ENHANCED SECURITY SCHEMES IN CLOUD USING BIOMETRIC BASED ACCESS

[#1]KULSUM SUBIYA, M.Tech Student, Dept of CSE,
[#2]Dr. MD.SIRAJUDDIN, Associate Professor, Dept of CSE,
[#3]Dr.CHANDRAMOULI NARSINGOJU, Associate Professor & HOD, Dept of CSE,
[#4]Dr. GULAB SINGH, Associate Professor, Dept of CSE,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TS.

ABSTRACT:

Our data-driven organisation is rapidly increasing the demand for remote storage and computing services, necessitating the need for secure access to both the data and the computing services itself. A new biometric authentication method for secure access to a remote (cloud) server is being developed as part of this investigation. The biometric data of a user is treated as a secret certificate in the technique that has been proposed. The biometric data of the user is then utilised to create a unique identity for the user, which is also used to protect the user's privacy. The authors also present an effective way for generating a session key for secure message transmission between two biometric templates communicating participants using biometric templates. In other words, the user's private key is not required, and the session key is generated without the need for any prior information to be disclosed. Numerous known attacks against (passive/active) adversaries are found to be resilient to the proposed technique, as demonstrated by the model formal security analysis, informal (non-math) safety analysis, and formal security checks performed with AVISPA. Finally, the effectiveness and applicability of the proposed approach have been demonstrated through extensive testing and comparison studies, as previously stated.

Index Terms—Authentication, biometric-based security, cloud service access, session key.

---

1. INTRODUCTION

Because of its inherent advantages, biometric identification systems have seen a significant increase in growth and attention in recent years. It effectively protects the privacy of cloud users while also ensuring the security of extremely sensitive cloud-based data and information. As a result, the most recent research trend is centred on user privacy protection, data integrity, and cloud data growth management. In addition to user privacy, data integrity processing, and maintenance, biometric system recovery played a critical role in ensuring that data was kept secure in cloud computing. Over the last few decades, new and successful algorithms for privacy protection and biometric information security have been researched and implemented. It is possible to utilise these methods to verify the authenticity of each individual user's identity. Using similitude algorithms, the biometric traits of a single person are matched to the biometric database template held by the system. Biometric qualities are often classified into two categories:
(1) biometrical characteristics and
(2) biometric characteristics.

Face, fingerprint, hand shape, DNA, and iris are the most important physiological biometric features to know. The gait, signature, and voice of a person are all examples of biometric behavioural features. Individual verification and identity authentication are made possible through the use of biometric traits that are unchanging and distinctive. When compared to traditional methods of authentication, biometrics provides substantial advantages (e.g. passwords and token systems).

(1) a higher level of data protection is maintained

(2) Preserving the privacy of users' personal information

(3) There is a slight possibility of forgery and

(4) solutions that are both cost-efficient and cost-effective

(5) The user-friendliness of the website.

According to paper smart device users (including smartphone users), the only alternative answer to token-based systems and passwords is biometric automation techniques, which are becoming increasingly popular. As a result, biometric authentication procedures are more reliable than traditional methods. As a result, biometric recognition systems provide an extremely high level of security. Biometric data, in contrast to passwords, is one-of-a-kind and irreversible. Comparing biometric test (quest) attributes from the recorded database with those of the registered individual biometric templates is part of the technique for detecting a biometric system detection.

As a result, biometric recognition systems are more ideal for storing the biometric characteristics of cloud users (subjects). When an individual was recognised and validated (i.e. through a biometric survey) in the cloud, the cloud biometrics that had been previously saved were used. When dealing with an increasing number of subjects, biometric-based recognition systems require additional storage space and processing power in order to provide adequate user privacy protection.

Private corporations and organisations can use all stored biometric databases to authenticate cloud users because they are all accessible, maintained, and monitored by all private companies and organisations. Who has access to confidential information? In order to justify the adoption of a cloud-based biometric recognition system, it was necessary to have extensive processing capabilities. In addition, the system protects and processes the privacy and integrity of the biometric data that has been saved. When it comes to user authentication in cloud computing, the security of sensitive data (biometric data and other data) and the preservation of personal information are critical factors. These difficult concerns must be taken into account at every level of the design and development of the system in question. Because of the rising use of cloud computing technologies, it has become even more critical to find solutions to these fundamental difficulties.

