Nat. Volatiles & Essent. Oils, 2021; 8(5): 6825 - 6839

NVEO
Natural Volatiles & Essential Oils

Two Factor Security Mechanism using Biometric Based Un-locker in Cloud Computing

Dr. Jameel Ahmad Qurashi
Assistant Professor
SCSS Jaipur National University
Jaipur
jameelqureshi41@gmail.com

Neha Alwani
M.Tech(CSE) student
Jaipur National University
Jaipur
nehaalwani98@gmail.com

***Abstract*—**This paper talks about the risks with the current security techniques that were prior utilized for the cloud framework and presents a novel feature with an idea of biometric confirmation and named as 'Biometric-based Un-locker'. As bio-metrics entities are exceptionally unique in this way, it will be awesome and practical answer for the cloud. The performance of this proposed method is examined by producing a cloud environment and carrying out it utilizing the .NET structure on five distinctive datasets. The outcomes are determined with the both attackers and normal users and execution are examined dependent on Time, Size of Data after Encryption, and Authentication Rate.

Keywords- *Biometric based Un-locker, Security Technique, Encryption.*

I. INTRODUCTION

Web is these days turning into the need of people and with its expanding request, the new advancements that utilization the web are on-request, Cloud registering is one of them as its services embraced by a few organizations and just as by numerous people as said by Arshad et al. [3]. The conversation on the issues of the cloud isn't done generally however its growth rate is expanding step by step. The principle justification for these expanding questions is its interest, use, cost, and a tremendous measure of data that makes an issue of safety, security, privacy, reliability, anonymity, liability, and it's capacity.

Cloud environment requires their security strategies on the grounds that the customary security approaches which were intended for different advancements are not fit to Cloud as its design isn't equivalent to different conditions because of its multitenant nature, resource sharing, information location, and protection prerequisite. The other separating factor is the idea of virtualization which is added to the cloud environment for performance improvement. The security issue is a significant issue that needs more consideration because of the quick development of the cloud advancements talked about by Gunasekhar et al. [4]. The fundamental inquiry emerges here is about the prerequisite of safety that can be replied with some investigation. Thus, the profound investigation of the various models of the Cloud is accomplished for various regions like, Cloud architecture, its portability and interoperability, data in the business centre, application security, identity, and access management, and encryption and key management.

The above all else attributes are its intricate architecture as contrast with different architecture on the grounds that here a few processing ideas and innovations are consolidated, for example, Virtualization, Web 2.0, Service Oriented Architecture (SOA), and other business applications that store data and software on the servers. The other attribute of the cloud is resource pooling and because of the centralized information, cloud providers need to focus in on the security resource to ensure its assets and secure its architecture. The second most significant trademark pondered by Winkler [5] is its standardization where it lacks and due to this it is hard to choose the policies for Cloud to secure services or utilization through Cloud VMware.

In this way, to manage these security issues there is a need to foster a design or structure that deals with the issues of safety. In the following areas, the conversations on a portion of the existed security instruments are done and afterward another structure for the cloud framework is proposed and examined the experimentation result on some

experimentation. This proposed architecture depends on biometrics where fingerprint modality is utilized and the performance is examined based on various components.

II. Background and Literature Survey

This section manages the security system that was utilized for giving security while putting away information on cloud servers and proposed a clever methodology for this. The following areas incorporate distinctive security techniques that were selected in the cloud by various creators, proposed FragSecure Framework, its execution on the nearby cloud climate, and execution examination dependent on schedule, size, and information loss.

In this work, five unique datasets are gathered and transferred on the cloud worker. Table 1 gives the subtleties of all datasets like the absolute number of records, sort of documents, and the complete size of information to be uploaded.

Table 1: Dataset Details

Datasets	Total Number of Files	No. of Image Files	No. of Text Files	No. of Audio Files	Size of Data (in KB)
Dataset-1	100	40	44	16	138683
Dataset-2	150	60	64	26	144895
Dataset-3	200	80	92	28	151127
Dataset-4	250	100	114	36	220468
Dataset-5	300	120	136	44	289810

All the above datasets are uploaded on the cloud server by different users and two different cloud environments. The details of the cloud environment are as given in Table 2.

Table 2: Different Cloud Environments

Cloud Platform	No. of Data-centres	Total Storage in GB	Framework Used	Key Generation Algorithm
3	1	100	Generic framework	RSA with ECC
4	1	100	RandFrag Framework [1]	RSA with ECC
5	1	100	FragSecure Framework	RSA with ECC

A. *RandFrag Framework:*

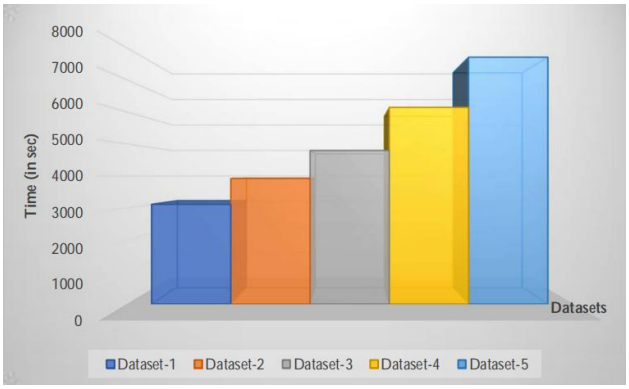
This system is only the execution of the current fragmentation scheme with a hybrid encryption algorithm. In paper [1], secure cloud architecture is created where information is partitioned into pieces and afterward each section is encoded utilizing a couple of keys produced at the

customer end for mark and unscrambling and other pair is created for file block identifier to actually take a look at the integrity of the data. This framework gives security however because of fragmentation data loss is there on the grounds that the kind of information may not be something very similar for every client and afterward here fragmentation expands the dangers of data loss.

