JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.2132-2142
https://publishoa.com
ISSN: 1309-3452

Biometric Authentication for Cloud Services

1. **Mr. Md. Ilias**, Assistant Professor, CSE, St. Peter’s Engineering College, Telangana, India.
2. **K Santosh Kumar**, Student (B. Tech-CSE), St. Peter’s Engineering College, Telangana, India.
3. **K Nandini**, Student (B. Tech-CSE), St. Peter’s Engineering College, Telangana, India.
4. **Md Arief**, Student (B. Tech-CSE), St. Peter’s Engineering College, Telangana, India.
5. **M Rishikesh**, Student (B. Tech-CSE), St. Peter’s Engineering College, Telangana, India.
6. **K Kavya**, Student (B. Tech-CSE), St. Peter’s Engineering College, Telangana, India.

Received 2022 April 02**; Revised** 2022 May 20**; Accepted** 2022 June 18

Abstract—as we manage our data, there is a growing need for remote information storage and computing solutions, which raises the need for services that provide secure access to data. In this paper, we suggest a brand-new biometric authentication system that offers safe access to a remote server. We treat the user's biometric information as a secret recommendation in the suggested method. We then obtain a distinct identity from the customer's biometric data, which is used to construct the individual's personal trick. Along with that, we offer a solid method for creating a session key between two connected events using two biometric templates for secure messaging. In other words, the user's private information does not need to be saved anywhere, and the session secret is created without revealing earlier information. The suggested method holds up against numerous known attacks against (easy/ energetic) opponents, according to a thorough Real-Or-Random (ROR) version based on official safety analysis, informal (non-mathematical) safety and security analysis, and official safety confirmation using the widely used AVISPA (Automated Recognition of Net Safety Method and Applications) tool. Finally, numerous trials and comparative research have demonstrated the efficacy and efficiency of the proposed strategy.

Keywords—Authentication; Privacy; Multifactor; Identity; security.

I.INTRODUCTION

A variant of on-demand network access to reconfigurable computer resources, such as networks, web servers, storage areas, applications, and solutions, is called cloud computing. The information processing services available in today's technologically evolved world can be compared to cloud computing, which is an improved version of those services. According to NIST, the cloud is defined as "a version that permits common, practical on-demand network access to a shared pool of programmable computer resources that may be quickly and briefly distributed with relatively little maintenance." Cost and cost savings for infrastructure. Cloud computing is typically thought of as a

shared service on a big scale, thus both the person and the service need to be verified to ensure the privacy and dependability of the cloud solution offered. Disregard, stability, and schedule are essential components of cloud computing. Because the data is stored in a distributed database, keep it private. Integrity refers to a feature that forbids unauthorised people from accessing data. Information that is freely accessible at any time is referred to as being available. A requirement to prevent access to the cloud solution from being restricted to those who access information saved within the cloud service is individual authentication. To validate and access cloud computing solutions, the person must be acknowledged by one or more recognition mechanisms. Password, biometric traits, and other things. Our approach involves testing out a variety of current authentication methods. The study used two excerpts from a study of attacks on information kept in cloud solutions to focus on information security and privacy in cloud computing. The types of evidence are then discussed throughout the study, along with a brief analysis of each type. The main goal of this work is to provide a thorough background analysis of biometric authentication techniques used in cloud computing services. We categorise all currently used biometric authentication methods into two categories: those that use physical biometric attributes and those that use behavioural biometric attributes. The article acknowledges most of the important verification techniques that have been used or developed and provides a quick overview of the biometric behaviour used for verification, reasons for recognition, strengths, and drawbacks.

II.LITERATURE SURVEY

Using biometrics to confirm

the goal of biometric verification is to identify a person based on their physical or behavioural characteristics. Recognition, authentication, and non-rejection are the three primary variables that biometric authentication typically supports when identifying a person's physical and behavioural features. The conventional form of verification, which employs key-based cryptographic techniques, has been supplanted by this one. A fixed authentication method that can be used to confirm a person at the start of the procedure itself is biometric verification. The process of biometric verification is thoroughly divided into a physical biometric technique and a behavioural biometric approach.

