
End if
Step 4: keep raw data originate all fill case record fields
Step 5: create a cloud environment CE req/res
If (req==valid)
{
Proceed CE get access else till reject
} end if
Step 6: Verify the cloud authenticate CE

After that, all attributes' concern is to fill in the situation or data to check whether it is empty. It verifies that the unstructured data is an effective form of the noisy file containing no noise data removal process at any other point in the unstructured file. The above algorithm disinfectant is used to clean the original data's noise and original data

without outliers forming different values and setting the cloud environment (CE).

3.2 Multi-Factor Authentication based OTUP Verifiable

The proposed multifactor authentication level access restriction and the service level dynamic OTUP generation plan carry out access restriction. For each service, this proposed method uses different OTUP generation schemes according to the requested service. The generation of OTUP is based that provides and manipulates restrictions for service access at the contract level.

Algorithm Steps
Input: User Request $UUrr$
Output: OTUP

Step1: Read input dataset Rd, service s

Step2: Identify the service s= Rd. service

If s. Type = Forget then

Hint

$\int_{i=1}^{size(Rd)} s(i)$.User == s. user && Hint H

Send Rd to User U

Hint Result R = Receive Hint answer from the user U

$\int_{i=1}^{size(Rd)} s(i)$.User == s. user && Hint Answer HA= = H

Then

Send OTUP to User

End

The generation of OTUP has been implemented according to different business types. For any service request, its type has been determined. Based on this type, the method generates an OTUP for the user that has been used to authenticate the user

3.3 Multi-Factor Authentication based Graphical User Authentication Verifiable

Multi-Factor Authentication based Graphical User Authentication Verifiable work on user already given password is compared with matching the original and predefined passwords. Using a graphical password system, user verify the hidden passwords images rather than type alphanumeric characters.
Algorithm Steps:
Input: User Request $UUrr$
Output: Graphical User Authentication
Step1: The number of images represented N as $nn1, nn2, nn3, \dots . nnnn$
Step2: P represented the number of registration password images required.
Step3: The system presents a set of images N and user U has click already registered password $rrpp$
Step4: The server S shows set of images with hidden $rrpp$ and check S as it done in the given $rrpp$ data.
Step5: User U has enter the Hint Result (Password) R as on each image.
Step6: The authentication server compare the enter R is as password stored in the database. R new ($rrpp$) == R old ($rrpp$) If it is true login successful.
Step7: Algorithm for password recovery phase.
If user U lost password it is recovered enter the mail M on the recover page$rrcc$.
Server matches the M id same as it entered in the registration M id new == M id old it is true server immediately sent the interned user U.
User verification password usage clues, click points, graphical password schemes, including security assessments of usability and memo capabilities. In the hidden password registered with click-based graphic password, the image pixel provides the database to load the image, and then gives access to all data in the database for authentication

3.4. Hybrid Revert Encryption (MAVHRE)

At this stage, the key is ready for data security encryption options through the integrated data owner. The security and user level of a service's public key data can be understood by the service selection private key associated with the GNU data. Frame update session data generated after this time is session-based. This implementation provides a private key that maximizes the number of golden layer units based on a formula and a number multiplied by the verification. Use plain text or glossy text, with block size data of 0 to 1 number size and some n values. Here's a simplified way to encode in multiple modules. Each block must be less than the number of binary values(b). Session time encryption is a multiplication phenomenon, which means that the plaintext of the product multiplied by the dwarf finds the ticker text output.

Algorithm steps
Input: data sd, time slot T
Output: output encrypted text
Start
Step 1. Random prime number P and Q is used to generate max value
Step 2 two-factor key used to encrypt the data
If (the prime and multifactor p ≠ q such that. p & q) key-value
{
Generate on multi session key Sk
Compute n= p × q;
} end if
Step 3. The encrypt data size compute
If (d(n) = (p-1) (q-1).) factors of exp value e
{
Int value be chosen 1<e Ps as e
User A possess the message m to encrypt B A
Update on key T Ps
}
Step 4. The message at the regular interval [0, nA − 1].
Select a random integer k , 1 < k < nA,such that gcd(k, nA)) = 1.
if (c1 = k eA mod nA.) and (c2 = meA k mod nA)
{
Return on state session T
}

End if
End if
Stop

Overtime security is choice-semantics protection against blank attacks, efficient extension-state encryption of sessions, and solving key leak issues for some security properties.