To dissect the performance of this RandFrag Framework, five distinct datasets were transferred by various cloud users, and estimation is done dependent on various boundaries.

Time*:* As information will be transferred on the server after encryption in this way, time taken by the cloud environment can be determined to break down the impact of the technique on the cloud environment. Here Figure 1 portrays that the Dataset-5 took additional time as contrast with other datasets as it contains an enormous number of files than other datasets. Thus, unmistakably the time taken by the information for transferring is expanded with the expansion in the quantity of files.

Figure 1: Total Time (Cloud Environment-4)



It has been seen that by and large, there is a 20% expansion in time with the expansion of 50 files into the existed data.

Size: The size of data might be expanded after encryption. Here in Environment-4, the size of all the five datasets has been expanded with an average of 0.11% with the expansion of 50 files into the existed data set. Figure 2 shows the original size of the data document before transferred on the server and the size after encryption.

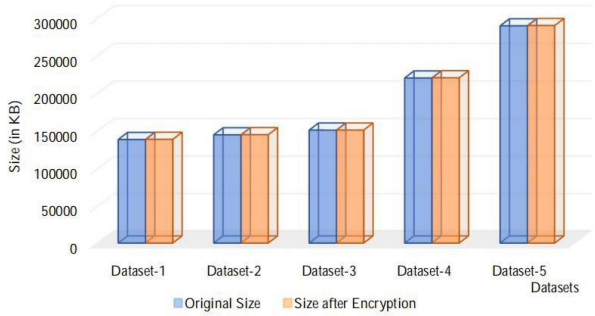


Figure 2: Size of Data after Encryption (Cloud Environment-4)

Data Loss: The determined Data Loss utilizing Cloud Environment-4 is as portrayed in Figure 3. As displayed in figure it is clear data loss doesn't continuously increment with the size of data, it relies upon the framework utilized.

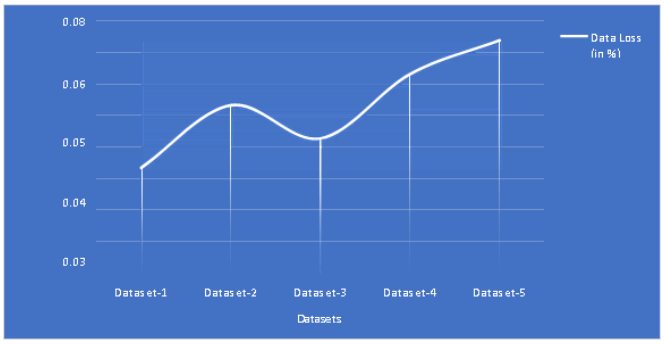


Figure 3: Data Loss (Cloud Environment-4)

B. *Efficient FragSecure Framework:*

In this high level period of technology, the utilization of Cloud comes to on its statures and the prerequisite of safety is builds step by step because of the increment in security breaks. Numerous specialists work on something similar and give various structures and designs to security. To manage this security and data loss issue, novel architecture design is proposed for a cloud climate where information is divided dependent on information type, size, and different boundaries, and each divided square is encrypted utilizing a hybrid encryption calculation.

The point by point plan of this proposed framework is as displayed in figure 4. In this system originally input information is sent to the cloud server by a client/user of the cloud. Data might be of text type, picture type, or sound data. This data is when gotten by a cloud server then first it is gone through fragment module where fragmentation models (F.C.) are checked for each kind of file and as needs be information will be divided into 'n' quantities of sections. Then, at that point, each part is encoded utilizing a hybrid encryption module. These encoded sections are then planned with the various servers situated at various areas.

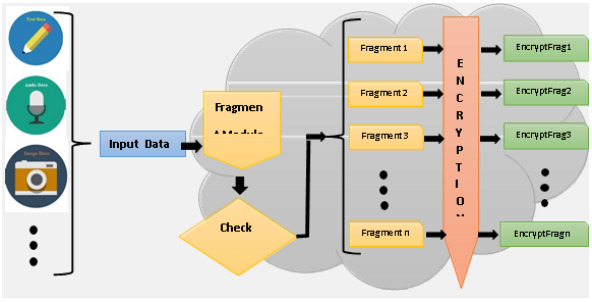


Figure 4: Proposed FragSecure Framework

In this work, two modules assume a significant part (I) Fragment Module and (2) Encryption Module. The detailed description of these modules is as given underneath:

1) ***Fragment Module:*** Fragmentation is the fundamental concern and, in this work, the principle centre is drawn around this module. Here first the sort of data is checked means data is a picture, sound, or text type on the grounds that each kind of information has various properties. Besides, the size of the data file is additionally checked in light of the fact that it likewise influences the performance of the fragmentation module.