Fingerprint - No two people have the exact same finger print, making it a unique characteristic of persons. Therefore, while performing verification, this is strong evidence of the customer's individual identification. Sub-characteristics such passing over, core, bifurcation, ridge discontinuity, island, delta, pores, and so on were used to identify fingerprint patterns. finger print evidence's calibre. Additionally, this verification is useless for those whose fingerprints are removed over time, such as long-term employees, the elderly, etc. disappeared. The usage of this authentication requires additional hardware, just like other physically based biometric verification techniques.

III. CURRENT SYSTEM

This section focuses primarily on individual authentication plans that already exist and are biometrically based. The three groups that make up the customer authentication process can be distinguished based on the sorts of evidence and components that were used: One-factor, two-factor, and three-factor models are the first three.

In a single element authentication mechanism, such as a smart card or personal biometrics, just one element can be used. Individual passwords and smart cards or mobile phones can both be used with the two-factor verification system. In

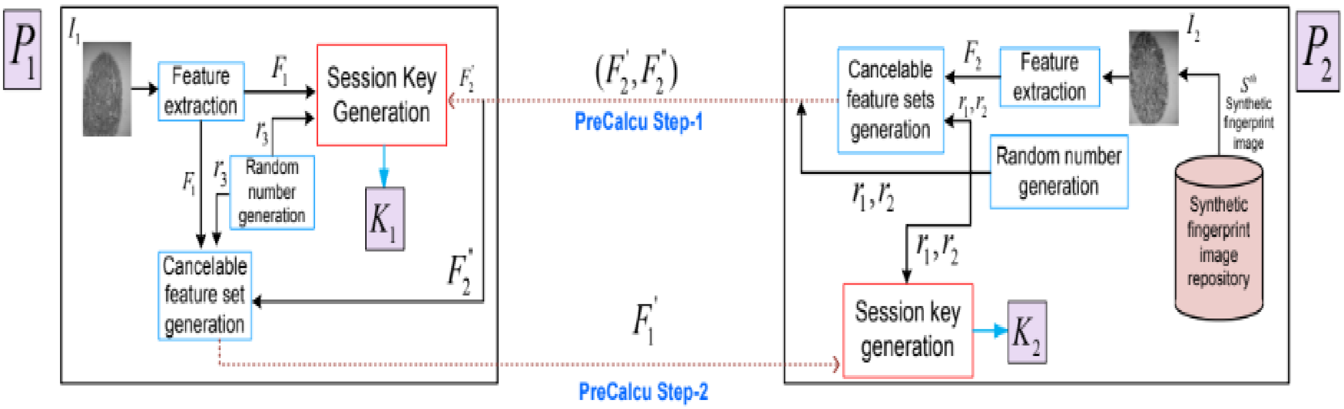


Figure 1PreCalcu Process

contrast, a three-factor verification scheme allows for the usage of a customer's chip card or smart phone, password, and biometrics. For cordless sensing unit networks, Jiang et al. offer a password-based individual authentication method (WSN). Due to its reliance on a smart card and a password, this authentication strategy uses two factors. The approved person registers or re-registers the dependability gateway node during the individual registration process (GW N). The relevant letters of evidence are then provided on the chip card by GW N together with the smart Map. Additionally, the GW N secure network is used to tape-record all input sensor nodes and retrieve their unique secret login credentials. The trusted user verifies the specified sensing unit node using GW N during the login and authentication phase using pre-recorded evidence letters. However, Das later on disclosed that this specific strategy is vulnerable to internal attacks, where a trusted insider (i.e., an attacker from within) could connect various other attacks to the system, such as impersonating the individual attacks, using the registered user's registration information. Additionally, this system stands out since it did not support new ones that placed the sensor node in the target field and did not provide excellent proof. Das advocates a better and more effective three-factor authentication method, where the three factors are an intelligent card, the user's password, and their unique biometric data. The Das-proposed approach, however, did not protect the privacy of the sensing unit node. In fact, Althobaiti et al. created a biometric user identification system for WSN. However, their plan offers no protection against man-in-the-middle attacks or acting. Das then offered a fresh biometric strategy for user authentication. An similarly genuine fundamental structure based on a short-term requirement system for WSN was also proposed by Xue and others. Additionally, they demonstrate that Xue et alsystem .'s lacks protection against user impersonation, offline password forecasting, adjustment, and replicating assaults on sensing unit nodes.

