



Improving cloud data security through hybrid verification technique based on biometrics and encryption system

Md. Alamgir Hossain & Md. Abdullah Al Hasan

To cite this article: Md. Alamgir Hossain & Md. Abdullah Al Hasan (2020): Improving cloud data security through hybrid verification technique based on biometrics and encryption system, International Journal of Computers and Applications, DOI: [10.1080/1206212X.2020.1809177](https://doi.org/10.1080/1206212X.2020.1809177)

To link to this article: <https://doi.org/10.1080/1206212X.2020.1809177>



Published online: 24 Aug 2020.



Submit your article to this journal [↗](#)





View related articles [↗](#)



View Crossmark data [↗](#)



Improving cloud data security through hybrid verification technique based on biometrics and encryption system

Md. Alamgir Hossain ^a and Md. Abdullah Al Hasan ^b

^aDepartment of Computer Science and Engineering, Prime University, Dhaka, Bangladesh; ^bBangladesh-Japan Information Technology, Dhaka, Bangladesh

ABSTRACT

Cloud computing is a unique network or environment where access, maintenance and process can be done from any part of the world. It is a customized internet-based computer server. It is a current trend of modern technology. For the massive computational power, it is the best option for storing data. There is no uncertainty that Cloud Data Server offers quick and solid types of assistance to its customers. When data is storing in the cloud storage the most important thing comes is the security of data. So, in recent years, cloud security is so much important issue because of the increasing of data. For the security of cloud computing, in this research, a hybrid verification technique is made which is based on biometric and encryption systems. In order to achieve strong and secure technique, this work use fingerprint as biometric technique and advanced encryption standard as a trustworthy encryption system. The primary goal of this paper is to avert information access from cloud information stockpiling focuses by unapproved clients. This new data security system can provide efficient authentication of cloud computing.

ARTICLE HISTORY

Received 22 June 2020
Accepted 7 August 2020

KEYWORDS

Cloud computing; cloud data security; cloud security; biometrics; encryption; fingerprint; OTP; ROI; AES algorithm

1. Introduction

These days calculation over cloud computing has become a typical thing for the vast majority of the applications. As the capacity on nearby circles is problematic sometimes, cloud-based capacity is pulling in everybody to store information on the cloud which can be available all over the place. Cloud computing qualifies asset clumsy customers to fathom their gigantic computational remaining tasks at hand through a cloud server that gives overwhelming computational force and it is likewise more affordable [1]. The quantity of people putting away their information on cloud expands step by step, so the security level should be in an updated way since when specific information is transferred to the cloud the data is straightforward to two gatherings. One is cloud administrations and the cloud director. It enables the clients to share assets, similar to programming, information framework on interest. It is noticed that the ongoing model for registering and associated issues like capacity, process, and programming. Data security and privacy is the biggest issues for cloud computing [2,3]. In all processing stages together with, uploading, processing, storing data must be secured. In cloud data storage center users can store their huge amount of data. There is a big chance our data may be hacked when it is present in one's server [4,5]. In order to build our data secured in cloud platform the best idea is that, to provide more applicable verification technique. Here, this system is improved the security of data by using biometric verification technique with secure encryption method. The fingerprint is the most widely and oldest biometric modality for human identification and advanced encryption standard (AES) is most reliable

algorithm. Encryption is the process of moving the original plain-text into non-readable format. In computer science and engineering, specifically, biometric is utilized as a type of personality get to the board and access control. When we compare other symmetric security system, it has been seen that hybrid model biometric system gives more advantage.

1.1. Motivation

Cloud computing has turned into the following enormous thing. Organizations, for example, Google, Amazon are effectively publicizing the utilization of these items. More customers are starting to end up mindful of the advantage of this innovation and how this could be used to further their potential benefit. Cloud computing offers simple entry since the majority of the assets can be promptly accessible on request. Consumers can quickly send their applications to the cloud and do not need to oversee physical servers which are taken care of by the cloud specialist organizations [6,7]. Clients can store their enormous measure of information in cloud information stockpiling focuses. Be that as it may, numerous customers are not prepared to execute distributed computing in light of the absence of legitimate security control approach and shortcoming in the assurance of information which prompts a major test for the cloud computing suppliers. The issue that influences the believed integrity of receiving the cloud is validation [8]. Altogether, to make our information verified in the cloud stage the best thought is to give increasingly fitting check framework. Cryptography is the science and craft of mystery composing that

it cannot frame without imagination activities with innovative ability [4,5]. It examines some scientific methods and gives components important to give angles identified with data security like privacy, information trustworthiness, substance verification, and information birthplace validation. Generally, the utilization of biometric gadgets has improved our capacity to give validated access to physical establishments. Biometrics is the utilization of an individual's extraordinary physiological, social, and morphological trademark to give constructive individual ID. Biometric frameworks that are as of now accessible today inspect fingerprints, impressions, iris, and retina examples, and face [9,10]. Frameworks that are near biometrics, however, are not delegated such conduct frameworks, for example, voice, mark, and keystroke frameworks. The test examples of social not parts of the body [11]. Throughout the following couple of years, the utilization of biometrics will proceed to develop and turn out to be significantly more ordinary. Cryptography does not make preparations for the vulnerabilities and dangers that rise up out of the poor plan of frameworks, conventions, and methods. These should be fixed through a legitimate plan and setting up of a cautious foundation [12–14]. Udendhran [15] proposed novel encryption and decryption method that fulfills information classification and honesty. This paper utilizes Homomorphic encryption and location-based decoding as two distinct procedures to give information security in distributed storage. The encryption procedure depends on Homomorphic encryption and decoding depends on the client area. Since the system is totally location-based, so its a problem. Selvarani and Malarvizhi [16] execute a multimodal biometric framework by utilizing a key for encryption and unscrambling of information in the cloud condition. As it is the situation with most innovation fueled frameworks, the biometric recognizable proof has its very own arrangement of favorable circumstances and burdens. In any case, it generally relies upon a specific use case that it will be increasingly worthwhile or disadvantageous whenever conveyed. Much of the time, utilizing biometric distinguishing proof has demonstrated to be progressively helpful over the long haul. As increasingly more biometric frameworks are sent, they are required to turn out to be significantly less expensive with expanded creation and economy of scale [17–19]. Also, with progressions in innovation and security, numerous inconveniences of biometric frameworks are relied upon to stop to exist like satirizing, ace fingerprints, and so forth. To counteract the information accessible from the cloud by unapproved clients and upgrade the security, we proposed a half and half confirmation framework dependent on biometric and encryption framework. This new information security framework can give productive validation of cloud computing.