The recorded biometric data is pre-processed and then compared to a biometric template database that has been saved on cloud servers for the purpose of user authentication. Theft, forgery, or duplication of sensitive data, as well as infringement of user integrity and authentication, may all be associated with threats in cloud computing, because stolen and misused data may be retained during the process of registration. The most significant advantage of biometric data is that users cannot replicate or fabricate biometric data from other users who have registered with the system. The use of biometric data encryption in biometric identification systems can thereby ensure the privacy and security of individual users.. As a result, to improve the privacy and security of a person's biometric information stored in the cloud, the biometric database must be encrypted before it can be used. It is a dependable and convenient technique to recognise cloud users who have provided their biometric information. The widespread use of biometric recognition provides excellent privacy and data security, but it also raises the possibility of abuse, information loss, and the leakage or theft of biometric information kept by individuals on the cloud, among other things.

Authentication of cloud users is accomplished through the use of encrypted biometric data that has been identified and confirmed for use with cloud services and system resources. In this case, the data base administrators or cloud administrators construct a credential for the candidate's biometric features and present it to the identification cloud for processing. According to this article, biometric face traits are used to match cloud users, which are critical attributes for gaining access to cloud-based services.

In order to authenticate the owners, the cloud servers identify encrypted data and provide matching scores based on this identification. Individual recordings make up the data that has been recorded. Saving personal information as a database is the most efficient method of creating an encrypted biometric database. The cloud biometry database contains all of the information about a person, including their name, birth date, residence, bank details, insurance papers, and unique identifiers (i.e. employee id or family number and Aadhar ID).

These personal details are necessary in order to protect the privacy of the user during the verification of the person in the cloud database. The user query input is matched against a stored biometric template database without the usage of biometric decryption in order to prevent eavesdroppers or unauthorised access to resources. The encryption procedure is made more difficult by variations in biometric data obtained as a result of lighting conditions and low image quality, respectively. As a result, even minor changes in plaintext (for example, biometric data) can have a significant impact on the experimental outcomes during the matching phase. It is because of these differences in the cypher text of the cloud user (encrypted biometric data) that there is a high rate of erroneous refusals during verification.

A large number of false matches to the recorded biometric template database during the recognition process may pose problems for these identifying systems, resulting in reduced performance. Deception is perpetrated by the large number of erroneous acceptances and fraudulent refusals. This is due to the fact that biometric encryption paradigms and projecting accurate performance measurement-based findings on secure and encrypted data are incompatible with the recognition system's requirements.

The biometric authentication features are calculated by the encryption technique. Initially, the biometric identifier system uploads the image to cloud servers, where it remains. The authentication of the user takes place in an encrypted environment, and the results (value) are derived from the encoded biometric data that was used. In this research effort, biometric templates are created and encrypted using the Paillier encryption technique and the Eigenface encoding algorithm, respectively. As a result, cloud computing systems did not provide access to biometric information since cloud computing systems did not have access to encrypted genuine biometric information stored in the cloud (face image data). Furthermore, cloud systems do not extract information from saved facial templates in order to protect the privacy of users' personal information from disclosure.

2. LITERATURE SURVEY

P., as well as Rajeswari [1] In the system, users were required to submit multiple [two] biometric fingerprints during the service registration procedure, which they were required to do. At the cloud's end, these templates are saved in a database. Users must always authenticate the fingerprint templates in the random number order in which they were generated. The provision of fingerprint templates and pictures was made when the level of security was raised to the maximum. There are three phases to the new model: I a third phase of registration, I, with two fingerprints that assign a single digit value for each of two fingers; (ii) a fingerprint access stage in order of the random number generated by the random number generator; and (iii) a matching phase that compares the fingerprints provided by the user with Randa's fingerprint database. When the

proposed new template for the two fingerprint inputs was applied to the two fingerprint inputs, the elliptical curve algorithm of the biometric photos, Rivest – Shamir–Adleman (RSA) numbers and mappings, as well as the RSA numbers and mappings, were found to be effective.

Zhu, Zhu, Hui, Zhu, Zhu, Zhu [2] This introduces a novel authentication mechanism for online fingerprints, e-Finga, that protects privacy by using encrypted outsourced data rather than traditional fingerprints. User authorisation would allow the user fingerprint to be outsourced to other servers, allowing secure, accurate, and effective authentication services to be delivered without the user's fingerprint information being compromised. In combination with a secure Euclidean distance computation, the enhanced homomorphic encryption approach of e-Finga may be used to protect the privacy and confidentiality of users while matching templates in composite order groups.