2) ***Encryption Module:*** The principle focal point of this module is to encrypt each divided block and store these blocks on various workers alongside its ID numbers. Here for encryption, a hybrid algorithm is utilized where a mix of RSA and ECC is utilized as a hybrid [2]. The performance of this mix gives better security as investigated.

To examine the performance of this FragSecure, five unique datasets were transferred by various cloud users, and estimation is done dependent on various parameters.

***Time**:* As data will be transferred on the server after encryption thus, time taken by the cloud environment can be determined to dissect the impact of the method on the cloud environment. Here Figure 5 portrays that the Dataset-5 took additional time as contrast with other datasets as it contains an enormous number of records than other datasets. In this way, plainly the time taken by the information for transferring is expanded with the expansion in the quantity of files.

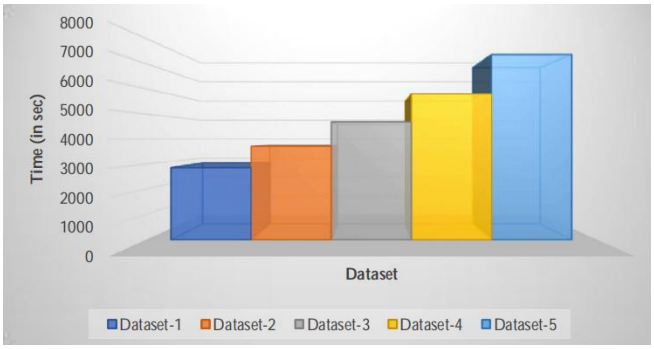


Figure 5: Total Time (Cloud Environment-5)

It has been seen that all things considered, there is a 21% expansion in time with the expansion of 50 files into the existed data.

Size: The size of information might be expanded after encryption. Here in Environment-5, the size of all the five datasets has been expanded with an average of 0.02% with the expansion of 50 records into the existed data set. Figure 6 shows the original size of the data file before transferred/uploaded on the server and the size after encryption.

Figure 6: Size of Data after Encryption (Cloud Environment-5)

Data Loss: The determined Data Loss utilizing Cloud Environment-5 is as portrayed in Figure 7. As displayed in figure obviously data loss doesn't continuously increment with the size of information, it relies upon the framework utilized.

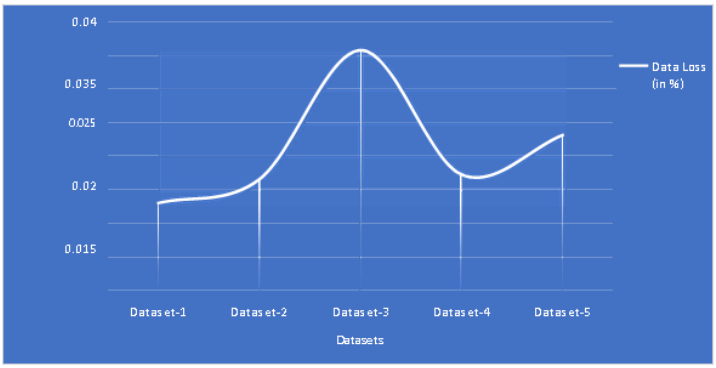


Figure 7: Data Loss (Cloud Environment-5)

In this section, a productive system for fragmentation and security is proposed. This system is proposed to accomplish the destinations to lessen data loss during fragmentation and give high-end security. For fragmentation, a part module is created which chooses the quantity of pieces and size of sections dependent on the original size of the data and for encryption, hybrid RSA and ECC algorithm is utilized which give double encryption of the data. To dissect the performance of this proposed system, five datasets of various sort of files are transferred to the local cloud climate with three unique framework and results are determined as far as time, size and information loss and reasons that the performance of this proposed effective FragSecure system is superior to the existed system where random fragmentation mechanism is utilized alongside a similar encryption mechanism. This proposed approach assists with diminishing the storage time just as storage necessities by lessening the size of encoded information with the least data loss.

III. Security in Cloud-Based Systems

Clouds are cost-effective and flexible and all the data is geographically disseminated over the network and everything is straightforwardly controlled by Cloud. To give security to the client's data is the most difficult task since resources are vulnerable to stealing, harm, or compromise. In this way, the chances of revealing data are increased and it must be secured by guaranteeing security.

Subashini and Kavitha[6] characterized that few associations enjoy a ton of advantages in the wake of taking on cloud computing however these days the hurdle in the method of innovation are seen and these are security issues and it has a place just with the serviced providers as it's just their obligation to deal with data, overseeing data, and secure information by giving it protection. To give security to the cloud architecture and forestall information loss and control, another framework is executed on cloud storage and the utilization of information as talked about by Waseem et al. [7]. They additionally talked about that the cloud environment with secure environment will brings about the decrease of the harm on physical devices too. The other significance of safety is the critical changes in the Cost and works on the performance by reducing harm to data, software , and hardware portrayed by Khorshed et al. [8].

This shows that the requirement for a security model in the cloud to adapt to adaptability and trust prerequisites as portrayed by Clay comb and Nicoll [9]. Resource pooling is the fundamental task of cloud computing and different users access it for putting away their information so it needs management and faces some security issues.