1.2. Specific objectives

The issue that influences the believed integrity of embracing the cloud is verification. This issue can be deeply limited by methods for actualizing a cross-breed check framework. In such framework, we are consolidating two techniques for the well-being of the biometric layout utilized in biometric confirmation for validation with the assistance of AES. While login after the main enrollment a similar rule is pursued that is, from purchaser side biometric format is given as info then it is contrasted and

the put away biometric test that takes on enlistment time. An encryption framework utilized with the biometric confirmation for expanding proficiency and reliability. To arrive at the objective, this investigation will be completed with the accompanying explicit objectives:

- Only biometric layouts are not unreasonably much secure. In our proposed model, we built up a component for the exceptionally secure biometric layout by methods joining biometric formats and encryption framework in both client side just as cloud server-side.
- Hybrid confirmation framework dependent on biometric and encryption gives preferable execution over individual biometric check and encryption framework for legitimate client validation.

1.3. Contribution

Our contributions are summarized below:

- We propose a new user verification architecture for valid user authentication to prevent accessing data by unauthorized user and enhance data security by a convenient hybrid system.
- We incorporate both biometric verification and encryption strategy in a single system to ensure valid user authentication.
- Used one-time password (OTP) as secret key for enhance system security.
- For the cloud security, more than 10 methods are studied and selected bests from them.
- In the result verification section, our provided system ensures the efficiency and verifiable guarantee.
- Finally, we process the average time of our proposed framework and contrast with the different existing framework with checking the performance and get a positive outcome from it.

1.4. System model

The system model for improving Cloud Data Security through biometrics and encryption System, as shown in Figure 1. In this design while customer need to get to the information put away in cloud, first need to check client in customer side utilizing biometric template. Then it's required to extract features from the biometric sample as a template using minutiae extraction algorithm. After then verify the template using store template in cloud database. In the wake of checking the customer, a login ask for sends to the cloud validation server. At that point, cloud verification server creates an OTP haphazardly from numerous characters. At that point, server scramble the customer information utilizing AES encryption calculation where one-time secret phrase utilized as symmetric key. Then server send the OTP to the client using HTTP gateway. Client decrypt the encrypted data using those OTP.

At whatever point the new client needs to get to the Cloud, the main thing he should do is to enlist by utilizing his fingerprints. When he is enlisted he turns into a legitimate client and can login to the cloud by following the technique. The unique finger impression put away in the database. There are

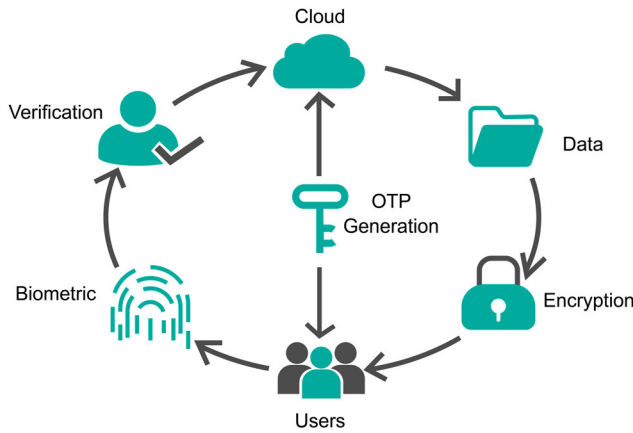


Figure 1. Proposed hybrid model.

Table 1. Description of notations used in this paper.

Notation	Description
AES	Advanced Encryption Standard
BT	Biometric Technique
UQ	Uniqueness
PR	Permanence
PF	Performance
CT	Cost
OTP	One-Time Password
ROI	Region Of Interest
AT	Average Time
FC	Face Recognition
FP	Fingerprint Recognition
IR	Irish Recognition
SG	Digital Signature
VC	Voice Recognition
PIN	Personal Identification Number
FPES	Fingerprint & AES Encryption
ED	Encrypted Data

additionally a second step check to discover substantial client utilizing the OTP. The OTP key send to the client for unscramble client information. All notations are used in this research are shown in Table 1.

1.5. Design goals

To enhance security and valid authentication, this design method must satisfy the following design goals:

- **Correctness:** We used to have passwords with numbers, alphabets, symbols, and so forth. That are turning into easy to hack every day. There are tens of millions of hacking incidents taking place each year and we are dropping our money constantly. Hybrid verification brings exceptional forms of solutions which are almost impossible to hack in contrast to passwords. This is a brilliant help for us, who are combating with safety problems for a long time.
- **Accuracy:** Customary security frameworks wreckage up routinely costing us a major measure of time, cash, and assets. The most widely recognized security frameworks are passwords, individual ID numbers and keen cards that aren't constantly exact. In any case, hybrid verification works with your physical attributes, for example, fingerprints, palm vein, retina among others that will consistently serve you precisely anyplace, whenever.

- **Convenient:** Envision every one of the occasions when you overlooked your passwords, very nerve-wracking, isn't that so? You are not the only one. We as a whole have experienced this procedure where it is difficult to retain or note down every single secret phrase and we are more than liable to overlook it at some tight spots. There are some helpful instruments to carry out the responsibility for you, however, none of these can beat the comfort of half and half check which stands to be the most advantageous arrangement ever. Your qualifications are with you perpetually, so it does not expect you to retain or note down anything.
- **Accountability:** Customary security frameworks wreckage up normally costing us a major measure of time, cash, and assets. The most widely recognized security frameworks are passwords, individual distinguishing proof numbers, and shrewd cards that are not constantly exact. Notwithstanding, cross-breed check works with your physical qualities, for example, fingerprints, palm vein, retina among others that will consistently serve you precisely anyplace, whenever.
- **Adaptability:** In contrast to different arrangements, hybrid verification profoundly versatile answers for a wide range of ventures. This innovation can be utilized in numerous administration ventures, banking security frameworks, workforce the board, and so on. It is conceivable in light of the adaptability of its answers.
- **ROI:** Hybrid verification will give anyone the best ROI contrasted with other security frameworks. Anyone can monitor a huge number of representatives of a huge organization with only one gadget and programming. Then again, you would need to deal with a colossal asset to do a similar activity costing you additional time than the proper mixture arrangement.