For wireless sensor networks, Wang and Wang suggested various homes of personal privacy perversion in two-factor authentication approaches (WSNs). To demonstrate the difficulties and nuances involved in developing two-facto authentication for ensuring privacy for WSNs, they created two separate sample systems. A game-based security mechanism for two-factor authentication was also introduced. To highlight the challenges with mobile device authentication techniques, Wang et al. suggested three potential identity-based user authentication schemes. They also considered session information attacks on short-term information, attacks on impersonation, and poor usability. To provide security in cordless sensor networks and mass storage devices, numerous different authentication processes have also been presented in the literature.

IV.PROPOSED METHODOLOGY

In this section, we first discuss the suggested biometric-based authentication system's system version and danger model before presenting its numerous stages.

Creating Systems

Figure 1 presents an introduction to the biometric verification system. containing three distinct entities. Client (C), authentication web server (AS), and a few distant servers are among these entities (RS). While RS generates the personal key for AS at the implementation stage and shares it with AS, AS has a database of registered individual data. Additionally, both AS and RS have a sizable database with an identical set of artificial fingerprint images. The suggested technique makes use of some publicly accessible artificial finger print databases.

If C wants to use the RS solution, C notifies AS of its need for verification.

Following a successful confirmation, AS replies to C. C sends the solution request to RS for access as soon as it receives the message in response to the recommendation. The service demand is verified by RS. If the service request is successfully confirmed, RS notifies C and delivers a confirmation response. C and RS both confirm one another. For more secure message exchange, a session secret is employed between C, AS, and C, as well as RS. Additionally, the message authenticator verifies the communication's trustworthiness.

Customer enrollment and individual authentication are the two main steps in the biometric authentication system. Individual registration necessitates the creation of private keys, whereas user verification calls for the creation of session keys and message authenticators. The user's private key can be rolled over using this strategy's functionality. Additionally, it overcomes the inherent flaws of biometric authentication and is secure and computationally less expensive. A small number of keys must be managed from both the application's and the user's perspectives, but it also does not require pre-shared secrets and offers a seamless shared authentication mechanism.

The stages in our suggested model are listed below.

A. Exclusive Crucial Generation for Users

First, we remove all the irrelevant information from the fingerprint image of the person. Align the image with the finger print first to improve the function's extraction accuracy. Right now, we select that usual location. Consistent area is the finger print place that has a high likelihood of appearing in any type of fingerprint image that has been acquired. To keep track of small details, we chose this usual place. We suggest using the horizontal section to select a set of minute elements from a dependable place. The picture's horizontal part is a short area with the greatest diversity of insignificant factors. We chose the details such that a Trellis convolution coding diagram and a code name could be created. Let's look at this codeword as BioCode, which can be used to generate a personal vital Kc as Kc = H (BioCode Kr), where Kr is an arbitrary number generated by C's programme, H suggests any kind of hash features (e.g., Protect Hash Algorithm (SHA-1)), and indicates one-way change of two input criteria, which is much easier to calculate in forward instructions but not in backward instructions. SHA-256 can also be used to achieve strong security.