These days the vast majority of the organizations moved their various undertakings to the cloud environment and to utilize cloud structure, they utilize their data, identities, and framework. Jaatun et al. [10] and Hajra et al. [11] talked about that the organizations should need to trust the providers and have some level of control so to check cloud processes and different events. The essential mechanisms utilized for confirmation and trust the management are information security, access control, event management, and compliance. The other fundamental mechanisms utilized for security are encryption, authentication, authorization, and data privacy. A portion of the classifications for cloud security mechanisms are as displayed in Figure 8:

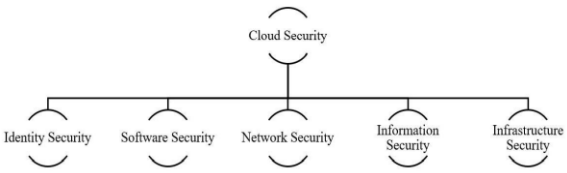


Figure 8: Categories of Security in Cloud Computing

A. *Identity Security:*

The term characterizes that this mechanism assists with empowering security while getting to the data from the cloud and it permits the individual to get to the information provided that their personality coordinated. In this manner it will assist the people with getting to the resources for the ideal choices as said by Hajra et al. [11]. Data and Application integrity and confidentiality are guaranteed by this. The procedures dependent on this technique give start to finish the management of the identity, services related to with outsider validation is deliberated by Sharma et al. [12]. This guarantees the capacities possess by it and users can make profit of these components and services without any problem.

B. *Software Security:*

These days with the improvement of a wide scope of software, it is hard to deal with them as far as extension since it requires assurances for security and there is no such strategy that will give 100% confirmation of security. In this way, the goal is to construct/make software with abilities of safety to secure against attacks.

C. *Information Security:*

It is characterized by Sehgal et al. [13] that the protection of the data whether it is digital or non-digital and discover the dangers brought about by various policies, processes, and tools. Different business processes can be set up with this with the obligation of the security of information and keep up with it in the manner it as of now implies whether in the transmission stage or storage stage.

Infrastructure Security:

The primary challenge in the cloud isn't just to secure the data, however infrastructure security is additionally a fundamental step and it can be a difficult challenging task because of tremendous number of physical and virtual machines. Outsider/Third Party based techniques might assist with keeping it from unauthorized access yet at the same time it is a critical step and needs security.

D. *Network Security:*

The most well-known necessity of the Cloud is the network security which incorporates both software and physical based safety efforts. In this insurance of the infrastructure, its abuse, alteration, malfunctioning, and any improper disclosure is incorporated and different security instruments were executed yet, the preventive measure required.

IV. Simulation Setup

A Web-based Cloud Environment is produced for simulation where clients can make accounts and transfer information according to their necessities. Information uploading on cloud is performed with various security stages to investigate the performance of various methods. In this work, five distinct datasets are gathered and uploaded on the cloud server. Table 3 gives the subtleties of all datasets like the total number of files, type of files, and the total size of data to be uploaded.

Table 3: Dataset Details

Dataset No	Total Number of Files	No. of Image Files	No. of Text Files	No. of Audio Files	Size of Data (in kb)
1	100	40	44	16	138683
2	150	60	64	26	144895
3	200	80	92	28	151127
4	250	100	114	36	220468
5	300	120	136	44	289810

All the above datasets are uploaded on the cloud server by different users and two different cloud environments. The details of the cloud environment are as given in Table 4.

Table 4: Different Cloud Environments

Cloud Platform	Number of Data-canters	Total Storage in GB	Framework Used	Security Algorithm
1	1	100	FragSecure Framework	RSA with ECC
2	1	100	Two-Factor Data Security	Biometric-based Unlocker

In the given table, both the fragmentation are frameworks based yet in the second stage two-factor information security-based methodology is utilized where a biometric trait is utilized for verification to improve the level of security. The subtleties of the proposed approach are clarified in the following areas.

V. Performance Metrics

A. *Time Analysis:*

Time can be estimated for taking care of each record on the server. Here Time can be portrayed as a period taken to store data on the server. Moreover, the total time can be dictated by including the hour of all documents that are taken care of on the server.

B. *Size:*

In this size of the data after encryption is calculated and compared.

C. *Authentication Rate:*

It is one of the safety measures that characterize the authenticity of the cloud model and furthermore show the amount it is secure to use for putting away data. The more authentication rate addresses the protection of information.

VI. Proposed Cloud Storage System

The proposed cloud framework is planned and carried out utilizing .Net Platform and by producing local Cloud Environment. This proposed Cloud Storage architecture has three fundamental stages named as: (a) Initial Phase, (b) Input Phase, (c) Output, and Shared Phase. Every one of the three stages assume a significant part in this architecture and incorporate a few modules. The subtleties of these stages are as given beneath in Figure 9