2. Literature review

Cloud computing is perhaps the maximum flamboyant technological innovation of the twenty-first century that holds its significance in nearly every field you could think of. This is because it has seen the fastest adoption into the mainstream than some other technology inside the domain. It permits us to run software programs without installing them on our computers, it allows us to save and get admission to our multimedia content via the net, it permits us to develop and take a look at packages without always having servers and so forth. So, information safety in the cloud could be very an awful lot crucial. Its want to recognize how the gadget for cloud safety are designed previously. This phase describes the maximum famous cloud records safety structures.

Cloud redistributing is an ideal method to lessen the weight of calculation. So its another significant thing for cloud information security likewise cloud security. Shweta et al. [9] proposed multimodal biometrics. Numerous unimodal have a few issues, for example, uproarious information, parody assaults and so on, which cause uncertain information. To beat these issues, multimodal biometrics is utilized. Multimodal biometrics permits flushing at least two qualities into single distinguishing proof. Kavita et al. [20] proposed facial acknowledgment framework for naturally recognizing and confirming individual from an advanced picture by looking at the chose highlights and facial

database. The 2D acknowledgment is influenced by changes in helping. Arun et al. [10] talked about crossover method which has the whole picture is considered while developing the edge include map. Particulars coordinating are utilized to decide the interpretation and revolution parameters relating the question and the layout pictures for edge highlight map extraction. Itering and edge highlight map extraction are actualized in the recurrence space in this manner accelerating the coordinating procedure. Itered inquiry pictures are caught to enormously build the one-to-many coordinating velocity. Prakash et al. [12] proposed new symmetric key calculation. They proposed a secluded 37 work and select any number and compute backwards of the chose whole number utilizing particular 37. The symmetric key dispersion ought to be done in the verified way. Shoup-Rubin proposed augmentation of Bellare-Rogaway demonstrate which depends on three gathering key dissemination convention and smartcard is utilized to store the long haul mystery keys. In their plan, smartcard is utilized to keep the foes and it is expected that smartcard is never bargained. So essentially the plan falls in a single-factor classification as two-factor plans can be broken by trading off both the variables as it were [17,19]. In 2014, Arockiam et al. [21] proposed efficient cloud storage confidentiality to ensure data security. The proposed procedure is secure to store the cloud user's information in the cloud storage. Encryption just or obscurity just is not adequate for cloud information storage. The integration of both techniques should provide maximum security to the user's data in the cloud data. But the problem is that obfuscation is also one kind of encryption. It is unnecessary to integrate the same type of techniques for encryption. Bedi et al. [22] develop a proficient and secure protection saving multi-distributed storage system for cell phones. Diverse multi-distributed storage administrations are accessible to expand the openly accessible capacity for clients, and yet, they are not secure and expending a lot of cell phone assets. That is the reason they proposed a proficient and secure protection saving multi-distributed storage system required for asset compelled cell phones. Liao et al. [18] endeavored to merge various passwords and smartcard based properties and proposed two-factor smartcard and secret phrase confirmation plot, which is as yet helpless against numerous assaults. Fleyeh et al. [13] proposed a calculation dependent on division and upgrade of pictures with low quality. Wang et al. proposed a unique finger impression coordinating calculation by utilizing decorated invariant minute highlights to accomplish the finger impression coordinating calculation [23]. Sahithi et al. [24] use both unique finger impression and palm-print affirmation together to give an improved component of sureness for singular checks and Identification for cloud information security. Zarnab et al. [25] depicts the security of the biometric framework through distributed computing is examined alongside progress with respect to its presentation to keep away from the criminal to get to the information. Biometric is a veritable element for the cloud supplier. The cryptography calculation will be disclosed utilizing blockchain innovation to beat security issues. The blockchain innovation will give more insurance through cryptographic keys to make sure about biometric information. Yassin [11] builds up the biometric acknowledgment framework for setting up the security to the client personalities in the cloud condition. The caught client

Algorithm 1 Procedure hybrid verification architecture through biometrics and encryption system

- 1: Collect biometric sample from user in client side.
 - 2: Extract feature from biometric sample as template using minutiae extraction algorithm.
 - 3: Verify the template using store template in cloud database. If success goto step 4 else access denied.
 - 4: Send login request to the server.
 - 5: Cloud authentication server randomly generate a OTP from unique characters. Then encrypt user data using the AES encryption algorithm and send the encrypted data to the client side.

$$ED \rightarrow \text{AESEncrypt}(\text{Data}, \text{OTP})$$
 - 6: Cloud authentication server also send the OTP to the user using the http gateway.
 - 7: User decrypt the encrypted data using the OTP.

$$\text{Data} \rightarrow \text{AESDecrypt}(ED, \text{OTP})$$
-

fingerprints are mostly encoded by applying the discrete wavelet change and the scrambled pictures are put away in the database which is utilized amid the layout coordinating procedure. This encoded and wavelet-based check conspire does not require overwhelming equipment and programming prerequisites additionally does not require the biggest sum. In this way, the creator proposes the proficient biometric acknowledgment framework for confirming the client data and allowing the entrance control authorization while getting to the information in the cloud condition.

3. Proposed method

The issue that influences the trust integrity of embracing cloud is validation. This issue can be limited profoundly by methods for actualizing the accompanying strategy convention. In such technique, we are fusing fingerprint recognition check as biometric confirmation and AES as secure encryption framework calculation. In the proposed hybrid model picture highlights are separated by distinguishing proof and details location process. As shown in Figure 1, the basic algorithm of proposed hybrid verification architecture is given below:

Using all procedures given in algorithm 1, the working flowchart are shown in Figure 2.