Tian Yangguang's formal name is Tian Yangguang. [3] Specifically, in this work, we look at the authentication of biometric remote users utilising homomorphic encryption (BRUA), which is used when authorised individuals attempt to remotely authenticate on a server using contained biometrics. When using the TLS1.3 and QUIC protocols, it is possible to encrypt the ID information of protocol users via homorphic encryption. The usage of primitive homomorphic encryption is essential for effective user authentication to be successful. To support all of the distance calculations mentioned above, complete homomorphic encryption is all that is required.

S. D. Yuvaraj, D. D. Valarmathi, S. D. Yuvaraj [4]. This work presents an updated approach to the cloud data security paradigm, which was previously used in other publications. The data security paradigm that is offered involves the generation of one-time passwords (OTPs) for user authentication using HMAC. In order to improve model implementation, a comparable MD5 and SHA algorithm has been added in this research. In the case of a single user ID OTP algorithm, such as the one used by the ID and Subscriber ID modules, a final alphanumerical token is generated that is only valid for a single session and one single application. When used in conjunction with the original one-time password approach, the cloud provides a two-way Authentication Factor that sends a code to mobile users for any user login. Therefore, we recommended the use of a one-way dynamic password as a strong authentication technique that involves the use of a mobile phone as an authentication system, which we believe is feasible.

Ruiu, Pietro, Using a biometric fingerprint and password to improve the security of a remote authentication system for mobile devices, the author has developed a two-factor authentication system that relies on a Schnorr digital signature and fingerprint extraction to protect mobile devices against impersonation. Some writers use keystroke dynamics, which is a common behavioural biometric, to design a user authentication solution for Windows. It is possible to record conduct biometrics such as keystroke dynamics without the user's knowledge, which is one of the advantages of conducting biometrics. The notion of homomorphic encryption is used by the authors to increase the security of voice prints. We demonstrate a complete cloud solution that makes use of biometric authentications, such as fingerprints, in conjunction with the OpenStack cloud platform.

Jian Ren, Zhou, and Kai [6] are three of the most prominent figures in Chinese culture. This paper describes how we can use our suggested Threshold Predicate Encryption Technology to encrypt two vectors, X and Y, in order to evaluate and compare the internal product of X and Y to an advanced threshold. When using TPE, it assures that only the results of a comparison are displayed and that essential x and y information cannot be gathered. The TPE that is recommended allows for the comparison of a computational model to

encrypted information. Our research demonstrates that this computer model can be utilised for a variety of privacy-protection applications, including biometric identification and encrypted data searches. Deployments of homomorphic encryption and safe two-part computing were made in this case. It is necessary to define the distance between these two templates as well as the distance that will be compared with the threshold. Both mobile devices and personal computers are capable of running the proposed TPE.

Santosh Kumar [number 7]. For cloud users, we offer a biometric facial recognition system that ensures their safety and privacy throughout their use of cloud-based services. Steps one through three are included in the proposed approach:

(1) Take a picture of your face.

(2) Preprocessing and extraction of a facial feature

(3) identification of the trait that was employed in a unique way

Paillier encryption and Eigenface encoding techniques are used to build biometric templates, which are then encrypted using the techniques. (1) Training phase and (2) Testing phase are the two stages of the identification system's development process. During the system's training phase, the system identification system collects individual images for the purpose of building a database. The biometric cloud database stores the photographs of the subjects' faces. When undergoing testing, the individual is recognised by the identification of face characteristics in the test images, which have been collected and stored in a biometric template database and are based on the test results (quest).

Weixin and Bian [8] Fingerprints are a biological trait that has been utilised in the biometrics business for a long time and is widely accepted. It is unique to the individual and remains so throughout life. Because of their distinct physical qualities, physically uncloneable functions (PUFs) were utilised in authentication procedures to ensure that no two people could use the same password. The study takes full advantage of the security qualities of user biometrics and PUFs in order to develop a novel user authentication and key contract system, which is referred to as Bio-AKA. A three-stage process is proposed, consisting of three steps: registration; registration; mutual authentication; and essential agreement stages.

B. Kezia and K. Sarat Rani and Chand[9] are sisters. In this study, we present an authentication solution that is secure, as opposed to a password or a key. Biometrics is the process of automatically identifying a person based on unique physiological characteristics. Every individual's biometric data is distinct from the next. As a result, our technique is designed to authenticate users through the use of biometric data. The fingerprint pictures are encrypted both at the end of the user's session and at the end of the service provider's session, resulting in increased security when using the encryption strategy. A hacker may be successful in obtaining a photograph of the fingerprint, but will be unable to decrypt the photograph to obtain the original. The process of biometric authentication is often divided into two phases:

1) The registration process; and 2) the identification process are both required.