B. Secret Generation Session

To create a session trick between two concepts P1 (i.e., client C) and P2 (i.e., the authentication server AS), we took information from two different biometric fingerprints for each of them. P1 recorded a synthetic fingerprint image, while P2 likewise took a finger print C photograph. Seating The PreCalc technique is the primary generating process. When P1 loads its application to start a session, the procedure begins. PreCalc includes PreCalc Steps 1 and 2, as seen in Figure 2. P1 will fill out the application on their computer, and P2 will run PreCalc step 1 after that. In response to feedback from P2, P1 executes PreCalc step 2 in P1.

Step 1 of PreCalcu P2 selects a fake fingerprint image at random from the data source in this stage. Permit P2 to choose Sth (state I2) synthetic picture at random.

Extraction of I2 features based on line angles: Allow M2 = m21, m22, - - -, where n2 is the number of minutiae factors in I2 and m2n2 is the collection of all extracted trivial matters points in enhancing order of their x coordinate values. It is calculated to find the Euclidean distance between two unimportant components, claim m2i and m2(i +1), where I = 1 to n2 - 1. The length of the line connecting the points x and y is the euclidean distance between them. If x = (x1, x2, - - -, xn) and y = (y1, y2, - - -, yn) are two elements in the Euclidean space, then the range (d) between x and y is given by the Pythagorean formula as d (x, y) = d (y, x) = i= 1n (xi yi) 2. Additionally, we determine the angle of the web connecting m2i and m2(i + 1). It's important to remember that the angle of inclination is the angle formed by a straight line and the x-axis. Let F2 be the set of tuples with I = 1 to n2 1, where l2i denotes the Euclidean space and a2i denotes the angle between m2i and m2(i +1) in M2. F2=, to put it simply.

We create two cancelable function collections, F2|and also F2||, to create the cancellable attribute set from F2.

PreCalcu Step-2: P1 captures a picture of C's finger print (claim I1) and also performs the subsequent steps:

Feature removal from I1: Here, features are extracted from I1 using the same line-angle-based feature removal technique, resulting in the creation of the attribute set F1.

Session key generation by P_1: Using $F_2^{|}$, P_1 calculates $K_1^{|}$ as,

$K^{|}_1=\{[(l_{21}*r_2)^a{}_{21}*r_1 \mod p]^a{}_{11}*r_3 \;x\; \{(l_{22}*r_2)^a{}_{22}*r_1 \mod p]^a{}_{12}*r_3 \;x\; \ldots\; x[(l_{2T}*r_2)^a{}_{2T}*r_1 \mod p]^a{}_{1T}*r_3\}$

Here, r_3 is a randomly generated number by P_1. P_1 then calculates the hash key of $K_1^{|}$ using any hash function H(.) to get a session key K_1.

Generation of cancellable function set from F1: P1 makes F1 cancellable via the usage of F2generation at P2: P2 uses and the functions of I2 for the era of session key.

P2 then calculates the hash key of the session key produced (say K2both the generated keys K1 and K2 are the identical. And this is how we create a session key among communication parties.

C. User Registration

Each C and AS use their cutting-edge session key, say K, and BioCAP uses PreCalcu technique previous to the registration device. C plays the subsequent. Block-based extraction of the entire function: C's software program takes a clean fingerprint photo of C, permit's anticipate Ireg. From Ireg, we take trivialities elements and create minutiae pairs. We to start with partition Ireg into some of little rectangular blocks so that it will produce a few trivialities elements (Fig. Three(a)). We stroll spherical every block in Ireg, making the pairings of minute elements by using taking into consideration all of the trivial factors which can be particular to every block and all of the trivial elements which might be specific to its 8 associated surrounding blocks. By shifting through each block one after the other, we are able to create trivialities factor pairs. We determine the Euclidean angles and distances of each of the straight away received strains.