First of all its needs to collect the biometric sample from the user which is basically the client section. Now using the minutiae extraction algorithm features will be extracted from the biometric sample which is the template. One another template is also stored in the cloud database. Basically clients entered the template when he/she enlist by utilizing fingerprints. Its time to verify the template using the stored template in the cloud database. If both templates are the same then this system sends the login request to the server. The cloud authentication server randomly generates a OTP using unique characters. And then encrypt the user data using the advanced encryption algorithm and send the encrypted data to the client which is called ED(Encrypted Data). Most important thing is that the cloud authentication server also sends the one time password using the HTTP gateway to the user. That means, the OTP is

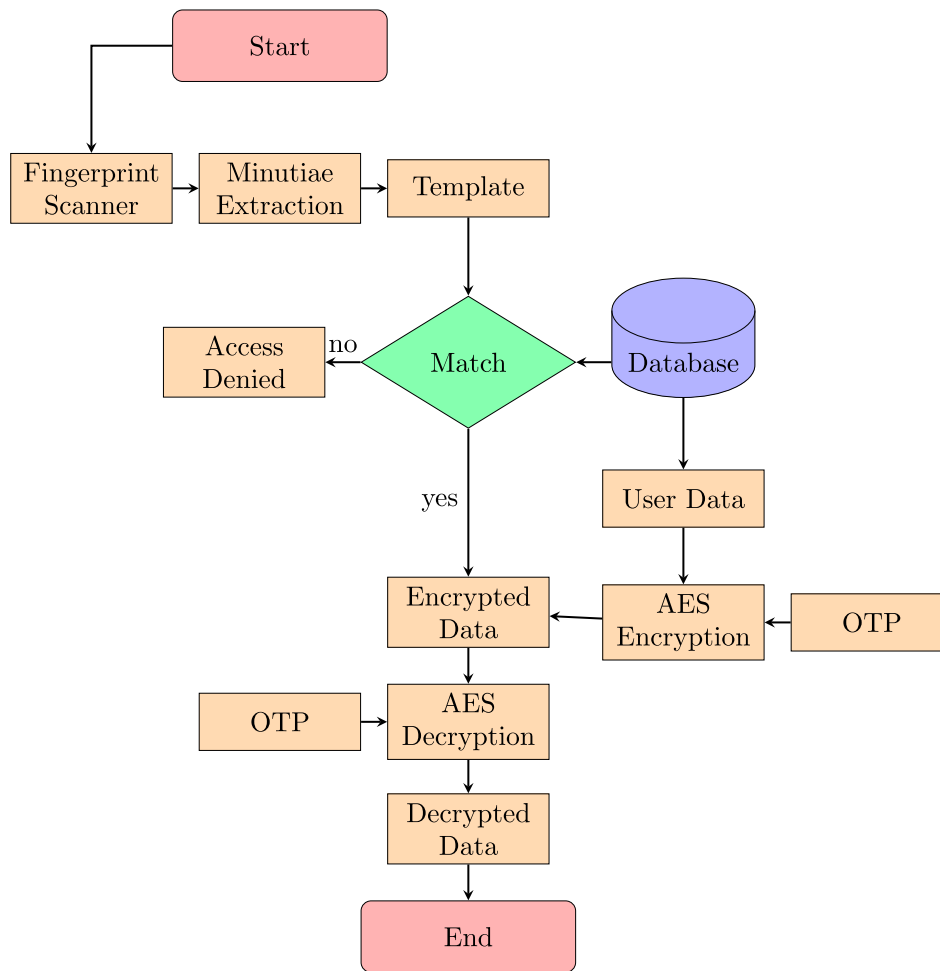


Figure 2. Proposed hybrid architecture of biometric and encryption system.

now present in the user's mail. Since the data is encrypted or unreadable. So for understanding the data users need to convert into a readable format. Using the OTP users can decrypt or convert the encrypted data into a readable format. From the next section, the framework will be implemented and we will calculate the average time and also compare it to the others implemented system.

4. Results and discussions

This section indicates the performance evaluation of the proposed approach. The assessment of other methods with the proposed technique is likewise proven. As the minutiae extraction algorithm diminishes an opportunity to separate the details from the biometric test, we pick the algorithm to process the biometric test in our strategy. By utilizing the AES, we can encrypt a lot of information helpfully and it additionally gives the best legitimacy and secure for both supplier and client. OTP include an unsure factor in verification with the goal that the client needs to give various messages to confirm each time. By along these lines, the application themselves can acquire higher security ensure than those utilized static secret word innovation. At last, we figure the procedure execution time and afterward contrasted and different existing technique and results are recorded in the table.

4.1. Minutiae extraction

Human fingerprints are affluent in nuances called points of interest, which can be used as recognizing verification engraves for one of a kind finger impression affirmation. To achieve incredible subtleties extraction in fingerprints with fluctuating quality, pre-planning in kind of picture overhaul, picture binarization, and picture division are first associated on fingerprints before they are surveyed. Histogram evening out and Fourier Transform have been utilized for picture improvement. At that point the fingerprint sample picture is binarized utilizing the nearby versatile edge strategy. Minutia extraction is finished by diminishing and minutia checking strategy [26]. By utilizing the match score technique, we separate the two fingerprints are the equivalent or not [8]. The process of extracting minutiae points using minutiae extraction algorithm is shown in Algorithm 2.