The user gives biometric data, which is captured by a biometric fingerprint sensor, which converts the biometric data into a binary string for further processing. The extraction function converts a binary string into a set of functions with a less number of variables (eliminates a redundancy). The service provider stores the user feature vector in a database that contains other information about the user. It is the same operations that are carried out when an individual seeks to log into a remote cloud service. The extractor extracts the functional vector and submits it to the appropriate module for further processing. During the registration process, the matching module intercepts the vector that was stored against the user's identity. Using the matching module, the algorithm is executed to ensure that the user logs in for the corresponding

resemblance between the registration and identification procedures.

M. Mostafa-Sami [10] is a writer and poet. Astama M. Hussein and Hala M. Abbas are co-authors of this work. The purpose of this paper is to provide an overview of various access strategies for cloud services that are both biometric and nonbiometric in nature. Approaches such as passwords, card tokens, and so on have demonstrated a basic deficiency in assuring the reality of an accessible user, which has been remedied by utilising biometric techniques based on human characteristics. Because of the variability in human behaviour, we might conclude that, when compared to physiological biometrics, behavioural biometrics cannot be considered steady and predictable. It does, however, provide clients with a continuous and visible authentication process in order to resolve the issue of static biometric authentication. The authentication approach is provided by a combination of dynamical biometrics, which results in a highly secure system that includes a number of additional features.

Padma, P. S. Sr. [11] and S. Sr. [11] The goal of the project is to apply existing biometric authentication techniques that are now being used to secure data in cloud-based services. In the field of biometric authentication, we looked at both physical characteristics and behavioural authentication procedures. The entire Cloud authentication procedure involving biometrics can be divided into three sections: the registration phase, the registration phase again, and finally the verification phase. During this stage, a user who wishes to utilise the Cloud service can register his biometric data with the cloud computing server, which is the first step in the process. The login process begins immediately after the registration phase and is completed in stages.

3. RELATED WORK

BIOMETRIC SYSTEMS

Several diverse characteristics of human physiology, chemistry, or behaviour can be utilised to authenticate a person's identity using biometrics. The selection of a particular biometric for usage in a specific application necessitates the consideration of a large number of factors. According to Jain et al. (1999), there are seven features that should be considered while evaluating the applicability of any biometric authentication function. The term "universality" refers to the fact that everyone should possess the characteristics of a system. According to the concept of uniqueness, individuals in a relevant population should have characteristics that are sufficiently distinct to allow them to be distinguished from one another. Permanence is concerned with how a characteristic changes through time. The persistence attribute of a given matching method will be reasonably consistent over time if it has a "good" persistence attribute associated with it. Measurability refers to the ease with which an acquisition or characteristic measurement can be performed. Aside from that, the data obtained should be in a format that enables for subsequent processing and removal of the corresponding functional sets from the database. Technology's precision, speed, and robustness are all measured in terms of performance. Acceptance refers to how well individuals in the relevant demographic accept this technology and are prepared to have their biometric features collected and assessed. Circumvention is a simple method of recreating or replacing an artefact or replacement.

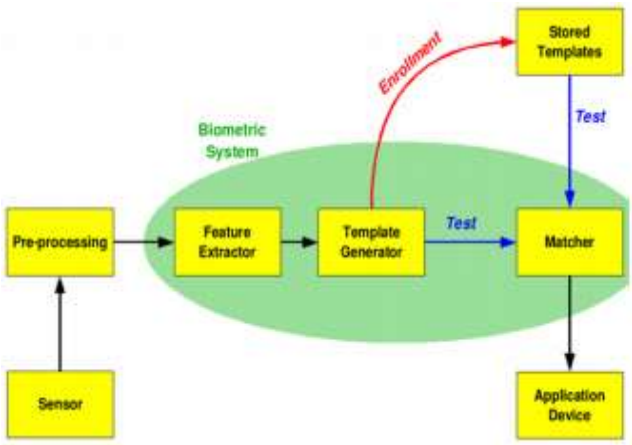


Fig.1: Simplified block diagram of biometric verification and identification.