We create trivia pairings thru the use of considering a center element and each triviality issue that is part of the 8 blocks that surround the recognized centre element (Fig. Three(b)). In a similar manner, we pick out the delta element and each minute factor from the 8 associated blocks that surround the block in which the delta trouble have become discovered (Fig. Three(c)). We compute the Euclidean distances and angles for each pair that is produced the usage of the middle difficulty and delta element. The delta element, which takes area on a friction ridge at or near the detail of divergence of type strains, is seemed as a fingerprint pattern in biometrics and fingerprint scanning.

Let F1 constitute a fixed of the Euclidean distances (li) and angles (ai) of each pair for all of the blocks, F2 denote a tough and speedy) of every pair the usage of the

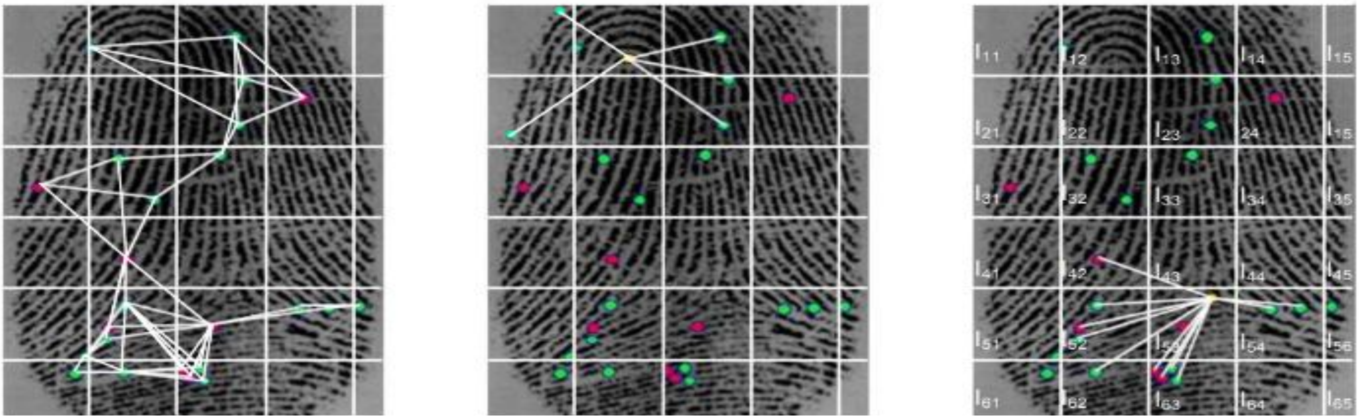


Figure 2(a) Straight lines detected using all the blocks; (b) Straight lines detected using core point; (c) Straight lines detected

middle problem, and permit F3 denote a hard and fast of the Euclidean distances (lithe usage of delta issue, then F1= (l1, a1), • • •,(lz1,az1), F2 =,a1, and F3= wherein z We create a common set via concatenating F1, F2, and F3. Let Freg be a commonplace set, with dimensions of z = z1 + z2 + z3, such that Freg = F3.

Freg encryption through Kc use Using Kc (C's private = EKc(Freg), wherein E stands for an encryption feature, we encrypt Freg.

Calculation of C's biometric index: During authentication, AS wants to get proper of access to C's registered statistics in AS's database. We endorse the following use of a biometric index to rush up retrieval. The biometric index of C is first of all calculated using C's BioCode (see Section III-C) as follows: Bx = H(GxBioCode), wherein Gx is quite a number of generated through AS at some point of the software deployment mechanism and is stored in C's software application. Gx is a not unusual huge variety that is to be had to all customer apps, and as a quit end result, AS can appropriately send the encrypted Gx to all Cs with the beneficial resource of using the already installation session key K.