4.2. Advanced encryption standard (AES)

AES relies upon an arrangement standard implied as a substitution-change orchestrate, mix of each substitution and organize, and is smart in each item system and gear. Rather than its antecedent DES, AES does not use a Feistel compose. AES could be a variety of Rijndael that joins a fixed square size of 128 bits, and a key size of 128, 192, or 256 bits. Against this, the Rijndael detail, all things considered, is ostensible with a square and

Algorithm 2 Minutiae Extraction Algorithm for Extracting Minutiae Points

- 1: Take input from fingerprint scanner.
- 2: Apply Histogram equalization on the input image.
- 3: Enhancement of image.
- 4: Binarized the enhanced fingerprint image.
- 5: Selection of ROI (Region of Interest) in binarized image.
- 6: Thinning of the Region of Interest as the part of fingerprint image.
- 7: Minutiae points are extracted from image.

key sizes which will be any numerous of 32 bits, each with at least 128 and the vast majority of 256 bits. AES works on a 4–4 section significant request framework of bytes, named the state, however, a few adaptations of Rijndael have a greater square size and include additional segments inside the state. Most AES counts have depleted a unique limited field. The key size utilized for an AES figure indicates the quantity of redundancies of change adjusts that convert the information, alluded to as the plain text, into a definitive yield, known as the ciphertext [6,7].

4.3. One-time password (OTP)

OTP is a password that substantial just once. Its essential thought is to include unbound factor in verification with the goal that clients need to give diverse messages to confirmation each time. By along these lines, the applications themselves can get higher security ensure than that utilization static secret phrase innovation. At the point when login ask for from the client is gotten, the server framework produces a one-time secret phrase and sends it through an email enrolled for that predefined client. The one-time mystery key has a default break. In the second time of the affirmation, an interest is sent with the customer id and a hash of the one-time mystery word. If both the one time and customer fingerprint is real, by then the customer will be affirmed. Secret word entropy depends on the character set utilized (which is expansible by utilizing lowercase, capitalized, numbers just as images) just as secret key length. Secret word entropy predicts how troublesome a given secret word is break through speculating, savage power splitting, lexicon assaults, or other normal techniques [13]. Password entropy is a measurement of how unpredictable a password is, concerning how troublesome it is split. By using this technique, we can try to check about the unpredictability of our created OTP. Password entropy is normally communicated regarding bits: a password that is now known has zero bits of entropy; one that would be speculated on the main endeavor a fraction of the time would have 1 bit of entropy [27]. The formula of entropy is:

$$E = \log_2(R^L) \quad (1)$$

Where E = Password entropy, R = pool of unique characters, L = number of character in your password, $E = \log_2(R^L)$ the number of bits in entropy. An example of password entropy is given below. Number of potential characters with an alternate sort that can be chosen for a secret phrase is appeared in Table 2.

$$\text{Entropy } E = \log_2(R^L)$$

Table 2. Possible characters for OTP.

Type	Pool of possible character
Lowercase	26
Uppercase	26
Digit	10
Special character	33
Total	95

$$\begin{aligned}
 &= \log_2(95^{14}) \text{ [We use 14 characters in our OTP]} \\
 &= 91.98 \\
 &\approx 92 \text{ bits}
 \end{aligned}$$

4.4. Simulation environment

Both the customer side and cloud side calculation is performed in the equivalent arranged workstation. In the event that we execute the two frameworks in diversely arranged workstation, at that point it might create distinctive normal time for an alternate design. We compute process execution time for different kind of information and attempt to compute the rough time that requirements to play out this model helpfully and produce an increasingly precise outcome. For this reason, we utilized some product like Visual-Studio-2017 and Arduino to play out our product side and utilized some designs like Arduino UNO and Fingerprint-Module R305 for taking the biometric test and send to the product side. Some jumper wires are also used. For programming, the C-Sharp language is used. The usage is done in an indistinguishable PC with an Intel Core(TM)i5-5200 CPU 2.70 GHz processor and 8GB RAM. Hardware Connection for this Model is given in Figure 3.

To communicate with the module, serial communication at 57600 baud is required. When using an Arduino, a message to prompt the user for input or debugging is sent through the hardware serial port and displayed on the serial monitor. Here, a software serial port was setup using pin 2(R_x) and pin 3(T_x) of the Uno. The module can be controlled utilizing 3.6 –6 V. For this situation, 5V was utilized. So the connection follows:

- Connect T_x module (green wire) with R_x of Arduino(pin 2)
- Connect R_x module (yellow or white wire) with T_x of Arduino(pin 3)
- Vcc of the module (Red wire) with 5V pin of Arduino.
- GND of the module (Black Wire) with GND of Arduino.

This is the time to integrate hardware and software for this architecture. At first, open the fingerprint verification software and set the serial port. The interface of the software is shown in Figure 4 (first). The software is making with the C# programming language. Now we can do enroll and detect the fingerprint. After enrollment is complete, we can do register which is shown in Figure 4 (Second). After completion of the registration process. By opening the verification software, we can find our ID. Besides the encryption–decryption software also works. It takes all information from the database, and via email we get the OTP key to encrypt the information. After encryption, using the OTP we can complete the decryption of our data. The encryption and decryption process are shown in

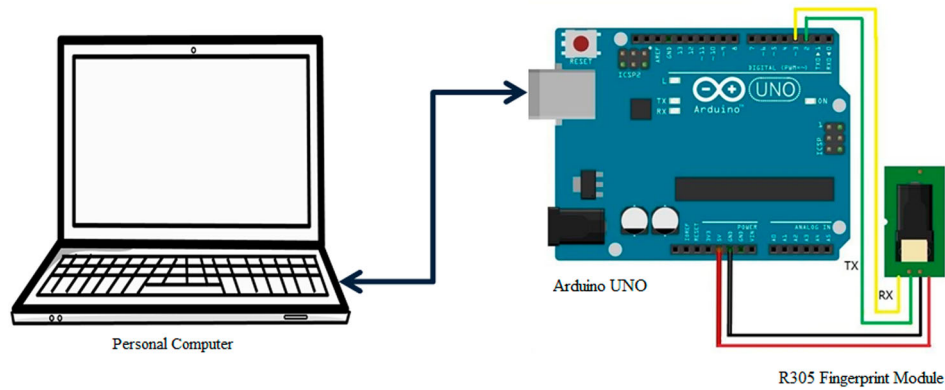


Figure 3. Hardware connection for this model.