The two fundamental modes of the biometric system are depicted in the block diagram (Fig.1). A single-to-one biometric mode is first compared to a template stored in a biometric database to ensure the individual claiming to be the person in question is indeed the person claimed to be. Verification of a person is accomplished in three ways. The first stage is to develop and save reference models for all users in the model database, which is the first phase in the process. A subset of samples is matched to reference models in the second phase, which allows for the calculation of the true and impostor values. The third phase is the examination. A smart card, a username, or an ID number can be used to designate a certain template (e.g. PIN). Positve recognition is a common application of the control mode in situations when "many people do not have the same identify."

Second, in identification mode, the system compares the identification of an unknown individual from the biometric database with the identification of an unknown individual from the biometric database. A biometric sample can be identified by the system if it matches a template in the database within a previously established threshold. A person's identity is determined by the identification mode, which can be either "positive recognition" or "negative recognition." The identification mode can be used for either "positive recognition" or "negative recognition," and "where the system determines whether the individual is the individual (implicitly or explicitly) he denies to be" (to ensure that the user does not have the template to be used to give information). Other methods of personal identification, such as passwords, PINs, or keys are ineffectual in the absence of biometric identification.

FINGER PRINT RECOGNITION

Generally speaking, the local version of FingerIdent can be divided into two primary categories: user verification (enrollment), which generates and stores a biometric template on a system database for a specific user; and (secondarily), user identification, which validates a specific identity claim for a specific user. An electronic fingerprint reader is used to capture the (biometric) fingerprint data. During the following phase, the quality of the sample is examined, and the data is extracted from the system functions and stored in the database as a biometric template, if it is determined to be appropriate for storage. After removing features from the gathered "live" fingerprint, the verification approach compares the remaining features to those already stored in the database. The comparison is made on the basis of matching patterns, which serve as the foundation for the confirmation of the assertion. Figure 1 depicts an illustration of both roles in action. In order to achieve a cloud-based biometric service, the local FingerIdent system must be moved into the cloud, and the infrastructure required to access the biometric service must be provided. This approach is described in greater detail in the following section.

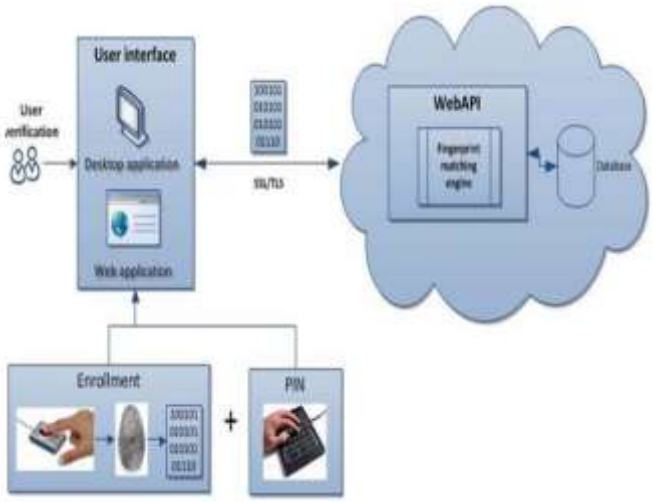


Fig.2: Scheme of the biometric verification system in the cloud

A. Designing Cloud biometric services

A review of certain existing cloud biometrics systems revealed some aspects that were similar to those found in the solutions under consideration. All solutions are based on the client-server paradigm, which is the foundation of all computing. Collection and transfer of biometric samples to the server, where the required process is carried out, is the responsibility of the client

software running on the user's computer. The traffic is used for network security between the client and server security protocols, and it is encrypted. The following is the check circumstance (as shown in Figure 2): Initially, a fingerprint scanner is used to acquire data. Scanning libraries must be included in the programme in order to capture the image (web, desktop). The programme establishes a connection with the API that is hosted in the cloud. The API is used to provide encoded photos to the fingerprint library, which then stores them. After that, the image is processed, and the results are returned to the user via the cloud. Because the solution is built in modules, it is possible to upgrade it in the future. In the context of multimodal authentication, our API solution might also be utilised for additional biometric modalities, such as face recognition.

B. Authentication data fusion and data security

It is our goal to combine various data points supplied by different authentication techniques into a meaningful representation through data integration. We combine login information from desktop applications with information from web applications, such as Moodle. Our system is secure on a number of levels, the most important of which are as follows: Cloud access is protected by a difficult 40-digit password, which is used in conjunction with HTTPS to transfer data and encrypt passwords and other database information. However, we would like to see other security approaches developed in the future, both for data storage and data transport.

