ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

SSO BASED FINGERPRINT AUTHENTICATION OF CLOUD SERVICES FOR ORGANIZATIONS

Ali Zaheer Agha1∗, Rajesh Kumar Shukla2, Ratnesh Mishra3, Ravi Shankar Shukla4
1 Research Scholar, Invertis University, Bareilly, Uttar Pradesh, India (ORCID - 0000-0002-7130-7160)
2 Professor & Dean - Faculty of Engineering and Technology, Invertis University, Bareilly, Uttar Pradesh, India
3 Sr. Assistant Professor, Dept. of Computer Science & Engineering, BIT Mesra, Patna Campus, Patna, Bihar, India
4 Assistant Professor, Dept. of Computer Science, College of Computing & Informatics, Saudi Electronic University, Saudi Arabia

Abstract:

Access to a pool of programmable resources, such as storage space, applications, services, and on-demand networks, is made possible by cloud computing technology. Involving the cloud with the organization reduces its efforts to meet the needs of its customers. The Single Sign-On (SSO) method, which enables users to access various application services using a single user credential, is one of the key benefits of cloud computing. There are numerous problems and difficulties with cloud computing that need to be highlighted. However, protecting user agent privacy against security assaults is far more challenging. To combat security and privacy assaults, this study suggests SSO-based biometric authentication architecture for cloud computing services. Since end devices are computationally inefficient for processing user information during authentication, biometric authentication is effective for resources controlled by end devices at the time of accessing cloud services. As a result, the proposed design minimizes security attacks in cloud computing. An innovative strategy that establishes a one-to-one interaction between the user agent and the service provider is also included in the suggested design. In this case, user agents can use their fingerprint to access various cloud application services and seek registration. The highlights of the suggested architecture have been offered based on comparison analysis with a number of existing architectures.

Keywords: Cloud security, Biometric authentication, Security algorithm, Privacy protection;

1. Introduction

Since it offers an adaptable and effective solution for many Internet-based services, cloud computing (CC) has experienced enormous growth over the past several years [1]. Organizations are required to store data or information in a location that is simple for stakeholders or authorized individuals to access. The best course of action in these circumstances is to store data in a cloud environment. This enables organizations to cost-effectively and easily share data with others [2]. Clients can use the cloud services of various programs by adopting CC rather than buying or installing the software on their own computers [3]. Although affordability and on-demand availability are the top two advantages of cloud computing, users' top worries are increasingly about trust and security. Highly sensitive data must be protected for corporate purposes, as well as frequently for ethical and legal reasons [4]. The main and necessary step in each application

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

to establish the legitimacy of the user is authentication [5].

- One of the most exciting technological advancements in recent memory is biometric authentication, which has the potential to revolutionize how most people live.
- Personal authentication using biometric technologies is a reaction to the growing need for security and authentication. Fingerprint recognition is the biometric authentication technique that is most frequently employed.
- The automatic identification or identity verification of an individual utilizing either a biological feature or physiological features like a signature is referred to as biometric authentication.

Two broad groups of biometric traits can be distinguished:

1. Physiological Features: These traits relate to how the body is shaped. Among the traits, fingerprints have been utilized for over a century. Other examples include face recognition, hand geometry, and iris recognition.

1. Behavioural features: These traits have to do with how people behave. The signature was one of the earliest traits to be utilized and is still often used today.

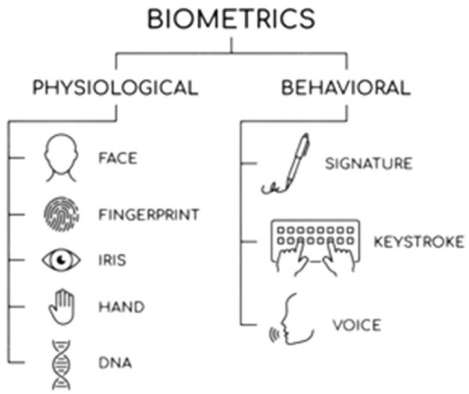

Figure 1 – Classification of Biometric Recognition

Users can securely authenticate and gain access to several applications and websites using the Single Sign-On (SSO) authentication technique by checking in using just a single username and password. For instance, accessing Google applications like Google Docs, Gmail, and Google Drive only requires a single sign-in to your Google account [6].

Prior to SSO, each user had to remember a different password for each application in order to access the various applications offered by a single application service provider. As a result, users tended to remain with shorter passwords or reuse them across many applications, which is a security issue. Theoretically, SSO allows for the selection of a more complex password as just one need to be remembered [7]. In many services offered in a cloud environment, this strategy is thought to be more acceptable and competent. Furthermore, SSO benefits from user account management that is independent of cloud environments. There are three preferred SSO authentication methods:

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

1.1 Kerberos

A trustworthy third party and a key distribution centre (KDC) are required components of the authentication protocol type known as Kerberos. This method creates a ticket that acts as an identification for requests for cloud permissions. The usage of third parties in the authentication process and key sharing by KDC are the fundamental weaknesses of the Kerberos protocol. Failure of the Key Distribution Centre (KDC) causes the authentication procedure to be delayed as well.

1.2 Smart Card

Smart cards are used to store user agent secret information. A user-encrypted smart card is provided by the registration entity with the aid of a smart card manufacturing device. The user logs in to the CSP login service site using an encrypted smart card. Without the needs to store and safeguard a lot of authenticate information, it can decrease the user's authentication time.

1.3 One-Time Password (OTP)

OTP is a two-factor authentication method that is effective for user verification authentication. Today's digital banking technology offers an OTP authentication tool to confirm the user's legitimacy. On the user's registered mobile number, an OTP is produced with a time limit. For it to function together, it needs a password, a physical token, and two key states.

All three of these SSO authentication systems, nevertheless, have security flaws. One user credential will be used to access all SSO-independent cloud services. However, in this case, if the user's credentials are stolen just once, everything they have stored in the cloud could be lost. Therefore, using a biometric authentication mechanism for SSO purposes is preferable to using smart cards, OTPs, Kerberos, and other authentication methods since it is more difficult to compromise the security of a biometric system than other authentication methods.