4. Result and discussion

The resulting secure MAVHRE gives a standard implementation done with encryption, decryption, and audit status profiling test parameters. The proposed framework will be used to assess existing schemes to address cloud security and privacy issues. The implementation was carried out through JAVA with MySql server authentication. The resultant given below shows the performance of proposed security proves the higher efficiency

Table 1 implementation parameter used in the proposed method

Processed Parameter	Value processed
Service levels	5
Type of data	Data files
Number of users	3000
Service provider	CSP

In table 1 above, the defined values and security analysis parameters of the proposed process. The efficiency of public audits was assessed, using either generated or not submitted for review by a third-party auditor to confirm proper access to the Master Key Policy. The proposed MAVHRE (Multi-factor Authentication Verifiable Hybrid Revert Encryption) compare with the previous Time-based One-time Passwords (TOTP), Hierarchical Sensitive Support (HSS), Authentication Role-based access control (ARRBAC), service level trust weight (SLTW), Multi-Level Legitimate Access Weight (MLAW).

Table 2 public auditing analysis

Methods/users	public auditing	efficiency	In %			
Users	TOTP	HSS	ARRBAC	SLTW	MLAW	MAVHRE
100	54	58.97	62.54	65.87	73.87	77.75
200	57.87	65.87	69.65	72.65	78.94	82.65
300	64.76	71.65	73.76	75.76	81.64	88.95

Above table 2 defines the key authentication verification of public auditing proficiency with different methods; the proposed MAVHRE system 88.95% efficient than the TOTP is 64.76%, HSS is 71.65%, ARRBAC is 73.76%, SLTW is 75.76%, MLAW is 81.64%. A security assessment is the verification of a security certificate's integrity with access given the right to encrypt and decrypt to provide security services

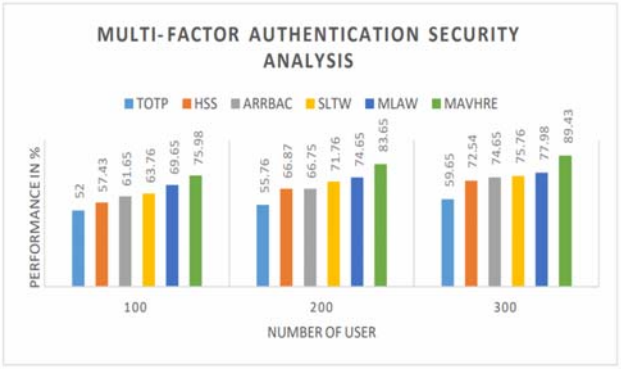

Figure 3 Multi-Factor Authentication Security Level

Figure 3 defines cloud multi-factor authentication security levels for encryption and decryption of security processes. Configure each service to provide the proposed verification measures to improve security compared to other traditional methods in 89.4%.

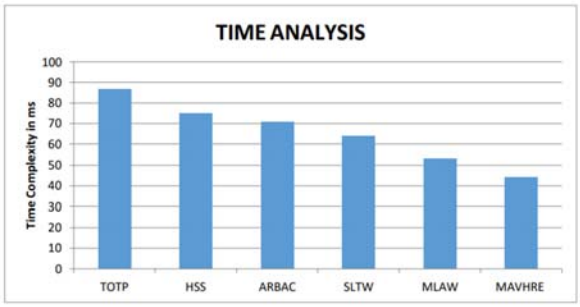

Figure 4 Time analysis

Figure 4 defined complex policies during various conventional methods to produce corresponding effects; apparently, other methods are more complex to manufacture and proposed over time.