C. Moodle with fingerprint verification

Moodle will enhance its biometric authentication capabilities by integrating it with a cloud-based fingerprint testing service in order to demonstrate the utility of this technique and to create a proof of concept. Considering that Moodle was also constructed in modules, a biometric authentication technique was implemented to strengthen existing procedures and provide additional access security as a (optional) authentication programme. Figure 3 depicts a block integration schematic. Figure 3: Block Integration Schematic The fact that different fingerprint readers are compatible with different browsers is the most significant integration challenge. Each manufacturer of fingerprint readers provides its own set of protocols and libraries to allow users to interact with their devices. There is still no consensus on what constitutes a standard. The solution offered for this case study makes use of an ActiveX component to gain access to the hardware. Internet Explorer is the only browser that is officially supported for ActiveX components. In future initiatives, it is planned to broaden the scope of the method to include support for additional popular browsers such as Firefox, Opera, and Chrome. In order to reflect these new functionalities, after the fingerprint authentication service was integrated with the Moodle frame, the display was adjusted to reflect these changes. The outcome of this strategy is depicted in Fig. 4. It should be noted that the additional biometric authentication elements can be readily added into the existing framework.

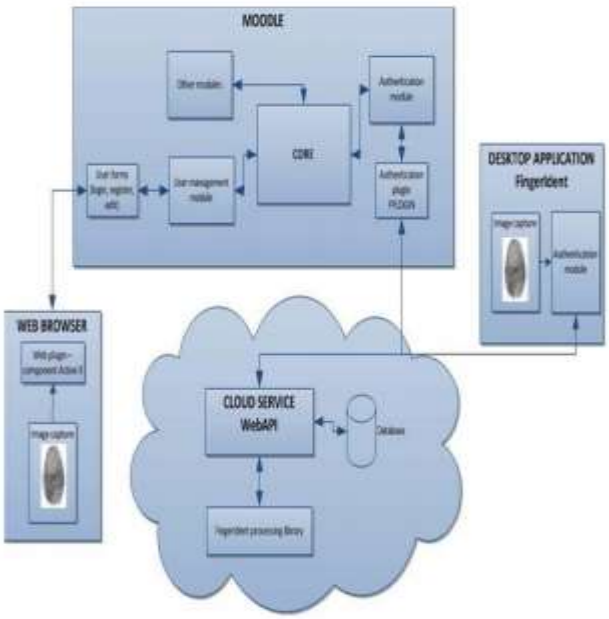


Fig.3. Cloud fingerprint verification in Moodle

Fig.4: Customized Moodle login

4. IMPLEMENTATION AND RESULTS

MODULES AND SPECIFICATIONS

Cloud Owner uploading a file to remote cloud services and requiring authentication of the remote servers between devices Decryption and download of encrypted files

1. Cloud Owner and User Registration & Key Generation

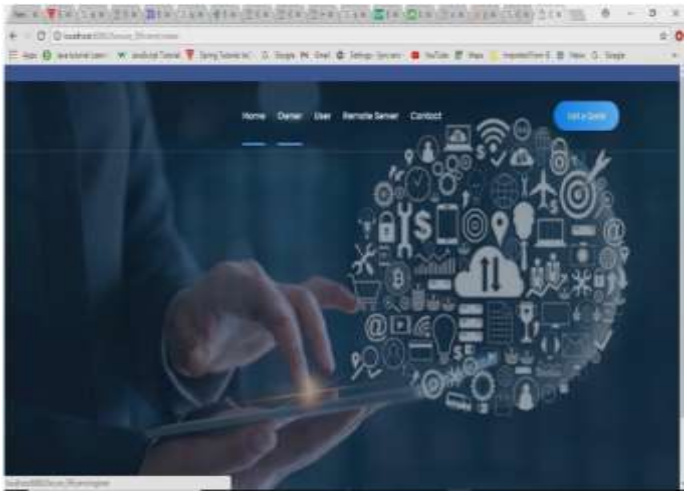
To begin, the user must create a cloud account by supplying all necessary user information, such as an email identity, a mobile number, an age name, a password, and the name of the cloud owner in exchange for a biometric fingerprint. After completing the registration process for both the owner and the user, the user requests that the Key Generation Center issue the user with a unique ID. It is only when the user has registered his or her name in the key generating centre that they will be able to access cloud data.