Enrollment and Verification are the two stages of every biometric authentication system [8]. The user's features are taken out throughout the enrollment process and entered into the database. During the verification stage, feature vectors from the database are compared to those retrieved from the user's features.

Figure 2 demonstrates that fingerprints are the most popular biometric, accounting for 48.8% of the market. Both the public and private sectors of the global economy are growing with the biometrics sector. According to a Gigya survey of 4,000 consumers in the United States and the United Kingdom, 52% of buyers would prefer utilizing biometrics instead of passwords and PINs [26].

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

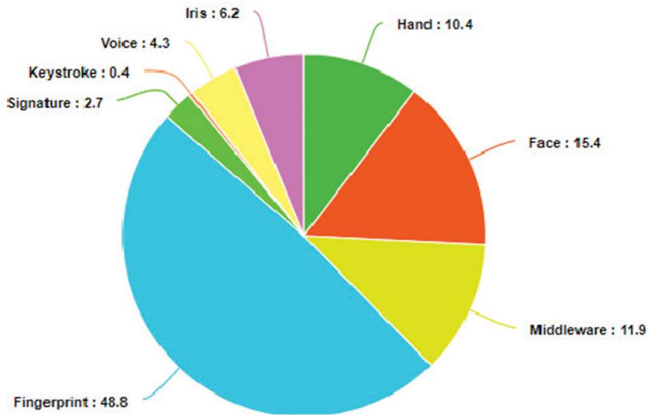

Figure 2 - Comparison of market shares for various biometric authentication system [26]

In general, biometric methods seek to recognize or confirm a person's identity using physical traits (such as a face, iris, fingerprint, DNA, or hand shape) and/or behavioural traits (such as speech, gait, or signature). For a fingerprint-based system, the pattern is established after birth, and even identical twins have unique fingerprints [9].

Users must use a public internet connection to access cloud services. These natural environments are susceptible to a number of harmful attacks. Distributed denial of service (DDoS) attacks, password spoofing, and message interception are the most significant vulnerabilities that need to be investigated in the context of cloud computing services as these providers use equipment with limited resources to offer clients with services and applications. In addition, there are many different service providers in cloud computing, which makes user account management another problem. End devices that access cloud-based services are computationally inefficient due to resource limitations. In [10], an attempt was made to address the issue of DoS attacks by using a status bit of 0 (when the user logged out) and 1 (when the user logged in). But what if a single user targets cloud services by creating numerous accounts with unique IDs and launching DDoS attacks that significantly impede network and data accessibility? This is another issue that has to be discussed. It is advisable to offer security improvements that could improve the method's performance [10] and handle DoS attacks as well as issues like lost smart cards and password interception. Some biometric system vulnerabilities are show in figure 3 below.

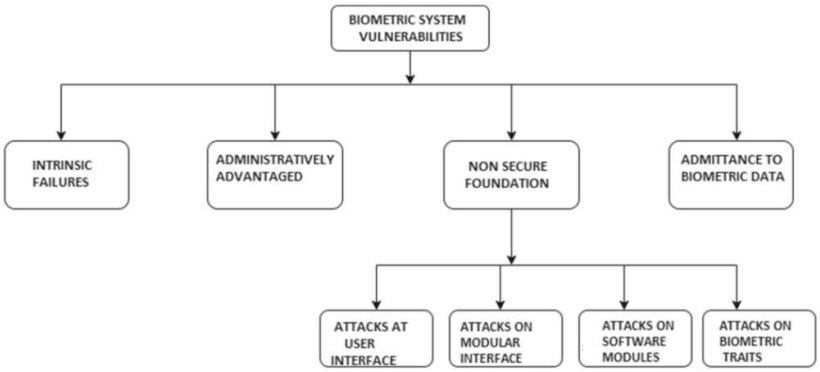

Figure 3 – Biometric System Vulnerabilities

Figure 4 summarizes the sequence diagram of the authentication and authorization procedure in

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

the SSO system. The actions in this process are:

1. User access request to the application.
2. Request for sign-in information or, if you haven't registered yet, a sign-up form.
3. Signing up or logging in, then providing the information to the authentication system.
4. Generating a unique ID to each user, registering that ID in the system database, or looking up a registered user in the database used for authentication.
5. User approval and notice to the user, or disapproval and notification for access denial.
6. Providing the application the user ID.
7. Establishing an access connection for this user ID to the service or application requested.
8. Issuing the user an access link.
9. Access to the requested application by the user.

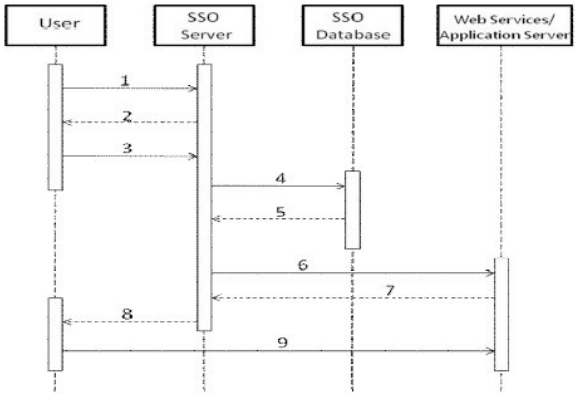

Figure 4 – Sequence Diagram of SSO

This paper explores fingerprint-based authentication architecture as a defense against security and privacy assaults in the cloud computing platform. The simplest form of handling accounts for using the Single Sign-On (SSO) concept to access numerous application services with a single credential, it is suited for end devices with limited resources that are used to access the services and reduces security assaults. The rest of the paper is organized as follows: Section 2 of the article covers the associated work of the authentication framework in the cloud environment. Section 3 discusses the proposed fingerprint-based authentication method and how it works. Section 4 examines the suggested method's security and functionality, while Section 5 presents the paper's conclusion.