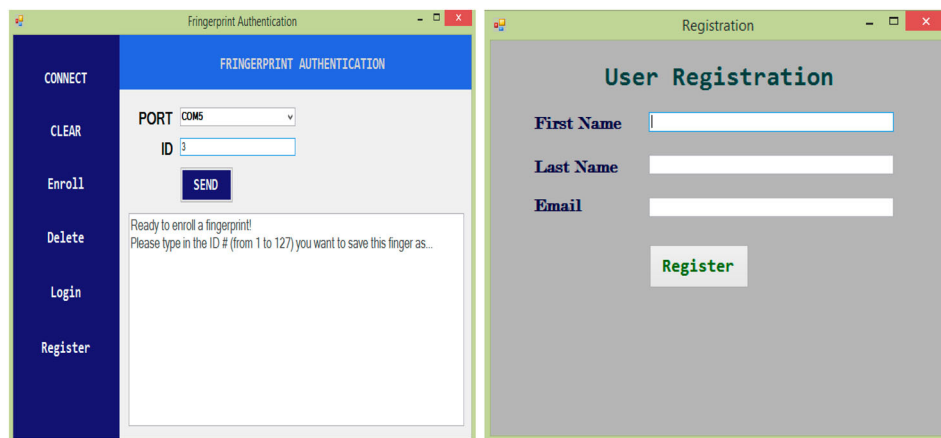


Figure 4. Fingerprint authentication and user registration interface.

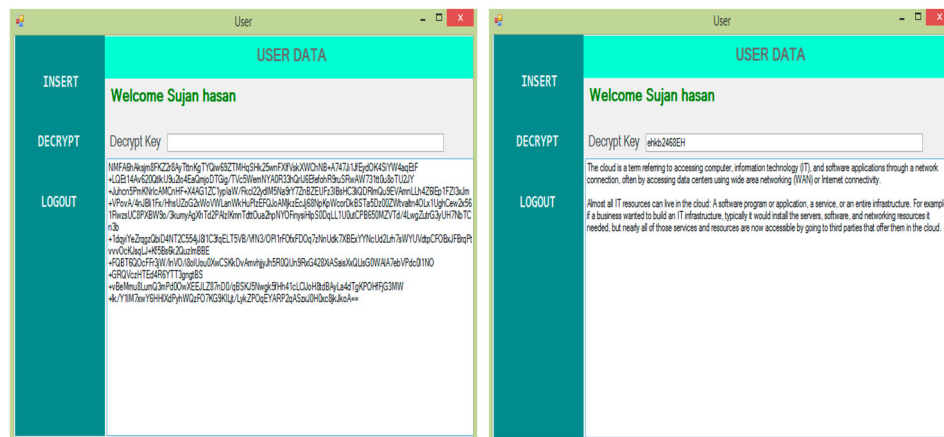


Figure 5. Data encryption and decryption process.

Figure 5. Here we are using some data for showing the encryption and decryption. All codes for this model, you can find from <https://github.com/hasansujan23/Fingerprint-Authentication>.

4.5. Performance evaluation

Strong security properties are achievable within simple security proposed designs that are suitable for implementation of hybrid verification technique based on fingerprint and AES algorithm for security of cloud. In this research, We

described about cloud security fundamental model, benefits and limitation of cloud security, fingerprint recognition, minutiae extraction and AES encryption process. For previous research, We got some concepts like that method is less secure and cost-effective besides the data does not secure from the social engineering meetings. For this reason, we are trying to set up a new system, which will give more security than the existing security system. The following parameters like required objects, Performance, Uniqueness, Permanence, cost, and Average time are used to how the proposed biometric

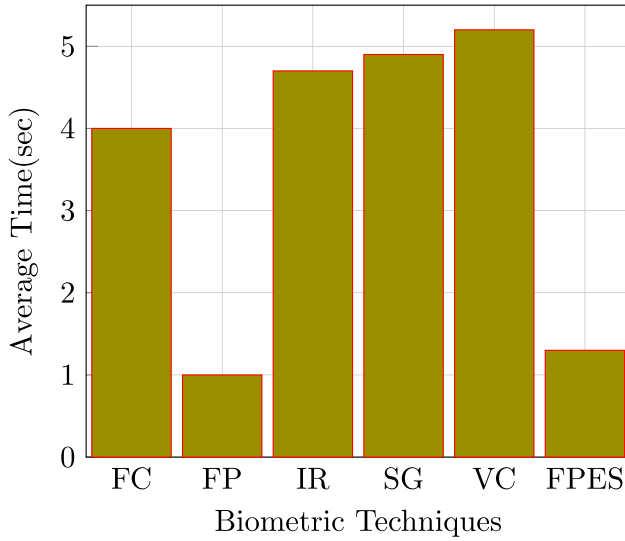


Figure 6. Comparison of the proposed hybrid technique's average time with various biometric techniques average time.

Table 3. Comparison of various biometric techniques with the proposed hybrid technique.

BT	UQ	PR	PF	CT	AT(s)
FC	L	M	L	M	4-5
FP	H	H	H	M	1
IR	H	H	H	H	< 5
SG	L	L	L	M	< 5
VC	L	L	L	M	> 5
FPES	H	H	H	M	1.30

feature helps to provide security while accessing the cloud data.

For the fingerprint verification, minutiae extraction algorithm are used in this research. In Table 3 L, M, H stands for Low, Mid, High. Here FPES is our proposed Fingerprint Biometric and AES Encryption technique. Code execution time is a default function that is used for calculation different times like encryption time, decryption time. Comparison of various biometric techniques with the proposed hybrid technique are shown in Table 3 and the graphical view are shown in Figure 6 with the average time.

We measure encryption and decryption time for different file for analyzing the performance of the hybrid architecture. For this purpose, we calculate encryption and decryption time for different bytes of data, text files and image files. For encryption-decryption, we take 5000, 10,000, 15,000, 20,000, 25,000, 30,000 bytes of data which are shown in Table 4. We also take 200, 400, 600, 800, 1024, 2048 kb text and image files shown in Tables 5 and 6. We calculate individual average time for various bytes of data or various size of text files and image files.