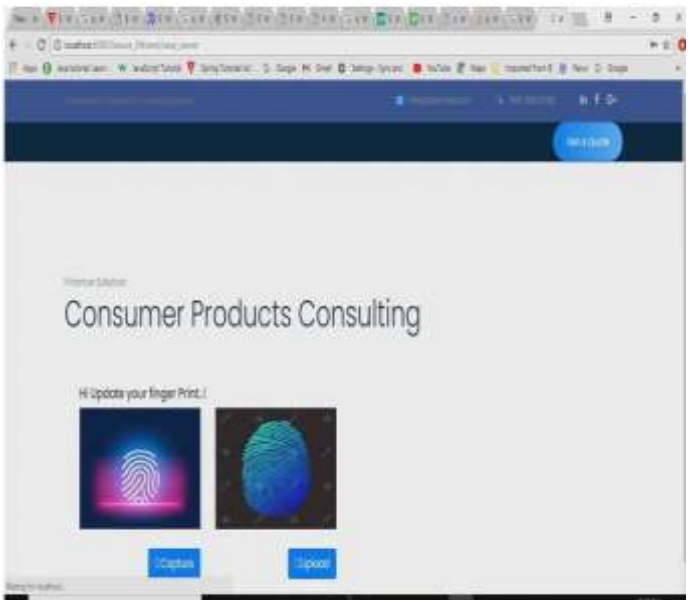
2. Cloud Owner Upload File to Cloud Server

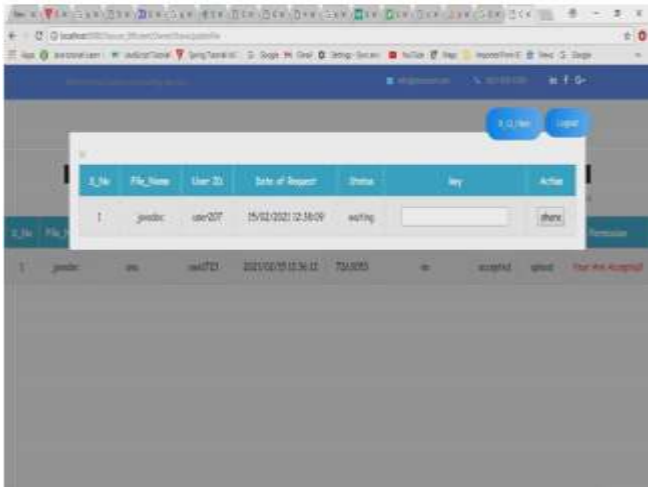
Users can upload any file to the cloud, and the information will be encrypted in the cloud, allowing the user to safeguard the file in the cloud. The cloud only retains the encrypted format information linked with the file as well as the parameter of the file that is associated with it. It is necessary for the security user to maintain the parameter for an initially generated file when used in conjunction with Data mode, public or private upload mode, if the user then requires a customer or a group of people who can access or download this file, the key is created on an RSA basis and the user should encrypt and upload the file using the key user created earlier.

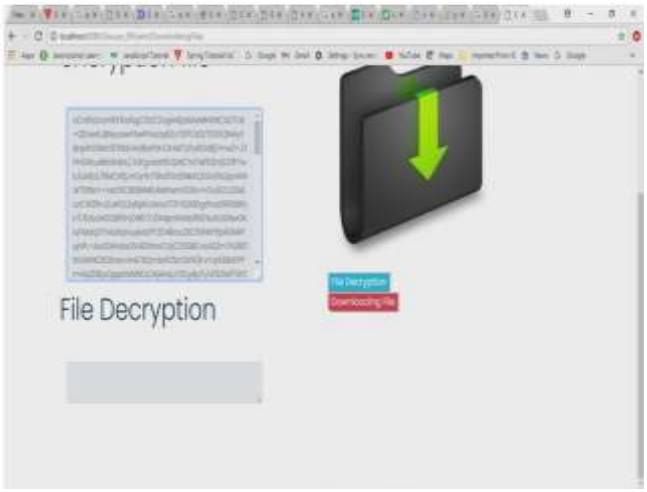
3. Decrypt and Download file:

Once the file has been located based on the parameter, and if any parameter matches the server, the user searches for it, and the server loads the complete file based on that parameter. After authenticating himself to the server with his fingerprint, the user will have access to the file, which is encrypted to allow the user to decrypt and download the KGC (Key Generation Center) user request file, together with the user attribute and file parameter, in order to download it.









5. CONCLUSION

It is the immense commercial value of biometric cloud services that has drawn the attention of research and development groups from throughout the world. The information in this paper describes the process of moving existing biometrics to a cloud platform. The presentation covered the issues that should be considered while designing cloud-based biometric services, as well as a case study describing the use of a Cloud fingerprint service in conjunction with the Moodle e-learning platform. Our long-term development plans include bringing in additional biometric modalities to the club and, if at all possible, constructing a cloud-based biometric system that is multi-modal and multi-modal.