Calculating the rollover parameter (R) for C In the event that C desires to rollover (or trade) KC at a later time, we suggest a rollover parameter. Utilizing Kr and C's private key KC, we will parent out C's rollover parameter. Let Kr be the random integer created inside the path of the manufacturing of C's private key, and allow R be the rollover parameter of C. R also can moreover then be obtained as Kr = H(Kr KC) (see Eqn. 1). Using the BioCode hash key, we encrypt Kr. Let Kb be the BioCode hash key, it truly is Kb = H. (BioCode). We encrypt Kr via Kb. Krshape of Kr, please. Additionally, we use the consultation to encrypt Bx simply so it may be utilized in encrypted shape. Allow AS to apply Rform of R at the give up. Using the maximum modern session key K, AS decrypts Bx and obtains Bx and R, consequently. As fast as ASstoresreg, Bx, R, and Kin within the database, the registration method is completed.

User authentication, factor D

The PreCalcu approach of generating session keys is the first step in the authentication technique for a person. Let K serve as the modern consultation key among C and AS.Each C and AS use their cutting-edge consultation key, say K, and BioCAP makes use of PreCalcu technique previous to the registration gadget. C performs the following. Block-based totally absolutely extraction of the entire feature: C's software takes a smooth fingerprint photograph of C, let's say Ireg. From Ireg, we take trivia factors and create minutiae pairs. We initially partition Ireg into some of little rectangular blocks a terrific manner to supply some trivia factors (Fig. Three(a)). We stroll spherical each block in Ireg, making the pairings of minute elements via considering all the trivial factors which might be specific to every block and all the trivial points which might be particular to its eight linked surrounding blocks. By shifting via each block separately, we are capable of create trivialities thing pairs. We decide the Euclidean angles and distances of each of the at once acquired traces.

We create trivia pairings thru thinking about a middle problem and every triviality trouble this is part of the 8 blocks that surround the diagnosed centre component (Fig. Three(b)). In a similar manner, we select out out the delta element and every minute factor from the 8 related blocks that surround the block in which the delta detail turn out to be positioned (Fig. Three(c)). We compute the Euclidean distances and angles for every pair this is produced the use of the middle component and delta issue. The delta difficulty, which takes place on a friction ridge at or close to the element of divergence of kind strains, is seemed as a fingerprint sample in biometrics and fingerprint scanning.

Let F1 constitute a difficult and rapid of the Euclidean distances (li) and angles (ai) of every pair for all the blocks, F2 denote a hard and fast) of each pair the usage of the middle factor, and permit F3 denote a hard and speedy of the Euclidean distances (lithe usage of delta issue, then F1= (l1, a1), • • •,(lz1,az1), F2 =,a1, and F3= in which z We create a not unusual set through concatenating F1, F2, and F3. Let Freg be a not unusual set, with dimensions of z = z1 + z2 + z3, such that Freg = F3.

Freg encryption thru Kc use Using Kc (C's non-public = EKc(Freg), wherein E stands for an encryption feature, we encrypt Freg.

Calculation of C's biometric index: During authentication, AS desires to get right of entry to C's registered records in AS's database. We propose the following use of a biometric index to rush up retrieval. The biometric index of C is initially calculated the use of C's BioCode (see Section III-C) as follows: Bx = H(GxBioCode), wherein Gx is quite various generated with the aid of AS all through the utility deployment mechanism and is stored in C's software. Gx is a not unusual variety that is to be had to all patron apps, and as a give up end result, AS can effectively send the encrypted Gx to all Cs through the use of the already set up consultation key K.

Calculating the rollover parameter (R) for C In the occasion that C desires to rollover (or exchange) KC at a later time, we propose a rollover parameter. Utilizing Kr and C's personal key KC, we are able to decide out C's rollover parameter. Let Kr be the random integer created in the course of the manufacturing of C's private key, and permit R be the rollover parameter of C. R also can then be acquired as Kr = H(Kr KC) (see Eqn. 1). Using the BioCode hash key, we encrypt Kr. Let Kb be the BioCode hash key, that is Kb = H. (BioCode). We encrypt Kr with the beneficial resource of Kb. Krshape of Kr, please. Additionally, we use the consultation to encrypt Bx in order that it could be carried out in encrypted form. Allow AS to use Rform of R on the end. Using the most latest session key K, AS decrypts Bx and obtains Bx and R, therefore. As short as ASstoresreg, Bx, R, and Kin inside the database, the registration manner is finished.