2. Related Work

Following the development of cloud computing, a number of proposed authentication methods to access cloud-based services have been made.

The authors of paper [1] provided a review and multi-level feature analysis of 33 cloud environment simulators. They concluded from this assessment that none of them are perfect in every way and still require improvement. Utilizing different software or software combinations for specific optimization goals, such as load balancing and energy efficiency, is one method.

Security and identification accuracy, two important (and competing) metrics for fingerprint-based biometric systems, are thoroughly reviewed in this study [09]. We have examined two types of

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

security-related attacks: those on user interfaces and those on template databases. Also included are defenses against these attacks and their defensive measures. Although recent developments in biometric templates protection and an improvement in recognition accuracy under less-than-ideal circumstances, they noted that there are still plenty of unresolved problems that require the attention of biometric researchers.

A number of cloud computing security measures are the topic of paper [11]. Although the vast majority of security measures provide an appropriate level of security, every gadget occasionally malfunctions. Deceptive technologies and user behaviour profiling are important elements of this strategy. In cloud computing, this technique helps with user behaviour tracking and predictions. Once the user has been located, it is possible to choose between sending the original data and a replica file that was generated dynamically utilizing deceptive technologies. As a result, the system's data will be protected, and encryption technologies may be used to further enhance security.

The method suggested in [12] explained how biometric authentication has been extensively researched and put into use in both academic and professional settings to reduce the hassle of managing passwords and improve the usability of authentication systems. The risk of attacks, however, substantially reduces end users' acceptance of the existing solutions. The authors examined recent developments in biometric authentication and discovered that the majority of the solutions now in use had security and privacy flaws. According to this survey, it is crucial to increase the security and privacy of biometric authentication systems.

In order to prevent theft of identities, Paper [13] presented a state-of-the-art survey of the various authentication techniques available in cloud environments. An effective authentication system that ensures security against data theft has been the focus of numerous research studies. In this paper, the contributions of each piece of work have been addressed, and the research methods used have been examined.

A multimodal biometric authentication system is suggested in paper [14] to increase the security of data in cloud environments. A secret key is created by combining the features taken from the fingerprint, iris, and palm print in several steps, and then using the MD-5 hashing method, converting the result into a hash of characters and numbers. Then, using the secret key and the three symmetric key encryption methods DES, AES, and Blowfish, the data that needs to be safeguarded is encrypted. On the basis of the robustness of the encryption process, DES among them takes less time to execute, but AES performs better than the other two methods. The incorporation of human modes as a component of framing the security mechanism allowed this model to demonstrate its robustness in terms of data security.

The first absolute fingerprint pre-alignment method based on deep learning was presented by the authors in this paper [16], and it has been demonstrated to attain competitive accuracy. Their solution definitely exceeds all other pre-alignment algorithms in terms of the accuracy of the rotation estimation and the quantity of big deviations from goal values compared to other published methods. As shown by the fuzzy vault technique, this is necessary to obtain realistic biometric performance in fingerprint-based cryptosystems.

According to the authors of study [19], compared to passwords, PINs, or densely packed keys,

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

fingerprints are a highly resilient and dependable biometric template for the purpose of authentication. Additionally, it should be emphasized that there is a sizable variation between one individual's fingerprint specimens obtained at various times. As a result, it is assumed that the comparison task is probabilistic, which is actually the opposite of the exact matching of passwords or keys. False rejection rate (FRR) and false acceptance rate (FAR) are errors that can result from probabilistic matching and depend on a variety of factors, including the matching method. The two key processes that make up the system's core are improving fingerprint images and verifying a person's identity.

The authors of paper [20] demonstrate how biometric user template protection procedures give the biometric data security. Since fingerprints are one of the most popular biometric qualities, it is necessary to design methods to safeguard fingerprint template data. In this research, a strong method to safeguard the fingerprint template is suggested. It creates a three-dimensional, non-invertible fingerprint template based on various user key-sets by using the location of minute details and unique spots in the fingerprint image. In the suggested method, intra-class changes like rotation and translation have been taken into account.

The major goal of this research study [22] is to convey the fundamental ideas of SSO and the method for putting those ideas into practice using JOSSO. Numerous security problems and assaults result from the interaction among users and service providers through the Internet. This research effort has implemented SSO in JOSSO, allowing users to access numerous apps on several servers with a single user credential. A single set of credentials could be used to access numerous applications via various servers, and SSO also offers security by thwarting the attacks that are covered in this paper. If the user gives the correct login information and logs in to one application, they won't need to do again in order to accessibility another application on a different server. The main cloud service providers have a tendency to deliver their services using the SSO approach. Multi-factor authentication (MFA) will be used in conjunction with single sign-on (SSO) as part of this project's future growth to improve security and fend off other assaults.

WORK	METHODOLOGY & GOAL	BIOMETRIC MODALITY	APPROACH	ADVANTAGES	DISADVANTAGES
[11]	Key generation for an encryption technique using fingerprint templates	Fingerprint templates	Data dependent cryptography	High privacy for the storage of user information	Complicated and vulnerable to masquerage attacks.
[12]	Utilising discrete Fourier transform and random projection	Fingerprint templates	Hybrid transformation	Robustness of the authorized templates	More complex to analyze the system
[13]	PIN and random salting are used to create the cancelable biometric	Fingerprint templates	K-nearest neighbour approach	Unbreakable by intruders	Vulnerable to record multiplicity attacks

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

[14]	Utilising hash coding as a one-way transformation method	Fingerprint templates	Hash coding	Serves the revocability and linkability	Less performance due to suffering from accuracy loss
[16]	The algorithm for fuzzy commitment was utilised to decipher the intricate aspects.	Fingerprint templates	Several spiral curves using fuzzy concepts	Achieves blind authentication	The system suffers from the instability that leads to high FRR

Table 1: Summary of the Existing Surveys

Problems with the current methods:

An attacker can use a skimming device to retrieve user information from a smart card, which can subsequently be used for authentication.