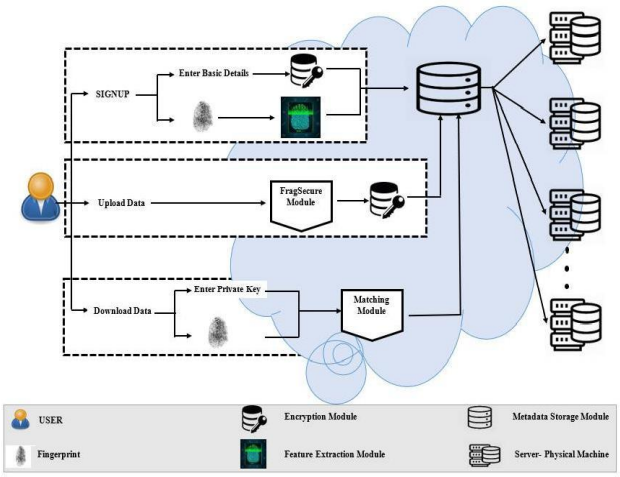


Figure 9: Proposed Cloud Storage System

Phase 1: Initial Phase

The most importantly period of this System is to make a record on the cloud portal. In this, the client can make a record by tapping on the signup link and entering its basic details and uploading fingerprint. For this work, the picture document of the finger impression test is utilized however ongoing clients can transfer finger impression utilizing a finger impression sensor. These essential subtleties are scrambled and afterward put away in the information base over the cloud. Clients will get an ID after registration and connected to the metadata.

Phase 2: Input Phase

The second significant stage, where the client transfers their information on the cloud framework. In this structure, information isn't straightforwardly transferred, it initially passed to the FragSecure module where information is isolated into fragments and afterward encrypted using Hybrid RSA and ECC based algorithm. Encrypted fragments are put away on the server and connected with the
metadata using ordering/indexing. User can transfer 'n' number of files and it may be of various types. For the examination of this work, the data collection/set of picture, audio, and test is used.

Phase 3: Output or Shared Phase

This is the last stage of this proposed framework where the end user can download their information or shared data. Data must be downloaded if the private key and finger impression of the end user are coordinated with the data set as characterized in two-factor based mechanism. The coordinating with module assists with decryption of data and join all the fragments. The performance of this proposed
framework is examined using diverse datasets and measures are determined in the following area.

A. Proposed Two Factor Data Security Mechanism Using Biometric Based Un- Locker:

The two-factor information security mechanism is extremely popular these days where authors use encryption systems and some outside devices to upgrade the level of safety. In conventional frameworks, user transfer their information which is first encoded and keeping in mind that
downloading it the private key is utilized for decryption reason however here in two-factor information security mechanism information isn't decoded until it gets verified utilizing the tool (possibly some hardware) which results with high level security yet the utilization of this external
tools prompts expansion in the expense for both the tools(device) and its upkeep/maintenance. This builds the load on the end users to deal with the device and in the case of loss or losing an additional expense should be paid. In this way, there is a need to grow a mechanismc312 that gives security also cost-effective which can be accomplished utilizing biometric properties.

Biometric attributes are known for its unique components and its security. Thus, rather than utilizing the hardware or any outside tools assuming biometrics will turn into the piece of cloud framework, it assists with keeping up with the level of safety with no additional expense or load on the clients. The biometric attributes like face, finger impression, and audio will be added to this system for opening data. These days, everybody has a cell phone, PCs, or work areas accessible with cameras, finger impression sensors, and mike facilities. Thus, it is an exceptionally simple interaction to incorporate face discovery, or finger impression detection, or voice identification as a security un-locker rather than any outer/external tools. In this proposed work, a unique finger impression based validation
framework is added to the cloud structure alongside the FragSecure framework proposed by Narang et al. [14]. For the expansion of this unique finger impression-based validation framework cloud needs to keep up with data for finger impression qualities and creates metadata for the equivalent alongside the information uploaded by the end user. The procedure of the two-factor information security mechanism is as displayed in figure 10. From the figure it is understandable that the information uploaded by the end user is downloaded just when both the key and the biometric attribute coordinated with the database of the cloud. This two-factor instrument has two principle factors: (a) Master Key, and (b) Biometric Entity.

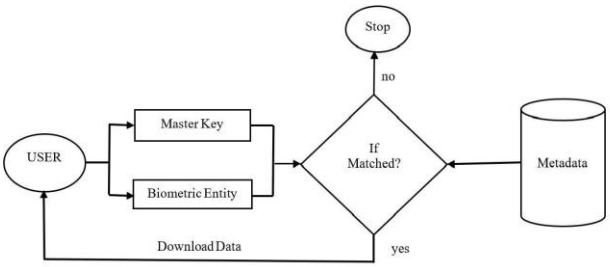


Figure 10: Two-factor authentication to Download Data

a. Master Key

This master key is the master private key which produces the 'n'- private keys for 'n'-parts. In this work FragSecure Framework proposed by Narang et al. [14] is utilized to get information while transferring on the cloud server. This system works dependent on two unique modules, (I) Fragment module: used to segment information dependent on its type and size and (ii) Encryption Module: used to encode each piece using hybrid RSA and ECC proposed by Narang et al. [15]. The private key of each section is tie together and an master key is created which then, at that point used for the downloading of the information.