User authentication, element D

The PreCalcu approach of manufacturing consultation keys is step one within the authentication way for a person. Let K function the modern-day-day consultation key among C and AS.

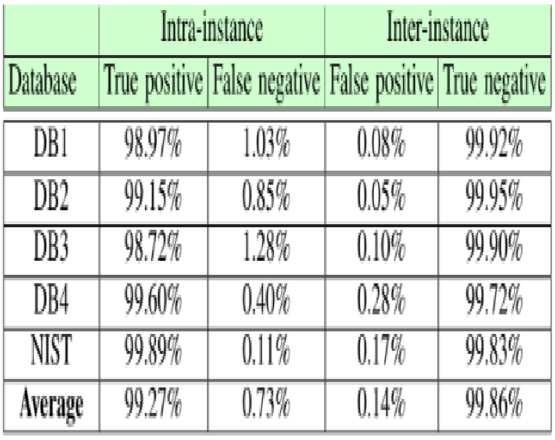
There are levels to the character authentication procedure.

The exercise's name is obtained with the beneficial aid of C within the first phase, and inside the 2d, he uses the records to deliver his biometric feature to AS for verification features. The authentication way in further detail is as follows:

There are degrees to the person authentication technique.

The game's name is received with the resource of C within the first phase, and within the 2nd, he makes use of the records to deliver his biometric characteristic to AS for verification abilities. The authentication approach in similarly element is as follows:

- C's Request$_1$ to AS
- AS's Reply$_1$ to C
- C's Request$_2$ to AS
- AS's Reply$_2$ to C
- C's request to RS
- RS's reply to C
- C's service access

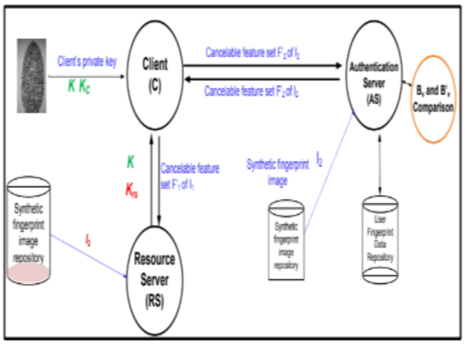


	Intra-instance		Inter-instance	
Database	True positive	False negative	False positive	True negative
DB1	98.97%	1.03%	0.08%	99.92%
DB2	99.15%	0.85%	0.05%	99.95%
DB3	98.72%	1.28%	0.10%	99.90%
DB4	99.60%	0.40%	0.28%	99.72%
NIST	99.89%	0.11%	0.17%	99.83%
Average	99.27%	0.73%	0.14%	99.86%

Table 1 Similarity in Feature vectors

Fig. 4 shows the Summary of the messages exchanged between entities for the user authentication.

Figure 3: Summary of messages exchanged between entities for the user authentication


Client's private key
K Kc
Client (C)
Cancelable feature set F'2 of I2
Cancelable feature set F2 of I2
Authentication Server (AS)
B, and B', Comparison
K
Krs
Cancelable feature set F'1 of I1
Synthetic fingerprint image
I2
Synthetic fingerprint image repository
I2
Resource Server (RS)
Synthetic fingerprint image repository
User Fingerprint Data Repository

V. RESULTS

Then, using a computer running Windows 10 and an Intel(R) Core(TM) i3-8130U CPU clocked at 2.85 GHz, we completed our task.

Based on the implementation procedure, we discovered that the biometric verification system performs effectively the majority of the time but may perform poorly when there is a greater similarity in function set.

Figure 4 This is the snap shot of the UI where our system asks client to submit biometric image before accessing files in cloud

Additionally, for the experiment, we considered fingerprints from many publicly accessible databases, including DB1, DB2, DB3, and DB4. After using them with the industrialised system, we also considered another data source, the NIST repository, and table 1 shows the commonalities in the attribute sets between the two.