In Table 4, it is attempted to demonstrate that all information are taken in byte. For each information, both encryption and decryption times are determined by the proposed strategy. At last, the normal time for all sources of info is likewise determined. In the event that the information sources information are in 5000b to 30,000b, at that point, the normal time of encryption and decryption is 39 ms. The graphical view for

Table 4. Encryption and decryption time for different bytes of data.

Input (byte)	Encryption time (ms)	Decryption time (ms)	AT (ms)
5000	25	41	39
10,000	28	47	
15,000	29	48	
20,000	30	48	
25,000	32	53	
30,000	33	54	

Table 5. Encryption and decryption time for different text files.

Input (kb)	Encryption time (ms)	Decryption time (ms)	AT (ms)
200	26	32	56.75
400	34	38	
600	45	48	
800	54	56	
1024	65	67	
2048	102	114	

Table 6. Encryption and decryption time for different image files.

Input (kb)	Encryption time (ms)	Decryption time (ms)	AT (ms)
200	30	31	51.50
400	35	35	
600	44	46	
800	52	52	
1024	58	59	
2048	85	91	

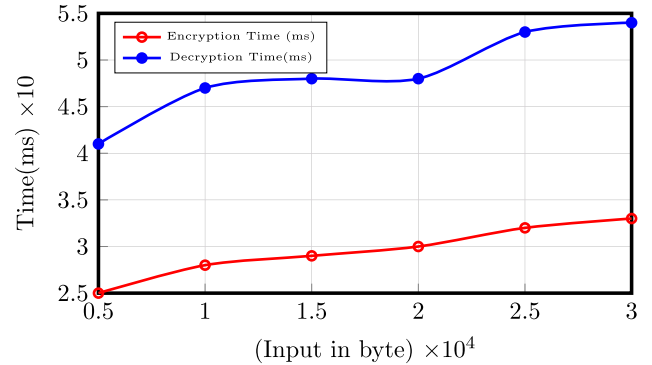


Figure 7. Encryption and decryption time for different bytes of data.

each contribution with encryption and unscrambling time is appeared in Figure 7.

Presently, we attempt to check the proposed technique for various content document with various sizes which are appeared in Table 5. For the assessment, we take contributions from 200 to 204 kb. In the wake of computing the encryption and unscrambling time, the normal time is 56.75 ms. The graphical view for writings information is appeared in Figure 8.

Finally, we attempt to test the proposed technique for a one kind of picture report with special sizes which are proven in Table 6. The proposed method can take all image format as enter. For the exam, we take input picture with different sorts from 200 to 204 kb. After calculating the encryption and decryption time, the average time is 51.50 ms. The graphical view for snap shots input is shown in Figure 9.

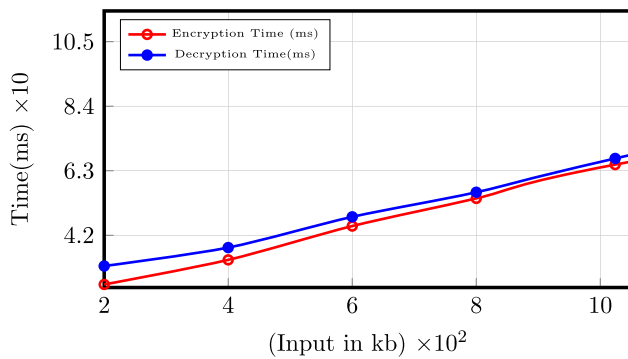


Figure 8. Encryption and decryption time for different text files.

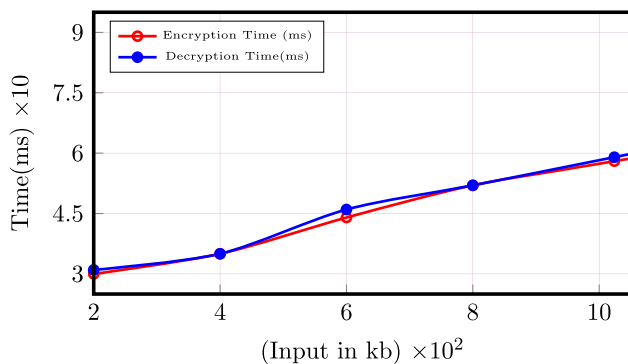


Figure 9. Encryption and decryption time for different image files.

To execution assessment of crossover confirmation dependent on biometric and encryption framework must contrast and existing different models. In this hybrid verification model, fingerprint recognition utilized as a biometric test and AES utilized as an encryption framework. All models execution parameters are enrolled here. Average time of the hybrid verification model is around 1.30 s that need to check a client by biometric test and encryption and decoding time of cloud information. From the recorded information obviously through the hybrid verification models need additional time than fingerprint recognition, it gives preferable security over fingerprint recognition and every single other model. At the point when the size of information differs, then encryption and decoding time may fluctuate that may change all out average time. Here time just changes in encryption and unscrambling framework. Despite the fact that the ideal opportunity for biometric confirmation is unaltered, being the difference in encryption and decoding time, it may change the absolute models average time.

5. Conclusion

This research gives an outline of cloud computing and discussions about a portion of the security issues related to cloud computing. It likewise acquaints a half breed approach with cloud information security. This technique utilized in the proposition for the confirmation in the cloud is the original thought for better and upgraded security of the cloud purchaser significant data. In every single dimension, security has been kept up profoundly. This will be a definitive technique adversary

improved confirmation framework in cloud condition. Encryption in finishes of verification will build the security of biometric layout and that will be especially valuable in giving secure confirmation. In our proposition, we have utilized a unique finger impression has biometric test and encryption has AES calculation. By implementing this model enhance the security of the cloud and provide valid user authentication. This model also required less time than other models but provide more security than others and fulfill our goal. However, in the future, it very well may be stretched out to some other biometric and other encryption algorithms. The proposed convention for confirmation will build the unwavering quality of the selection of distributed computing to our registering condition. In the future, we will do the usage of the equivalent above said show for better verification which improves the security, which improves the trust among the cloud condition. And after that rather than fingerprint as the biometric test we can attempt some different biometrics like iris, face etc.