The master key algorithm is utilized to separate the information into 'n' number of sections and afterward encode each part. The encoded sections are then put away on the cloud server and the master key is created. The master key is created when the end user needs to download the data/information and afterward it is sent to the end user's enlisted email ID.

b. Biometric Entity

The second key factor of this model is the biometric unit. The end user can't download information with the master key information is downloaded just when both the master key and biometric unit will be the input element for downloading. Here, the finger impression quality is utilized as a biometric substance, and the unique finger impression-based authentication/recognition framework is utilized for second-factor verification. The finger impression is the most secure attribute for biometric-based frameworks because of its uniqueness. This attribute is also cost effective because no additional expense spent on the sensors, these days the majority of the devices/systems have inbuilt sensors for finger impression catching. For this proposed work, the finger impression is caught at the time of enrolment and the featuring of the qualities are saved at the cloud data base. A similar unique finger impression should be the contribution at the time of downloading the information in any case client will be treated as forged and will not ready to get to/download information. The unique finger mark-based authentication framework in the cloud is as displayed in Figure 11 characterizes the various parts of this module. These stages are: (I) Pre- preparing phase, (ii) Segmentation phase, and (iii) Feature Extraction Phase.

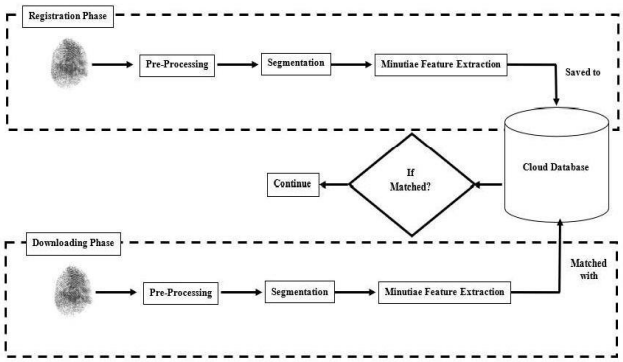


Figure 11: Fingerprint Authentication Module Phase

Phase 1: Pre-processing

Pre-processing is a major stage of any identification system that directly-indirectly improves the consequences of the identification system. In this stage the nature of the input test is improved using the filtration procedure. As the examples are obtained utilizing sensors and afterward sent to the cloud system so there is a more possibility of external noise in the examples and to diminishes, these noise filters are needed in the field of the identification system. For this work, the median filter is utilized to smooth the gained test and eliminate the noise.

Phase 2: Segmentation

Segmentation is the second major stage of the identification system. This will assist with examining the example from each part as in this example is deteriorated into an alternate number of portions and afterward plan for a next level. Here, discrete wavelet-based disintegration is utilized which changes alongside the rows and afterward alongside columns and proceeds till 2- levels.

Phase 3: Feature Extraction

In this stage, various elements of the biometric characteristics are removed. In this work, for each section details features are removed which characterized the edge bifurcation or edge finishing on a finger impression.

All the removed features are then put away into the cloud data set/ database and it will use for confirmation when the end user needs to download their data/information.

B. Experimentation & Result Analysis:

The execution of this proposed architecture is examined with the execution of Cloud Environment alongside the storage features. For this, the local cloud design is produced using the .NET platform where end user can transfer sound, text, and picture data. In this environment, the client can make their cloud accounts and store their information of any size however the greatest space accessible to clients is 10 GB.For this experimentation, the cloud account of 50 clients was made and that end users had the option to upload just three distinct sorts of information files that are: (I) Text (.txt), (ii) Image (.jpg, .png or some other picture configuration), and (iii) audio file (.wav or .mp3). For the investigation of execution diverse execution measurements are viewed as like, Time, Size of Data after encryption, and authentication

rate. The principle objective is here to further develop the authentication rate for original end users and secure information from establish end users.

Datasets Used: The investigation of the proposed architecture is finished utilizing five distinct datasets where ten unique end users have transferred their information on this cloud design. The subtleties of the dataset like, the total number of files, the details of the type of files, and the size of total files are as given in Table 3. These documents are transferred by 50 distinct end users and in this; end users can likewise impart their information to certain limitations.

Result Analysis: The experimentation results for this system are determined dependent on various boundaries by transferring the above-characterized datasets. These presentation factors characterize and dissect the exhibition of both security and calculation properties.

Total Time: Time can be estimated for putting away each document/file on the server. This boundary influences the performance of the cloud as far as speed since, in such a case that the time of putting away information will build then the exhibition of the cloud will be moderately lethargic. Here Time can be characterized as a period taken to store information on the server. Additionally, the all out time can be determined by summation of the time taken by the system to transfer all records on the server.

The total time taken by different dataset to upload on cloud is as given in Table5.

Table 5: Total Time for Storing Data on Cloud Server

Datasets	Total Number of Files	Size of Data (in KB)	Total Time (in a sec)
Dataset-1	100	138683	2267
Dataset-2	150	144895	3315
Dataset-3	200	151127	4465
Dataset-4	250	220468	5473
Dataset-5	300	289810	6772

The time factor likewise relies upon the quantity of records and the size of data/information. As displayed in Figure 12, the total time taken to transfer dataset-2 is 31.6% more than the Dataset-1 and if compares with the Dataset-5, it expanded by 66.5% from Dataset-1.

Figure 12: Total Time is taken for uploading different datasets

Size of Encrypted Data: However the size of the data/information will be expanded after encryption the expanded rate ought not be high as it will devour more space and straightforwardly builds the heap on the server. Table 6 gives the subtleties of the size of data/information previously, after the encryption.