1. If a user's smart card is misplaced, they can no longer be permanently authenticated.
2. The service provider's OTP, which is utilized for authentication, can be interrupted by an attacker.
3. One-time registration is only used to eliminate duplicate user IDs, but a DOS assault on the cloud can still be carried out by a single user with many registrations.
4. The user may lose all of the data stored in the cloud if their smart card is lost.
5. Adding a mechanism for password changes to the current system adds to the effort for IoT end devices.
6. The manufacturing of smart cards involves exponential computation, which is bad for Internet of Things (IoT) devices with limited resources.
7. Because the framework is hardware-based, there is still identity tracing and masquerade threats that can occur throughout the authentication process using the aforementioned method.

3. Motivation and Research Gap

It is evident from a survey of the literature that there are several strategies available for biometric authentication of user for accessing cloud services.

The algorithms mentioned below are all symmetric in design. These algorithms all rely on the data owner to enter the encrypted data, which is now developed enough to be uploaded to cloud storage. Data must be encrypted before being sent to cloud storage because the technology is still in its infancy with regard to security, even though it isn't as safe as our desktop.

One unanswered issue arises in this situation: Because we must always encrypt data before transmitting it onto cloud storage, why not create a system or algorithm that does it automatically? There is a void in the field as a result, and this work proposed an approach to fill it.

4. Proposed Architecture

A framework for fingerprint-based authentication is proposed in this study to lessen security and privacy risks in the cloud computing environment. It is suitable for end devices with limited

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

resources that are used to access the services and is the simplest method to manage user accounts for accessing various application services that use the Single Sign-On (SSO) concept, in addition to minimizing security assaults. The process flow of the fingerprint biometric authentication system is elaborated in figure 5 below:

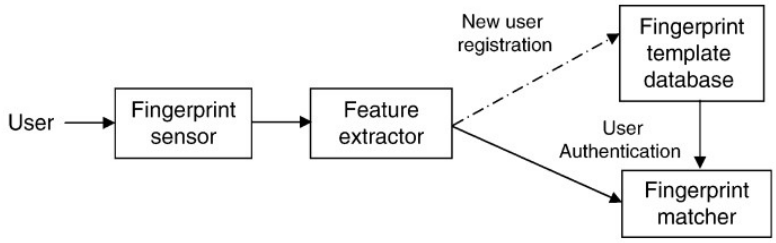

Figure 5 – Process Flow of Fingerprint System

A live-scan fingerprint scanner may rapidly and easily acquire a digital fingerprint picture of a fingerprint. The majority of these scanners sample the pattern at 500 DPI (Dots per Inch) and provide an 8-bit grayscale raw image (see Figure 6) [27].

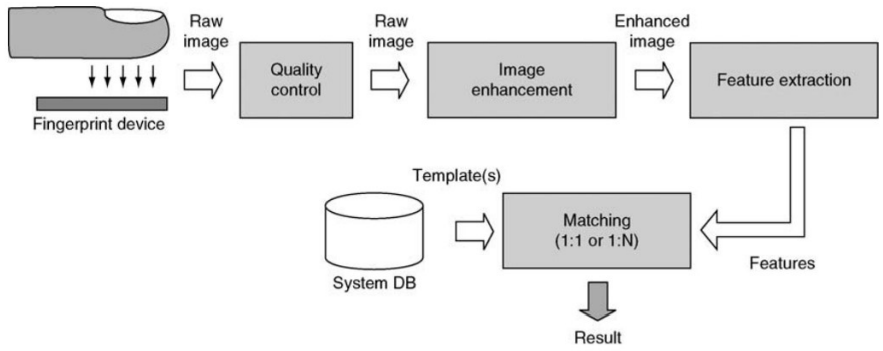

Figure 6 – Diagram of Fingerprint Biometric Recognition System [27]

The framework can be applied to social media platforms like Facebook and Twitter to stop users from creating duplicate accounts. It can also be used to get rid of duplicate accounts and bogus accounts. The following organizations are included in the suggested architecture:

1. User: An individual who requests to access cloud services
2. Client: A computer, workstation, or other device with internet access and fingerprint scanning capabilities. A feature extractor process scans the biometric data to extract the feature vector as shown in (Figure 6) after the biometric sensor has scanned the user's fingerprint using fingerprint scan technology.

   X = (x1, x2, x3, x4, ... , xn)

3. The cryptographic module: It is in charge of encrypting requests sent to the Registration and Verification Server (RVS) via registration requests utilizing the user's private key Epru(X), password hashing algorithm h(pwd), and user id (Ui). The secured information is determined as stated in (2) when a client tries to log in to a cloud service provider (CSP).

   S = (EPucsp(Ui)(EPru(X)))

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

4. **Registration & Verification Server (RVS):** In charge of user and cloud service registration and verification.

4.1 Registration Procedure:

The user's public key from (3) and RVS's private key can be used to calculate the secured information S.

S = (DPrrvs (Ui)h (pwd) (Dpuu (X))) (3)

where S=secured data received from the user

User Identity is Ui.

one-way collision-free hash function, h

Decryption utilizing the Registration and Verification Server's Private Key

Dpuu stands for decryption using a user's public key.

When RVS gets a request to register from an individual, it records an identity for the user that is decoded using the RVS private key, hashes the password, runs an encryption module with the user's public key, transforms the request via the verification module, and saves the outcome as a template to its database. Through a secure link, the user gets the registration reply from the responding RVS. Anybody can access cloud services by sending the SIDj (Cloud Service provider identity) to RVS, which is subsequently verified. The client receives a trust certificate as a result.

4.2 Verification Process:

The verification server in charge of confirming the user's fingerprint and identity. Si = Sj, where Si is the secured information given by the user during registration and Sj is the secured user information received by CSP, is what is matched when CAS forwards the user's request to the verification server. If the data is confirmed, an authentication response is sent to CAS.