5.1. Recommendation for future work

The proposed framework for verification will expand the unwavering quality of the reception of distributed computing to our processing condition. Likewise, we will run the test to check whether there are any extra computational overhead brought about by utilizing this methodology. Later on, we will do the execution of the equivalent above-said model for better confirmation which improves the security, which improves the trust among the cloud condition. And afterward rather than a fingerprint recognition as a biometric test, we can attempt some different biometrics like iris, face, and so on. Likewise, attempt to refresh the key age strategy by broadening the scrambled OTP calculation with the goal that the framework turns out to be increasingly secure.

Notes on contributors

Md. Alamgir Hossain is working as a lecturer at the Department of Computer Science and Engineering at Prime University, Dhaka, Bangladesh. He completed his B.Sc. in Computer Science and Engineering from Jashore University of Science and Technology, Jashore, Bangladesh. He is a researcher and his main research focuses on cloud outsourcing, data security, and image processing.

Md Abdullah Al Hasan is a software engineer in Bangladesh-Japan information technology. He completed his B.Sc. in Computer Science and Engineering from Jashore University of Science and Technology, Jashore, Bangladesh. He is a researcher and his main research focuses on data security and artificial intelligence.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Md. Alamgir Hossain  <http://orcid.org/0000-0001-5120-2911>

Md. Abdullah Al Hasan  <http://orcid.org/0000-0002-2913-7380>

References

- [1] Md. Alamgir H, Jannatul F, Marjia K. A study and implementation of large-scale log-determinant computation to cloud. *Int J Comput Appl.* 2019;0:1–9.

- [2] Xiaowei Y, Xiaosong Z, Ting C, et al. The research and design of cloud computing security framework. *Adv Comput Commun Control Autom.* **2011**;121:757–763.
- [3] Jamil D, Zaki H. Cloud computing security. *Int J Eng Sci Technol.* **2011**;3:3478–3483.
- [4] Aamir N. Cloud computing: security issues and challenges. *J Wirel Commun.* **2016**;1:10–15.
- [5] Adnaan A, Thariq H. Cloud computing: study of security issues and research challenges. *Int J Adv Res Comput Eng Technol.* **2018**;7:2278–1323.
- [6] Subhashini P, Yeshwanth R. Securing cloud data using encryption algorithms. *Int J Adv Res Sci Eng.* **2017**;6:1188–1194.
- [7] Rohit B, Sugata S. A survey on security issues in cloud computing and associated mitigation techniques. *Int J Comput Appl.* **2012**;47:47–66.
- [8] Geetanjali C, Jainul A. Modified secure two way authentication system in cloud computing using encrypted one time password. *Int J Comput Sci Inform Technol.* **2014**;5:4077–4080.
- [9] Shweta M, Chander V. A hybrid approach for securing biometric template. *Int J Eng Adv Technol.* **2013**;2:2249–8958.
- [10] Arun R, Anil J, James R. A hybrid fingerprint matcher. *Pattern Recognit.* **2002**;3:795–798.
- [11] Yassin A. Efficiency and flexibility of fingerprint scheme using partial encryption and discrete wavelet transform to verify user in cloud computing. *International Scholarly Research Notices*; 2014.
- [12] Prakash K, Saeed Q. Implementation of security through simple symmetric key algorithm based on modulo 37. *Int J Comput Technol.* **2012**;3:335–338.
- [13] Hasan F. Segmentation and enhancement of low quality fingerprint images. *International Conference on Web Information Systems Engineering*; Vol. 10042, 2016. p. 371–382.
- [14] Jyoti C, Pardeep K, Mangal S, et al. A strong user authentication framework for cloud computing. *Proceedings – 2011 IEEE Asia-Pacific Services Computing Conference APSCC*; 2011. p. 110–115.
- [15] Udendhran R. A hybrid approach to enhance data security in cloud storage. *Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing*, Vol. 90, 2017. p. 1–6.
- [16] Selvarani P, Malarvizhi N. To enhance the data security in cloud computing using multimodal biometric system. *World Wide J Multidiscip Res Dev (WWJMRD).* **2017**;3(7):196–201.
- [17] Victor S, Avi R. Session key distribution using smartcards. *International Conference on the Theory and Applications of Cryptographic Techniques*; Vol. 1070, 2001. p. 321–333.
- [18] Liao I, Lee C, Hwang M. A password authentication scheme over insecure networks. *J Comput Syst Sci.* **2006**;72:727–740.
- [19] Mihir B, Phillip R. Provably secure session key distribution – the three party case. *Proceedings of 27th ACM Symposium on the Theory of Computing*; 1995.
- [20] Kavita T, Renu L, Kalakot L. Fingerprint recognition and feature extraction using transform domain techniques. *International Conference on Advances in Communication and Computing*; 2011. p. 1–5.
- [21] Arockiam L, Manikandasaran SS. Efficient cloud storage confidentiality to ensure data security. *International Conference on Computer Communication and Informatics*; 2014. p. 1–5.
- [22] Rajeev Kumar B, Jaswinder S, Sunil Kumar G. An efficient and secure privacy preserving multi-cloud storage framework for mobile devices. *Int J Comput Appl.* **2019**;0:1–11.
- [23] Jing S, Hongxia W, Qing Q, et al. An efficient fingerprint identification algorithm based on minutiae and invariant moment. *London: Springer*; **2017**. p. 71–80.
- [24] Sahithi S, Anirudh A, Swaroop B, et al. Biometric security for cloud data using fingerprint and palm print. *Int J Innov Technol Explor Eng (IJITEE).* **2019**;8(6S3):338–343.
- [25] Zarnab K, Aysha S, Maryam S, et al. Cloud server security using bio-cryptography. *Int J Adv Comput Sci Appl (IJACSA).* **2019**;10: 166–172.
- [26] Sree V, Chandra E. Multimodal biometric hashkey cryptography based authentication and encryption for advanced security in cloud. *Biomedical Research Special.* 2018.
- [27] [Cited 2020 28 April]. How to calculate password entropy. Available from: <https://ritcyberselfdefense.wordpress.com/2011/09/24/how-to-calculate-password-entropy/>.