Table 6: Size of Original and Encrypted Data

Datasets	Total Number of Files	Size of Data (in KB)	Size of Data (in KB)- After Encryption
Dataset-1	100	138683	138886.2
Dataset-2	150	144895	145073.2
Dataset-3	200	151127	151284
Dataset-4	250	220468	220666.4
Dataset-5	300	289810	290012.9

The size of information after encryption is expanded by some rate as displayed in Figure 13. It shows that the percentage expansion in data/information size is diminished with the increment of the quantity/number of files. For instance, the Dataset-5 which contains300 files their size after encryption is expanded by 0.07% though, for 100 files, the size of encoded data is expanded by 0.15%.

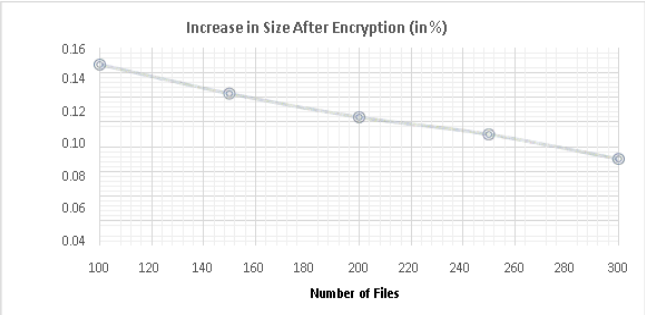


Figure 13: Increase in the size of Data after Encryption

Authentication Rate: Security of the cloud can be examined through the rate of authentication which decides the insurance of the information against the assailants. For this examination, the authentication rate is determined utilizing the proposed cloud framework. For this testing reason, 50 distinctive record for end user is made, while making a account finger impression is taken from the end user. In this work, finger impression picture information is utilized for every individual and when the end user needs to
download information it is utilized for confirmation. The examination of authentication is finished by downloading of information in light of the fact that while downloading an information client needs to present his finger impression. To test this verification a few presumptions are likewise taken in this work and these are:

Assumption 1: an attacker may be attacked through the network using malicious nodes
Assumption 2: cloud account of a user is hacked by fake user/Attacker (40% chances)
Assumption 3: the account linked with cloud account is also hacked by the attacker (20% chances)

Table:7 tells about the data uploaded by which user and downloaded by which user for 10 users and whether they are successful in downloading the data or not.

Table 7: Authentication Details

File Uploaded By	File Downloaded by	Download Successful/ Unsuccessful
user1	user 1	Successful
user2	Fake	Unsuccessful

user3	user 3	Successful
user4	Fake	Unsuccessful
user5	user 5	Successful
user6	user 6	Successful
user7	Fake	Unsuccessful
user8	user 8	Successful
user9	user 9	Successful
user10	user 10	Successful

As the above outcomes, the phony user is consistently failed in downloading the information in light of the fact that while downloading an information unique finger impression of the user is required which he/she transfers at the time of the enlistment of his/her record.

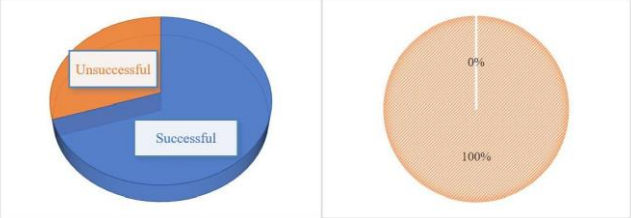


Figure 14: (a) Successful and Unsuccessful Attempts (b) Authentication Rate

The finger impression is a unique trait and can't be forged. So, in each attempt, the phony user is failed as shown in Figure 14 (a).

In light of these outcomes, the authentication rate is determined as displayed in Figure 14 (b). For this work, the Authentication rate is determined uniquely for the validation to download information which is 100% by utilizing Biometrics based Security Unlocker.

VII. Comparative Analysis

To think about and investigate the exhibition of various cloud framework with and without fragmentation and security in cloud computing various boundaries are utilized. These are:

Time Analysis: Testing has been accomplished for all the cloud conditions on five distinctive datasets that contain the diverse number of a picture, text, and sound/audio files and Total Time for storing data/information on the server is as given in Table 8:

Table 8: Total Time (in sec)

	Cloud Platform-1	**Cloud Platform-2**
Dataset-1	2868	2267
Dataset-2	3723	3315
Dataset-3	4687	4465
Dataset-4	5793	5473
Dataset-5	7355	6772

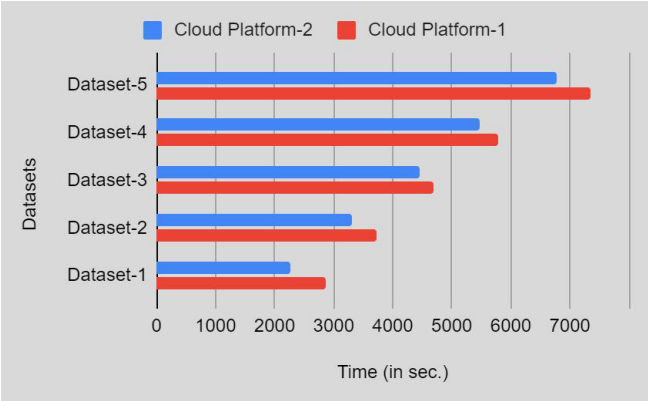


Figure 15: Total Time (for Different Cloud Environments)

The above Figure 15 shows that the time taken by Cloud Platform-2 where two-factor authentications dependent on biometrics are utilized is lesser as contrast with any remaining conditions for all the datasets. As indicated by examination, obviously the performance of Cloud Environment-2 where the Two-factor authentication mechanism is utilized is better and it requires 10% lesser time than Environment-1.