5. LS (Login Server): It offers a user interface via which they can access cloud services. A user can log in to the cloud service portal using their fingerprint and user id (Ui) if they want to use the cloud services. The login server sends requests to the authentication server, which uses S as described in (4) to confirm the user's legitimacy.

   S= (EPucsp(Ui)(EPru(X)))

6. Authentication Server (AS):

It authenticates the user who is attempting to access the cloud. CAS Decrypts (Sj= (DPrcsp(Ui)(DPuu(X))) and compares Ui and (X) against data they previously have stored. The system forwards the request for RVS if it is made for the first time. If the user is authorized and the AS received an authentication response from RVS, it set the status bit to 1. If the user's request is not being sent for the first time, the system will check its database to see if the user's UI matches one that has already been stored, and the user's status bit will be examined. When a user enters the OTP that was sent to him by the CAS along with the trust certificate, the server checks his identification and sets the relevant user's status bit to 1.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

7. Application Server (AS): Offers the users the necessary applications, services, and data.

8. IoT Devices: A variety of IoT devices that can be found at the user or server end can provide real-time data to cloud servers.

4.1. Working method

Users must send a request containing their fingerprint scan, hashed password, and registration details to the registration and verification server in order to use cloud services for the initial instance. The feature extractor identifies and recovers the unique feature of the fingerprint when the client obtains the fingerprint scan. After being encrypted with the encryption key, these extracted features are subsequently transmitted to the registration and verification server through a secure connection. If the client is not previously registered, the data will be saved as a template. This encryption module is delivered to the registration and verification server, which then applies transformation and vector computation. When the biometric device is registered, the user can send a login request using the registered finger scan. The feature extraction and encryption modules follow behind the client, which is in charge of scanning. The CSP Login server also receives a login request. To verify the client's information, the Login Server sends the request to the Cloud Authentication Server, that approves it and passes it. When a client makes an initial request for cloud services, the authentication server forwards this fingerprint template to the registration and verification server. If the user has already requested cloud services, however, the authentication server authenticates itself by checking and updating the status bit. When the CSP asks the registration and verification server to validate a user, the server checks the template to modules that have previously been entered into their database. In the event that a match is found, it validates the user's credentials and sends them over a secure channel to the CSP. Upon verifying the user, the authentication server provides access to the cloud services that are appropriate for that particular user. Consequently, in the event that the user's request for a single login is approved, they will be able to access multiple Cloud Services via single Sign-On (SSO). The user can use his password credentials to send a request to the RVS to modify his fingerprint number.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

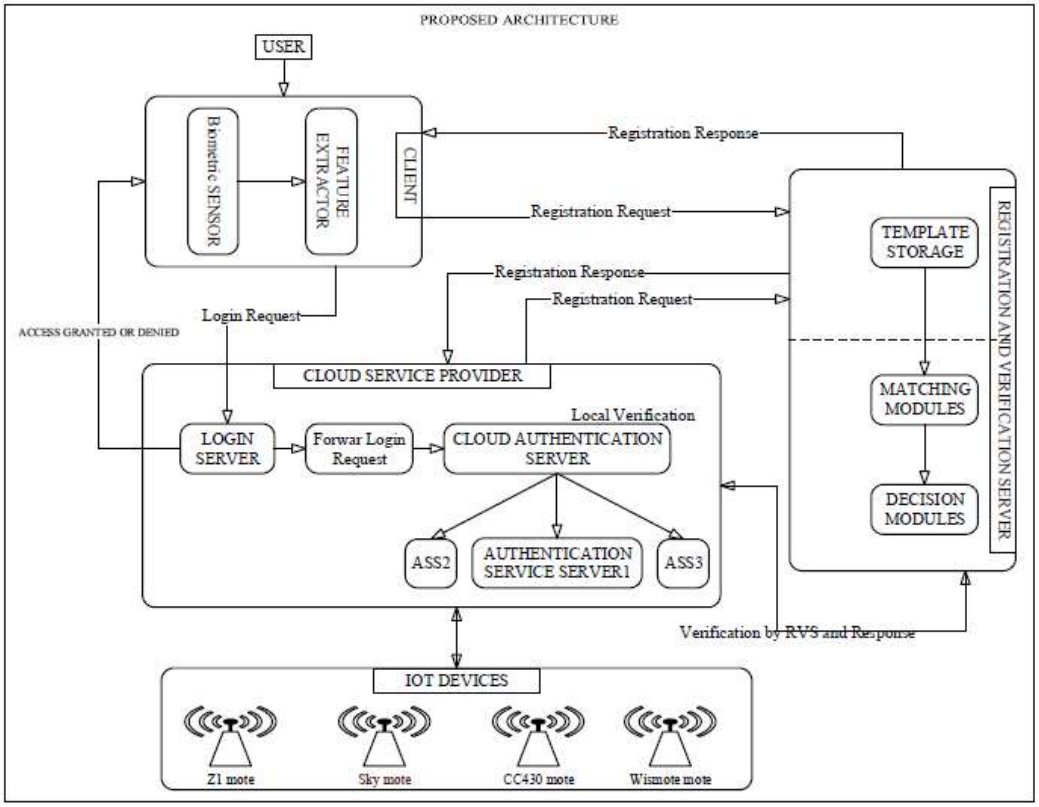

Figure 7 – Proposed Architecture

4.2. User Agent Registration Algorithm

Figure 2 shows how users can sign up for this algorithm through the Registration & Verification Server (RVS). For biometric authentication, the user first submits fingerprints to RS, which are later verified against the database. The agent registration request is denied by RVS if the same fingerprints are already present in the RS; otherwise, the fingerprints are saved in the database and registration is successful.

INPUT: **Users Provide Private Information**

USER PROVIDE FINGERPRINT TO RS

IF (FINGER_PRINT == EXIST)

RVS DENY USERS

END IF

ELSE IF (NEW_USER == TRUE)

RVS SAVE FINGER_PRINT

REGISTRATION SUCCESSFUL

RVS FORWARD TO AS

THEN,

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

AS SAVE THE_INFO ON ITS DB

END ELSE IF

ELSE

GO_TO_END

END ELSE

OUTPUT: **Users Registered**

4.3. Authentication Algorithm

The second algorithm addresses the verification and validation of the user. Figure 3 illustrates how the user provides information to the AS using biometric authentication. Based on the authentication information stored in databases at AS, a decision is taken regarding authentication.