REFERANCE

- C Neuman, S. Hartman, K. Raeburn, "The kerberos network authentication service (v5)," RFC 4120, 2005.
- "OAuth Protocol." [Online]. Available: http://www.oauth.net/
- "OpenID Protocol." [Online]. Available: http://openid.net/
- G. Wettstein, J. Grosen, and E. Rodriguez, "IDFusion: An open architecture for Kerberos based authorization," Proc. AFS and Kerberos Best Practices Workshop, June 2006
- Mell, P., Grance, T.: The NIST Definition of Cloud Computing. National Instituite of Standards and Technology (2009)
- Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I.: Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future
- Gener. Comput. Syst. 25, 599–616 (2009)
- Neuman, B.C., Ts'o, T.: Kerberos: An Authentication Service for Open Network Systems. IEEE Communications 32, 33–38 (1994)
- Chandra ShekharVorugunti, "A Secure and efficient Biometric Authentication as a service for cloud computing," IEEE, October 09-11 2014
- Kiran Kumar K, K.B Raja, "Hybrid Fingerprint Matching using Block filter and strength factor," Second International Conference on Computer Engineering and Applications,2010
- Panchal, G., Samanta, D., Das, A. K., Kumar, N., & Choo, K. K. R. (2020). Designing Secure and Efficient Biometric-Based Secure Access Mechanism for Cloud Services. IEEE Transactions on Cloud Computing.
- Batool, R., Naveed, G., & Khan, A. (2015). Biometric authentication in cloud computing. Int J Comput Appl, 129(11), 6-9.
- Identity, C. B. (2016). Authentication: BIOMETRICS-AS-ASERVICE.
- Wong, K.S. and Kim, M.H., 2012, June. A privacypreserving biometric matching

protocol for iris codes verification. In 2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (pp. 120-125). IEEE

- Wong, W.K., Cheung, D.W.L., Kao, B. and Mamoulis, N., 2009, June. Secure kNN computation on encrypted databases. In Proceedings of the 2009 ACM SIGMOD International Conference on Management of data (pp. 139-152). ACM.
- Y. Shu, Y. Gu, and J. Chen, "Sensory-Data-Enhanced Authentica- tion for RFID-Based Access Control Systems," Proc. IEEE Ninth Int'l Conf. Mobile Ad Hoc Sensor Systems (MASS), 2012.
- Juels, "RFID Security and Privacy: A Research Survey," IEEE J. Selected Areas Comm., vol. 24, no. 2, pp. 381-394, Feb. 2006.
- Ahonen T, Hadid A, Pietikainen M (2006) Face description with local binary patterns: Application to face recognition. IEEE Trans Pattern Anal Mach Intell 28(12):2037–2041
- Ali M, Khan SU, Vasilakos AV (2015) Security in cloud computing: Opportunities and challenges. Inf Sci 305:357–383
- M. Hussein,H.M. Abbas,M.S.M. Mostafa."Biometric-based Authentication Techniques for Securing Cloud Computing Data - A Survey",Researchgate.net,International Journal of Computer Applications (0975 – 8887) Volume 179 – No.23, February 2018
- G.Naveed, R.Batool, "Biometric Authentication in Cloud Computing", JBMBS, Vol.6(5),2015.
- Yuan, X. Sun, and Q. M. J. Wu, "Difference co-occurrence matrix using BP neural network for fingerprint liveness detection," Soft Computing, vol. 23, no. 13, pp. 5157–5169, 2019.
- S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo, "Chaotic Map-Based Anonymous User Authentication Scheme with User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2884– 2895, Aug 2018.
- H. Sieger, N. Krischnik, and S. Moller, "POSTER: User Preferences for Phones", proceeding of 6th Symposium on Usable Privacy and Security.
- A.K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," Transactions on Circuits and Video Technology vol. 14, no. 1, pp. 4-20, 2004.
- Rajeswari, P., et al. "Multi-fingerprint unimodel-based biometric authentication supporting cloud computing." Intelligent techniques in signal processing for multimedia security. Springer, Cham, 2017. 469- 485.
- Zhu, Hui, et al. "Efficient and Privacy preserving Online Fingerprint Authentication Scheme Over Outsourced Data." IEEE Transactions on Cloud Computing (2018).