VI. CONCLUSION

Compared to conventional password and token-based security systems, the use of biometrics has benefits.

In this post, we provided a biometric authentication solution for users attempting to access data and computer resources remotely. Our ground-breaking technique makes it possible to generate a special key from a finger print image. because creating the exact same key using a user's finger print is 95.12% accurate. When using our suggested session trick generation method that uses two biometric data, it is not essential to disclose any prior knowledge. Our approach is more resistant to several known attacks when compared to many other similar procedures. New biometric traits and multi-modal biometrics for more delicate applications, such national security systems, will be the focus of future research.

VII REFERENCES

[1] C. Neuman, S. Hartman, K. Raeburn, “The kerberos network authentication service (v5),” RFC 4120, 2005.

[2] “OAuth Protocol.” [Online]. Available: http://www.oauth.net/

[3] “OpenID Protocol.” [Online]. Available: http://openid.net/

[4] G. Wettstein, J. Grosen, and E. Rodriguez, “IDFusion: An open architecture for Kerberos based authorization,” Proc. AFS and Kerberos Best Practices Workshop, June 2006.

[5] A. Kehne, J. Schonwalder, and H. Langendorfer, “A nonce-based protocol for multiple authentications,” ACM SIGOPS Operating System Review, vol. 26, no. 4, pp. 84–89, 1992.

[6] B. Neuman and S. Stubblebine, “A note on the use of timestamps as nonces,” Oper. Syst. Rev., vol. 27, no. 2, pp. 10–14, 1993.

[7] J. Astorga, E. Jacob, M. Huarte, and M. Higuero, “Ladon : end-to-end authorisation support for resource-deprived environments,” IET Information Security, vol. 6, no. 2, pp. 93–101, 2012.

[8] S. Zhu, S. Setia, and S. Jajodia, “LEAP: efficient security mechanisms for large-scale distributed sensor networks,” Washington D.C., USA, October 2003, pp. 62–72.

[9] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, “SPINS:security protocols for sensor networks,” ACM Wireless Networking, vol. 8, no. 5, pp. 521–534, 2002.

[10] P. Kaijser, T. Parker, and D. Pinkas, “SESAME: The solution to security for open distributed systems,” Computer Communications, vol. 17, no. 7, pp. 501–518, 1994.

[11] G. Wettstein, J. Grosen, and E. Rodriguez, “IDFusion: An open architecture for Kerberos based authorization,” Proc. AFS and Kerberos Best Practices Workshop, June 2006.

[12] M. Walla, “Kerberos explained,” Windows 2000 Advantage Magazine,2000.

[13] Q. Jiang, J. Ma, X. Lu, and Y. Tian, “An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks,” Peer-to-Peer Networking and Applications, vol. 8, no. 6, pp. 1070–1081,2015.

[14] O. Althobaiti, M. Al-Rodhaan, and A. Al-Dhelaan, “An efficient biometric authentication protocol for wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 2013, pp. 1–13, 2013,Article ID 407971, http://dx.doi.org/ 10.1155/2013/407971.

[15] K. Xue, C. Ma, P. Hong, and R. Ding, “A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks,” Journal of Network and Computer Applications, vol. 36, no. 1, pp. 316 – 323, 2013.

[16] M. Turkanovic, B. Brumen, and M. Holbl, “A novel user authentication and key agreement scheme for heterogeneous

ad hoc wireless sensor networks, based on the internet of things notion," Ad Hoc Networks,
vol. 20, pp. 96 – 112, 2014.

[17] M. Park, H. Kim, and S. Lee, "Privacy Preserving Biometric-Based User Authentication Protocol Using Smart Cards," in 17th International Conference on Computational Science and Engineering, Chengdu, China,2014, pp. 1541–1544.