INPUT: **Users provide Login Information**

USER PROVIDES PRIVATE_INFO TO AS

IF (FINGER_PRINT == TRUE)

IF (STATUS_BIT == 0)

STATUS_BIT = 1;

USER IS ALLOWED;

END IF

ELSE

USER IS DENYED

END ELSE

END IF

ELSE

USER IS BLOCKED

END ELSE

OUTPUT: **Users Logged into the Cloud**

4.4. Service provider Registration Algorithm

The service providers are registered using the registration ID provided to RVS by the cloud service provider. As seen in figure 4, the RVS issues a trust certificate after the cloud has been verified.

INPUT: Service Provider Request for Registration

CLOUD SENDS REGISTRATION ID TO RVS

RVS VERIFIES THE CLOUD AND PROVIDE TRUST CERTIFICATE

RVS FORWARDS THE CLOUD INFO TO AS

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

OUTPUT: Service Provider Registered

4.5. Service Access Algorithm

The duration as well as status of the login and logout times are tracked by the service access algorithm. The method can be expanded to include additional data based on the needs of the customer, such as the authentication key and service provider resource access. Figure 5 depicts the overall service access technique.

INPUT: **Login Information**

IF (LOGIN == TRUE)

STATUS_BIT = 1;

END IF

ELSE IF (LOGOUT == TRUE)

STATUS_BIT = 0;

END ELSE IF

ELSE

USER BLOCKED

END ELSE

OUTPUT: **Accessing Cloud Services**

5. Analysis of Security and Functionality

A number of current architectures are compared to the proposed architecture. Following are a few potential outcomes of the suggested architecture based on the comparative study:

- The usage of public key cryptography and biometric authentication reduce the vulnerability of cloud computing to security and privacy attacks.
- The architecture is appropriate for end devices with limited resources employed in a cloud computing environment since it does not require intensive data processing, an exponential computation process for authentication, or additional workloads like password changes.
- The failure of a dependable third-party server is the cause of the delay introduced in the earlier works.
- One user agent can only have one account for a variety of cloud application services, eliminating duplicate or fictitious user accounts at the cloud. Users and cloud services have a one-to-one relationship.
- The cloud-based data is not lost if the user's smart card is lost thanks to the biometric technique; the user can modify their fingerprint preference in the RVS by entering a secure password.
- The user can quickly modify their preferred finger number by sending an email to RVS with his password.
- Because RVS does not always require user identification, the computational cost is reduced.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

- A hacker trying to replicate the fingerprint utilizing mark tracked print is unable to access the services through mutual authentication as OTP is only provided to registered users' devices.
- By using the status bit, malevolent users are prevented from repeatedly logging in using the same user credentials, which reduces the risk of a DOS attack.

5.1 Comparative Analysis with Previous Security Models

Comparison Parameters	**[23] Park N. at. al.**	**[24] T.D.P. Bai**	**[25] B.B.Gupta**	**Proposed Model**
Authorization Method Used	eID Smart Card	Smart Card	Smart Card	Biometric
Technology Used	PACE & EAC Protocol	ECC	OTP	Fingerprint
Number of Hash Operations	6	2	4	5
Complicated modular or exponential operations	No	Yes	No	Yes
User-chosen credentials	No	No	Yes	Yes
Registration Entity participation in each session	No	Yes	No	No
Preventing fraudulent users from signing in repeatedly using the same credentials	Yes	No	Yes	Yes

Table 2: Comparison with other related schemes

5.2 Biometric Type Comparison

Following a review of a large number of research papers and materials, assessments are done based on a number of different areas of this subject, such as the identifying biometrics employed, biometric characteristics, physical attributes, technological features, assessment and other factors.

Biometric identifier	Distinctiveness	Complexity	Universality	Quantifiability	Performance	Comparison	Collect capacity	Acceptance	Cost	Use
Fingerprint	M	L	H	H	M	H	H	H	M	H
Iris	H	M	H	H	H	H	H	H	H	M
Facial	M	M	H	H	M	M	H	H	M	M
Palm	M	H	H	H	M	M	L	L	H	M
Ear	M	H	H	H	L	L	L	L	H	L
Footprint	M	H	M	M	L	L	L	L	H	L
Finger vein	H	H	H	L	H	H	L	L	H	L
Voice	M	H	H	M	M	M	L	L	H	L
Signature	L	H	H	H	L	L	M	H	L	L
Keystroke dynamics	L	M	M	L	L	L	L	L	H	L

H = High; M = Medium; L = Low

Table 3 - Using the features of biometric entities, a comparison of biometric types is made.

According to the traits of the biometric entities, Table 1 compares various kinds of biometrics.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

Below is a detailed explanation of each phrase used:

- Uniqueness: Every individual needs to have several traits that set them apart from other people.
- Complexity: The biometric shall grow largely stable after some time.
- Universality: Population distribution is universality. Each individual ought to possess their own biometric trait.
- Quantifiability: Measurable with simple technological resources. As a result, extraction is easy.
- Comparison: Compares the uniformity of two models, one of which is being saved and the other of which is a living model.
- Collect capacity: The efficiency with which data may be gathered and evaluated
- Performance: accuracy, quickness, and stability
- Acceptability: How well the system is received by users, taking into account cultural influences.
- Cost: The cost of using a biometric kind of identification.
- Use: The global adoption of biometrics

The table 3 contrasts a few of the biometric systems now in use in terms of accuracy, price, the number of devices needed, and social acceptability. The tables below show that fingerprint has a nice balance in regards to everything.

