International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Biometric Authentication in Cloud Environment based on Statistical Modeling

Sanoop Kumar Parayil, Srinivas Yarramalle

Abstract: ***With the advancements in the area of science and technology, the usage of multimedia applications have raised enormously. This raise in data has led towards different issues such as storage and confidentiality. Lot of devices and techniques has been embarked to compact the data so as to safeguard the information. Recently, cloud computing is considered to be one of the notable innovations having advantages with respect to reduction in cost, increase in throughput and flexibility in usage. However there are certain security hinges that are associated with this regard. The literature reviewed showcased several techniques coined towards the safeguard of data in cloud environment. In this article, a novel biometric authentication system is developed for the ease of computing and distributing the data without any security issues.***

Keywords: Biometric, Cloud Computing, Statistical computing, Security, Data Access

I. INTRODUCTION

Cloud computing refers to the provision of providing scalable services to the end users by means of internet. There are various services that are being provided by the cloud computing environment which include Software as a Service, Platform as a Service and Infrastructure as a Service. With the various services associated with cloud, the cost incurred for the user has been declined and therefore lot of clients have started migrating towards the cloud environment. However, one of the main issues that are associated with this regard is the security. Since, by the usage of cloud, distributed access of the data is possible, at the same time, data breaches are also highly possible. In order to safeguard the data, many applications have been coined in the literature which includes methodologies based on cryptography, [1],[2],[3],[4],[5], privacy preserving techniques [6],[7],[8], knowledge based authentication techniques, possession based authentication techniques emit these methods, each one of the methodologies has their own limitations with respect to provision of security[9],[10],[11]. Therefore, to overcome these limitations, methodologies based on biometric authentication has been popular [12],[13],[14]. However the main assumption underlining the advantage of biometric includes authenticity, uniqueness and non-tamperedness. Therefore, the methodologies considering biometric as a means of security are found to be more robust. With this assumption, different approaches were highlighted in the literature for effective transfer of data/ sharing of data based on biometric security. In this regard, biometric traits such as fingerprint, ear, hand geometry, voice and DNA are being utilized [15],[16],[17],[18],[19]. Also, models have been developed based on univariate biometric techniques and multimodal biometric methods [20],[21]. Techniques based on neural networks, data mining, machine learning are considered for these approaches. However, statistical models are assumed to be more compared to non statistical approaches. (S. K. PAL, N. R. Pal (1993)). Therefore, numerous statistical models are considered for secured transmission of data in the cloud using statistical mixture modals and in this regard, Gaussian mixture modals are being utilized. However, in reality, the usage of Gaussian mixture model can be effective if the data is of more volume and in practicality, the data that is been transferred/ shared across the globe through internet using different servers is generally of finite length. Therefore considering Gaussian mixture modal for such applications fails. Also, considering only a solitary feature for the purpose of security is again considered to be suspicious and ineffective. Therefore, it is necessary to develop technologies based on bivariate features together with statistical modeling approaches which can truncate the data such that only finite information which needs to be transferred can only be safeguarded. Therefore, in this article an attempt is made in this direction by proposing a multivariate truncated Gaussian mixture modal. The rest of the article is articulated as follows: Section-II of the article deals with brief information about the cloud environment. In Section-III, an insight about biometric models and techniques has been presented. Feature extraction methodologies are highlighted in Section-IV of the article. In Section-V, the methodology is presented together with the various insights about the components, procedure for enrollment and verification are presented. In order to validate a modal, data need to be tested based on various measures such as efficiency, accuracy, correlation coefficient, precision and recall. The results derived are highlighted in Section-VI of article. The final Section-VII concludes the article by summarizing the results derived from earlier sections.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Sanoop Kumar Parayil*, Research Scholar, Department of CSE, Centurion University of Technology and Management, Parlakhemundi, India & Assistant Professor, Department of CSE, Gayatri Vidya Parishad College of Engineering (Autonomous), Visakhapatnam, India.
Srinivas Yaramalle, Professor, Department of Information Technology, GITAM (Deemed to be University), Visakhapatnam, India.