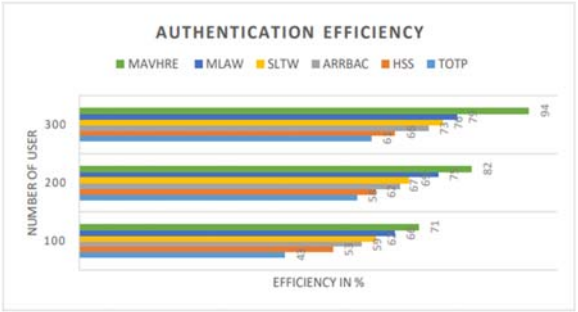

Figure 5 Authentication Efficiency

Figure 5 shows data authentication efficiency. Other programs are more susceptible to several security

vulnerabilities when users send sensitive data to the cloud, which means they cannot provide a user name that may be missing. The program does not provide data confidentiality. Therefore, it is clear that certification authentication can be higher to provide better protection.

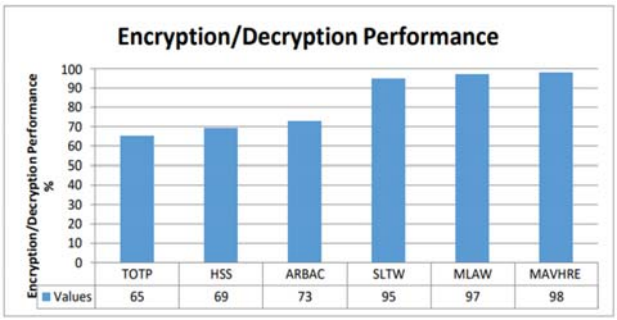

Figure 6: Performance in Encryption / Decryption

The encryption and decryption efficiency is measured and plotted in Figure 6. The MLAW algorithm achieved higher performance apart from other methods.

5. Conclusion

Cloud security is a set of strategic technology and security control data, applications, and cloud-related infrastructure. The technology of current cloud innovation provides unlimited access to cloud server-linked security. The public / private key combination here is encrypted to protect the need to use the data. OTUP, Graphical user authentication and cloud access key validation provide enhanced security in the cloud, improving cloud computing security using cloud consumers and cloud providers, merged through multi-level encryption. It protects, store, retrieve, process, and access cloud data while others. In this proposed method, MAVHRE implementation parameter analysis compare to all other existing methods will high efficiency and security. The proposed MAVHRE to give public auditing analysis is 88.95%, multi-factor security analysis is 89.43%, time analysis is 44 ms, authentication efficiency is 94%, performance in encryption / decryption is 98%. In future work authentication for cloud computing using face recognition is based on security based to data access and cloud database in a cloud. Face Recognition System in the cloud computing. It gives good security to the cloud environment to provide service to the user or access the data or service.

References

[1] Shichao Guan, E. De Grande, Azzedine Boukerche, Robson "A Task-centric Mobile Cloudbased System to Enable Energy-aware Efficient Offloading 2018 IEEE Transactions On Sustainable Computing, pp - (1-14).

[2] Huijin Cao and Jun Ca "Distributed Multiuser Computation Offloading for Cloudlet-Based Mobile Cloud Computing: A Game-Theoretic Machine Learning Approach" IEEE Transactions On Vehicular Technology, Vol. 67, No. 1, January 2018, pp - (752-764).

[3] Lei Jiao, Wenzhong Li, ACM, and Xiaoming Fu, Xu Chen "Efficient Multi-User Computation Offloading for Mobile-Edge Cloud Computing"2015 IEEE/ACM Transactions On Networking, pp - (1-14).

[4] Ben Liang, Min Dong, Meng-Hsi Chen "Multi-user Multi-task Offloading and Resource Allocation in Mobile Cloud Systems" 2018 IEEE, pp- (1-16).

[5] Min Dong, Ben Liang, Meng-Hsi Chen" Resource Sharing of a Computing Access Point for Multi-user Mobile Cloud Offloading with Delay Constraints" 2018 IEEE Transactions on Mobile Computing, pp - (1-14).

[6] Limin Han, Weiwei Chen "Time-efficient Task Caching Strategy for Multi-server Mobile Edge Cloud Computing" IEEE 2019, pp - (1429-1436).

[7] Maryline Laurent, Nesrine Kaaniche "Privacy-preserving Multi-user Encrypted Access Control Scheme for Cloud-assisted IoT applications" 2018 IEEE 11th International Conference on Cloud Computing, pp - (590-597).