Biometric Technology	**Accuracy**	**Cost**	**Devices Required**	**Social Acceptability**
DNA	High	High	Test equipment	Low
Iris recognition	High	High	Camera	Medium-low
Retina	High	High	Camera	Low
Facial recognition	Medium-low	Medium	Camera	High
Voice recognition	Medium	Medium	Microphone, telephone	High
Hand Geometry	Medium-low	Low	Scanner	High
Fingerprint	High	Medium	Scanner	Medium
Signature recognition	Low	Medium	Optical pen, tourch panel	High

Table 4 - Comparison of Different Biometric

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

5.3 Pros and Cons of Various Biometric Authentication Schemes:

The technology known as biometrics is used to measure and analyse human features such as DNA, fingerprints, iris patterns, and facial recognition. Biometrics is a special way of identifying features for security purposes in a different way than a standard password or security code. In the table given below (Table 3) some advantages (Pros) and disadvantages (Cons) of various biometric authentication schemes are given.

Biometric Authentication scheme	*Pros*	*Cons*
Finger vein high-dimensional space self-stabilization (FVHS)	• combines the use of machine learning, biometrics, and cryptography technology. • Flexible and convenient. High accuracy with Genuine Accept Rate of more than 99.9%.	• It mainly depends on the finger vein biometric, and it does not contain any other authentication mechanism like, password. It is a unimodal biometric which could fail in the case of finger vein recognition failure.
Multimodal Biometric Systems (MBS)	• best performance in terms of security because they provide multiple information for authentication. • provides protection against spoofing attack. • Reliability. • Automation.	• Increases the system complexity. • Needs large storage. • Bad user experience.
Cloud based biometric authentication system using Microsoft cognitive face API.	• The model provides confidentiality by encryption using AES. • Accuracy. • Scalability.	• Dependency on face recognition only for authentication. • High computation time due to transmission between Microsoft API and Dropbox.
Face authentication processes for accessing cloud computing services using iPhone.	• LBP-based technique is used to reduce the computation time. Histogram equalization used to improve face detection in low brightness conditions.	• Dependency on face recognition only for authentication. • High privacy risk if compromised. • Not accurate in the case of facial expressions change
Palm-print biometric authentication	• Easy to capture • Easy to implement • easily detected in the case of low brightness and resolution	• Authentication accuracy can be affected in the case of injuries. • High privacy risk if compromised.
Fingerprint biometric authentication	• High user acceptance. • Easy to use. • Low error rate.	• Authentication accuracy can be affected in the case of injuries. • High privacy risk if compromised.
Keystroke biometric authentication	• Does not need any additional hardware device. • Cost effective • Reduces privacy risk • Suitable for multi-factor authentication systems.	• Not suitable for all type of systems; it cannot be used in banking systems or mobile devices.

Table 5 – Summary of Biometric Authentication Schemes in the Cloud

6. Conclusion

Providers of cloud computing services are scattered over the market and expanding swiftly in order to offer customers with the conveniences of adequate resource computation and storage. This study uses fingerprint-based authentication in particular to discuss the history of achieving cloud computing security through biometric techniques. According to the architecture that has been built, it is possible to reduce security assaults that have happened in cloud computing and get rid of fake accounts by exhibiting fingerprint-based authentication throughout the registration process. Users of end devices with restricted resources can be encouraged to access cloud services because the suggested algorithm uses several cloud application services and provides a single

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

SSO login. However, since consumers may place their fingerprints on any object and offenders can use that surface for authentication, fingerprint-based authentication solutions still have a vulnerability. By including the finger's pulse rate, a security problem can be fixed. Performance study using AVISPA and framework installation in the future could be used to validate the suggested architecture.

Reference

[1] N. Mansouri, R. Ghafari, B. Mohammad Hasani Zade, Cloud computing simulators: A comprehensive review, Simulation Modelling Practice and Theory, Volume 104, 2020, 102144, ISSN 1569-190X, https://doi.org/10.1016/j.simpat.2020.102144

[2] I. Indu, P.M. Rubesh Anand and Vidhyacharan Bhaskar, Encrypted Token based Authentication with Adapted Security Assertions Markup Language Technology for Cloud Web Services, Journal of Network and Computer Applications, https://doi.org/10.1016/j.jnca.2017.10.001

[3] Alemami, Yahia & Al-Ghonmein, Ali & Al-Moghrabi, Khaldun & Afendee, Mohamad. (2023). Cloud data security and various cryptographic algorithms Corresponding Author. International Journal of Electrical and Computer Engineering (IJECE). 13. 1867-1879. 10.11591/ijece.v13i2.pp1867-1879.

[4] Sai Siddhartha Chary Aylapuram, Challenges of Implementing Cloud Security System Through Identity, Access & Risk Management [IARM] In a Hybrid IT Environment, Turkish Journal of Computer and Mathematics Education Vol.13 No.03(2022), 691-698, https://turcomat.org/index.php/turkbilmat/article/view/13098/9376

[5] D. Anand, V. Khemchandani , Munish. S., O. Cheikhrouhou, O.B. Fredj, Security and Communication Networks, Volume 2021, Article ID 9940183, 15 pages, https://doi.org/10.1155/2021/9940183

[6] Jacqueline Lam, Introduction to Single Sign-On, https://www.geeksforgeeks.org/introduction-of-single-sign-on-sso/

[7] Vijay Koundinya, Shwetha Baliga, "A Review on Single Sign on as an Authentication Technique",IRJET,Volume 7, Issue 6, June 2020.

[8] Al-Assam, H., Hassan, W., Zeadally, S. (2019). Automated Biometric Authentication with Cloud Computing. In: Obaidat, M., Traore, I., Woungang, I. (eds) Biometric-Based Physical and Cybersecurity Systems. Springer, Cham. https://doi.org/10.1007/978-3-319-98734-7_18.

[9] Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). Security and accuracy of fingerprint-based biometrics: A review. Symmetry, 11(2), 141.

[10] B.B. Gupta, Megha Quamara, An identity based access control and mutual authentication framework for distributed cloud computing services in IoT environment using smart cards, Procedia Computer Science, Volume 132, 2018, Pages 189-197, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2018.05.185.