II. CLOUD ENVIRONMENT

There are three major models which are mostly considered in the cloud environment viz., Infrastructure as a Service, Platform as a Service and Software as a Service. Among these services, the lowest level is considered to be Infrastructure as a service where it concerns about the hardware components required for processing the data. In contrary, Software as a Service is assumed to be the highest level of consideration as it provides various services in par with the requirements of the end user. Amazon web services are assumed to be the best examples for Infrastructure as a Service and salesforce.com is considered to be the best suited example for Software as a Service. The main advantage, of this service to the user is, any software can be given privileges to run the software's running in cloud environment. Its ability as Platform as a service is considered as the basic source which supports the user requirements (i.e. tools, library, services) and user can use the platforms without having any control, and in infrastructure as a service, user can use the infrastructure but has no control Cloud computing environment generally uses four deployment models viz., (i) Public Cloud model helps common community and is owned by a specific company, (ii) several users can use the services by means of Community cloud, (iii) personal clouds for private companies and (iv) two or more clouds can be combined to formulate a Hybrid model, and serves for specific purposes. However, in spite of its advantages, there are also several security concerns in the cloud setup, which include virtualization, immense distributed processing, traffic management, application security, and validation and admittance control. Cloud environments lack in providing suitable physical shielding procedures and frequently depend on mechanisms to authenticate the user. To solve these issues, Senk and Dotzler, 2011 has coined the concept called, Biometric Authentication as a Service (BioAaaS) in order to have a more secured transformation of data in the cloud environment.

III. BIOMETRIC USER VALIDATION

While authenticating the user over the Internet, his/her details will be taken into consideration and are mapped against the data available in the database. If the details coincide, then the user is given permission to access the services. In this article, the details already available are only considered over the cloud. The details which are considered for authentication and validation include; password, digital certificate, encrypted data and biometric traits acquired from the individuals. The traits extracted from the iris patterns, face, fingerprints, palm prints and voice will be submitted by the user as the credential for authentication over the cloud. Biometric-based validation systems afford a higher degree of security as compared with conservative authentication systems. In addition, it also helps in understanding the user's actions, due to the fact that individual biometric characteristics cannot be altered. Every biometric authentication systems encompasses of, the biometric sensor, feature extractor, template storage, matching module, and the decision module. In current approaches, univariate models are considered and these models are considered to be unstable and are prone to attacks such as spoofing, forgery, etc. To overcome the limitations, bivariate feature extraction methods are mostly considered. In bivariate methods, more than one feature is considered for authentication and hence ensures robustness. In biometrics, among the biometric traits available for this article, we have considered the fingerprint templates.

IV. FEATURE EXTRACTION

Feature extraction plays a vital role in the extraction of a template. In fingerprint analysis there are generally two features namely, micro features and macro features. Macro features are visible through the naked eye while the micro features need to be analyzed by sophisticated tools. In order to analyze the features, in this word we have considered both micro features such as delta points and macro features such as core. These features are extracted among each of the template and are stored in database. For this work we have considered fingerprints available from real-time data available at GITAM (Deemed to be University). Each fingerprint template is processed so as to remove the blur and degradation. These processed data is considered for analysis.

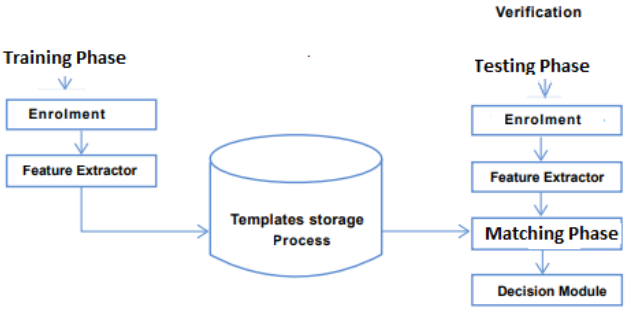

Figure-1 Authentication Process

V. MULTIVARIATE GAUSSIAN MIXTURE MODALS

In general each of the fingerprint trait acquired by feature extraction takes a shape which is generally platy-kurtic, meso-kurtic and lepto-kurtic. To validate the user more appropriately, the data acquired should be properly monitored. Therefore to monitor such type of data having variation, multivariate Gaussian mixture models are mostly preferred. The main advantage of this model is that it has a shape parameter beta, varying the parameter of beta, different distributions can be exhibited so that all the above three kurices can be managed. The probability density function of the generalized Gaussian Mixture model is given by: Let y be a random p-dimensional vector ($p \geq 1$) generated by a Gaussian mixture model (GMM) with K components:
Given by

$$f(y) = \sum_{k=1}^{K} \pi_k \phi(y|\mu_k, \Sigma_k),$$

where each $\pi_k > 0$ and $\sum_{k=1} \pi_k = 1$, and $\varphi(\cdot; \mu_k, \Sigma_k)$ is the probability density function of a p-dimensional

Gaussian variable with mean μ_k and covariance matrix Σ_k i.e. $N(\mu_k, \Sigma_k)$. The authentication procedures, together with its validation in cloud and the matching procedures are explained in the following sections (A), (B) and (C) respectively.