[8] Zhikai Kuang, Songtao Guo, Jingpei Dan Yawei Shi "Multi-user Offloading Game Strategy in OFDMA Mobile Cloud Computing System "2019 IEEE Transactions on Vehicular Technology, pp - (1-12).

[9] Huansheng Ning, Hong Liu, and Laurence T. Yang, Qingxu Xiong "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing" IEEE 2013, pp - (1-11).

[10] Xing Liu, Yun Li Hsiao-Hwa Chen "Wireless Resource Scheduling Based on Backoff for Multiuser Multi-service Mobile Cloud computing" 2015 IEEE Transactions on Vehicular Technology, pp - (1-13).

[11] Yaqiong Chen, Yousheng Zhou, Wenjun Luo, "Dynamic Searchable Encryption with MultiUser Private Search for Cloud Computing"2015 IEEE International Conference on Computer and Information Technology, pp - (176-182).

[12] Hui Tian, Cigdem Sengul Xinchen Lyu, Ping Zhang "Multi-User Joint Task Offloading and Resources Optimization in Proximate Clouds " 2016 IEEE Transactions on Vehicular Technology, pp - (1-13).

[13] Mrs.Vaishali Sahare, Ms.Neha Mahakalkar "Implementation of Re-encryption Based Security Mechanism to Authenticate Shared Access in Cloud Computing "International Conference on Trends in Electronics and Informatics ICEI 2017, pp - (547-550).

[14] Emilio Calvanese Strinati, and Sergio Barbarossa Jessica Oueis "Distributed Mobile Cloud Computing: A Multiuser Clustering Solution " IEEE ICC 2016 SAC Cloud Communications and Networking, pp - (1-6).

[15] Wei-Ho Chung, Ai-Chun Pang, and Junshan Zhang, Te-Chuan Chiu, "Latency-Driven Cooperative Task Computing in Multi-User Fog-Radio Access Networks" 2017 IEEE 37th International Conference on Distributed Computing Systems, pp - (615-624).

[16] Chengcheng Cai, Qin An Qin, Wang, Yiyang Ni "Game Theoretical Multi-User Computation Offloading for Mobile-Edge Cloud

Computing" 2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), pp - (328-332).
[17] S. Malande, Kirti Ashokrao Tayade, G. "Survey Paper on a Secure and Authorized Deduplication Scheme using Hybrid Cloud Approach for Multimedia Data" International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS2017), pp - (2966-2969).
[18] Xi'an, Zhang Wei, "A BGN-type multi-user homomorphic encryption scheme "2015 International Conference on Intelligent Networking and Collaborative Systems, pp - (268- 271).
[19] Hong Wen, Bin Wu, Yuanpeng Xie, and Jiaxiao Meng, Yixin Jiang "A Modified Hierarchical Attribute-Based Encryption Access Control Method for Mobile Cloud Computing" Journal Of Latex Class Files, Vol. 13, No. 9, September 2014, pp - (1-9).
[20] Jiannong Cao, Hui Cheng, Lei Yang, and Yusheng Ji "Multi-user Computation Partitioning for Latency Sensitive Mobile Cloud Applications" IEEE Transaction On Computers, October 2013, pp - (1-14).
[21] https://cloudscomputing.net/cloud-architecture

Mohammed Ubada. J completed B.Sc Computer Science in 2011. In 2014 received the MCA degree from Bharathidasan University, Tiruchirappalli. Serving as a Communication Trainer in Jamal Mohamed College from 2015 till date.

Dr. M. MOHAMED SURPUTHEEN received the M.Sc. Mathematics degree, from Madurai Kamaraj University, Madurai, India in 1986 and receive P.G.D.C.A., Degree from Bharathidasan University, Trichy in 1988 and M.Phil in Computer Science Degree from Regional Engineering College (NIT), Trichy, in 1996. Completed Ph.D. in Computer Science from M.G.R. University, Chennai, in 2014 A committed and qualified Associate professor with over thirty-three years of experience at leading Indian Academic Institution “Jamal Mohamed College” affiliated with Bharathidasan University from 1988 till now for teaching students from heterogeneous backgrounds. Also, serving as a Controller of Examinations from 2018 till date