[11] Bachkar Tejashri, Bangar Gitanjali, Sonawane Monali, Shinde Bipin, Journal, I. R. J. E. T. (2020). IRJET- STUDY PAPER ON VARIOUS SECURITY MECHANISM OF CLOUD COMPUTING. IRJET, Volume:07, Issue:02,Feb 2020, https://www.ijrti.org/papers/IJRTI2208034.pdf

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

[12] Zhang Rui, Zheng Ya, "A Survey on Biometric Authentication: Toward Secure and Privacy Preserving Identification," IEEE Access, Volume 7, January 16, 2019.

[13] Carmel, V. V., & Akila, D. (2020). A survey on biometric authentication systems in cloud to combat identity theft. Journal of Critical Reviews, 7(03), 540-547.

[14] Joseph, T., Kalaiselvan, S. A., Aswathy, S. U., Radhakrishnan, R., & Shamna, A. R. (2021). RETRACTED ARTICLE: A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment. Journal of Ambient Intelligence and Humanized Computing, 12(6), 6141-6149.

[15] Sarkar, A., Singh, B.K. A review on performance, security and various biometric template protection schemes for biometric authentication systems. Multimed Tools Appl 79, 27721–27776 (2020). https://doi.org/10.1007/s11042-020-09197-7

[16] B. Dieckmann, J. Merkle and C. Rathgeb, "Fingerprint Pre-Alignment based on Deep Learning," 2019 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 2019, pp. 1-6.

[17] Nguyen TAT, Dang TK, Nguyen DT (2019) A new biometric template protection using random orthonormal projection and fuzzy commitment. In: Lee S, Ismail R, Choo H (eds) Proceedings of the 13th international conference on ubiquitous information management and communication (IMCOM) 2019. IMCOM 2019. Advances in Intelligent Systems and Computing, vol 935. Springer, Cham

[18] Sarkar A, Singh BK (2018) Cryptographic key generation from cancelable fingerprint templates. In: 2018 4th international conference on recent advances in information technology (RAIT), Dhanbad, pp 1–6. https://doi.org/10.1109/RAIT.2018.8389007

[19] S. Hemalatha, "A systematic review on Fingerprint based Biometric Authentication System," 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Vellore, India, 2020, pp. 1-4, doi: 10.1109/ic-ETITE47903.2020.342.

[20] Syed Sadaf Ali, Vivek Singh Baghel, Iyyakutti Iyappan Ganapathi, Surya Prakash, Robust biometric authentication system with a secure user template, Image and Vision Computing, Volume 104, 2020, 104004, ISSN 0262-8856, https://doi.org/10.1016/j.imavis.2020.104004

[21] M VK, Venkatachalam K, P P, Almutairi A, Abouhawwash M. 2021. Secure biometric authentication with de-duplication on distributed cloud storage. PeerJ Computer Science 7:e569 https://doi.org/10.7717/peerj-cs.569

[22] Prakash V, Sridevi J, "Secured identity management using single sign- on in private cloud ", International Journal of Science & Engineering Development Research (www.ijrti.org), ISSN:2455-2631, Vol.7, Issue 8, page no.211 - 218, August-2022, http://www.ijrti.org/papers/IJRTI2208034.pdf

[23] Park, N., & Lee, D. (2017)"Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment." Personal and Ubiquitous Computing 1–8.

[24] Bai, T. D. P., Raj, K. M., &Rabara, S. A. (2017, February)"Elliptic Curve Cryptography Based Security Framework for Internet of Things (IoT) Enabled Smart Card."2017 World Congress on Computing and Communication Technologies (WCCCT)IEEE 43–46.

[25] B.B. Gupta, Megha Quamara, An identity based access control and mutual authentication

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

framework for distributed cloud computing services in IoT environment using smart cards, Procedia Computer Science, Volume 132, 2018, Pages 189-197, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2018.05.185.

[26] N. Bhartiya, N. Jangid and S. Jannu, "Biometric Authentication Systems: Security Concerns and Solutions," 2018 3rd International Conference for Convergence in Technology (I2CT), Pune, India, 2018, pp. 1-6, doi: 10.1109/I2CT.2018.8529435.

[27] Maltoni, D. (2009). Fingerprint Recognition, Overview. In: Li, S.Z., Jain, A. (eds) Encyclopedia of Biometrics. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-73003-5_47

[28] Rousan, Mohammad & Benedetto, Intrigila. (2020). A Comparative Analysis of Biometrics Types: Literature Review. Journal of Computer Science. 16. 1778-1788. 10.3844/jcssp.2020.1778.1788

[29] Nguyen HT. Fingerprints classification through image analysis and machine learning method. Algorithms 2019;12(11):241.

[30] Yang, J., Wu, Z. and Zhang J., A robust fingerprint identification method by deep learning with Gabor filter multidimensional feature expansion; 4th international conference, icccs 2018, Haikou, China, June 8–10, 2018, pp. 447–57.

[31] Michelsanti D., Ene, A.D., Guichi, Y., Stef, R., Nasrollahi, K. and Moeslund, T.B., Fast fingerprint classification with deep neural networks, Visual Analysis of People (VAP) Laboratory, Aalborg University, Aalborg, Denmark, 2017. ISBN: 978-989-758-226-4, DOI: 10.5220/0006116502020209.

[32] A. K. Jain, D. Deb and J. J. Engelsma, "Biometrics: Trust, But Verify," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 4, no. 3, pp. 303-323, July 2022, doi: 10.1109/TBIOM.2021.3115465.

[33] https://www.m2sys.com/blog/guest-blog-posts/what-role-will-biometric-authentication-play-in-the-post-pandemic-world/

[34] Habibu, T., Talina Luhanga, E., & Elikana Sam, A. (2022). Assessment of How Users Perceive the Usage of Biometric Technology Applications. IntechOpen. doi: 10.5772/intechopen.101969