Size: In this size of the information after encryption is determined and thought about. Testing has been accomplished for all the cloud conditions on five diverse datasets that contain an alternate number of pictures, text, and sound/audio files. The size after encryption is given in Table 9:

Table 9: Size (in KB)

	Cloud Platform-1	**Cloud Platform-2**
Dataset-1	138701	138886.2
Dataset-2	144919	145073.2
Dataset-3	151181	151284
Dataset-4	220506	220666.4
Dataset-5	289877	290012.9

Figure 16 shows that the size after encryption of the data is nearly similar in each environment for all the datasets.

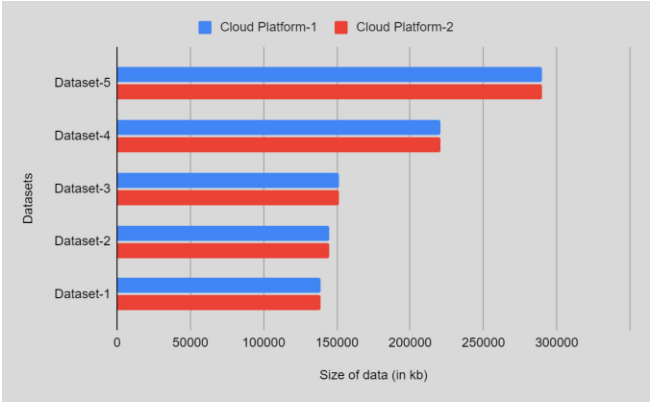


Figure 16: *Size after Encryption (for Different Cloud Environments)*

VIII. Conclusion

In this work, the Biometric based Security procedure is executed for two factor-based verification where finger impression methodology and crossover encryption calculation are utilized. To investigate the exhibition of this proposed design execution is done and different parameters are determined with various experimentation where information transferring and downloading are performed. For a security perspective, the first information is divided

and encoded utilizing the FragSecure Module and afterward authentication is checked and coordinated with dependent on finger impression gave. The outcomes show the viability of the proposed cloud design and give an exactness of 100% to the recognizable proof of phony and genuine users.

REFERENCES

[1] Ahmed, F. Q., & Mohammed, A. S. (2018). Enhancing The Data Security In Cloud Computing By Using New Encryption Method. *Qalaai Zanist Scientific Journal,3*(1), 1011-1021.

[2] Enhancing the Data Security In Cloud Computing By Using New Encryption Method. (2018). *Qalaai Zanist Scientific Journal, 3*(1).

[3] Arshad, J., Townend, P., Xu, J., & Jie, W. (2012). Cloud Computing Security: Opportunities and Pitfalls. *International Journal of Grid and High Performance Computing (IJGHPC), 4*(1), 52-66.

[4] Gunasekhar, T., Rao, K., Kiran, P., Reddy, V., & Rao, B. (2019). Security Architecture of Cloud Computing. In *Detection and Mitigation of Insider Attacks in a Cloud Infrastructure: Emerging Research and Opportunities* 1-11.

[5] Winkler, V. J. (2011). Securing the Cloud: Key Strategies and Best Practices. *Securing the Cloud*, 153 185.

[6] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1-11.

[7] Waseem, M., Lakhan, A., & Jamali, I. A. (2016). Data Security of Mobile Cloud Computing on Cloud Server. *OALib*, *03*(04),1-11.

[8] Khorshed, M. T., Ali, A. S., & Wasimi, S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems*, *28*(6),833-851.

[9] Claycomb, W. R., & Nicoll, A. (2012). Insider Threats to Cloud Computing: Directions for New Research Challenges. *2012 IEEE 36th Annual Computer Software and Applications Conference,*387-394.

[10] Jaatun, M. G., Zhao, G., & Rong, C. (2009). First International Conference, CloudCom 2009. In *Cloud Computing, 1-707.*

[11] Hajra, S., Rebeiro, C., Bhasin, S., Bajaj, G., Sharma, S., Guilley, S., & Mukhopadhyay, D. (2014). DRECON: DPA Resistant Encryption by Construction. *Progress in Cryptology- AFRICACRYPT 2014 Lecture Notes in Computer Science*,420-439.

[12] Sharma, D. H., Dhote, C., & Potey, M. M. (2016). Identity and Access Management as Security-as-a-Service from Clouds. *Procedia Computer Science*, *79*,170-174.

[13] Sehgal, N. K., Bhatt, P. C. P., & Acken, J. M. (2019). Additional Security Considerations for Cloud. *Cloud Computing with Security*,193-215.

[14] Narang, A., Gupta, D., & Kaur, A. (2019). Efficient FragSecure Framework for Data Security and Fragmentation in Cloud Computing. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, *8*(7), 1011-1016.

[15] Narang, A., & Gupta, D. (2018). In International Conference on cyber security and privacy in communication networks (ICCS-2018). Jaipur, Rajasthan: ELSEVIER-SSRN Digital Library.