A. Biometric Authentication

Biometric recognition systems are systems for identifying patterns that are able to identify individuals based on their physiological or behavioral properties. These characteristics are considered unique for each individual and, unlike knowledge or security mechanisms based on tokens, cannot be forgotten, lost or stolen. The most common features used for biometric identification are faces, fingerprints, iris, handprints, speech, etc. The development of biometric cloud services emphasizes the need to make a decision as to which components of the biometric system need to be moved to the cloud, carried out locally. This authentication process uses the proposed system: Finger Print as a so source. A biometric is an authentication process that is used for security purposes.

The proposed system uses biometric data, of fingers. We use the matching algorithm to compare the images. Since the first step in the biometric process, we use finger print images. An analysis was made of the user image and the image of a hacker. The algorithm is used here to compare images. If a hacker tries to show the data he will return, "Authentication failed".

B. Cloud Security

Cloud security is provided by biometric techniques, such as iris authentication and fingerprint. The electronic key is unique to the individual user. It is a combination of data such as encrypted information and user ID. The electronic key is checked for every authentication. Finger Print has greatly increased the efficiency of authentication.

C. Matching Procedure

With the help of the procedure, the pointing points from the input and template are extracted. The algorithm provides the following two outputs: (a) a set of minus points, each of which is indicated by its spatial position and orientation in the shape of fingerprints. (b) Local information about the ridge near each point of the minus. The two sets of minutia points are then matched to the matching procedure. The procedure first selects the minutia reference pair (one from each image) and then determines the number of corresponding minutia pairs using the remaining set of points. The reference pair, the result of which is the maximum number of matching pairs, determines the best alignment.

VI. VERIFICATION

To build the framework, ANEKA cloud is considered. The fingerprints are first extracted and the values are obtained based on biometric sensor. The values are processed and both the micro and macro features are extracted. These features are given as inputs to the multivariate Gaussian mixture model discussed in Section-5 and against each trait a unique probability density function value is extracted. These values are encrypted using simple RSA algorithm and transmitted in cloud environment. At the receiving end, the value is decrypted and the message received against these decrypted values is considered, and thereby the authenticity of the user is established.

VII. RESULTS

Method	Function mechanism	Advantages	Disadvantages
Finger print	Difference between human finger prints	Very low error rate, being used for over 10 years	Dirty or damaged fingers can affect accuracy

VIII. CONCLUSION

The Cloud is based on biometric services with a large market size and thus attracts research and development teams from all over the world. In this paper some instructions on how to adopt existing biometric technology to the cloud platform have been introduced.

REFERENCES

1. Pant, V.K., Prakash, J. and Asthana, A., "Three step data security model for cloud computing based on RSA and steganography", In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 2015, October. IEEE. (pp. 490-494).
2. Rahman M.O., Hossen M.K., Morsad M.G., Chandra A, "An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding", IJCSNS- 2018 Sep-18(9),pp.85.
3. Khan M.A, "A survey of security issues for cloud computing", Journal of network and computer applications 71, 2016, pp.11-29.
4. Awadh, W.A. and Hashim, A.S., 2017. "Using steganography for secure data storage in cloud computing",IRJET, 4(04), pp.3669-3672.
5. Maitri PV, Verma A., "Secure file storage in cloud computing using hybrid cryptography algorithm", In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) 2016 Mar 23, IEEE. pp. 1635-1638.
6. Al Hamid, H.A., Rahman, S.M.M., Hossain, M.S., Almogren, A. and Alamri, A., "A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography", IEEE Access, 5,2017, pp.22313-22328.
7. Yassin A.A, Jin H, Ibrahim A, Qiang W, Zou D. "A practical privacy-preserving password authentication scheme for cloud computing", In2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum 2012 May 21, IEEE. pp. 1210-1217.
8. Choubey S.D, Namdeo M.K. "Study of data security and privacy preserving solutions in cloud computing". In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) 2015 Oct 8, IEEE. pp. 1101-1106
9. Yi, S., Qin, Z. and Li, Q., 2015, "August. Security and privacy issues of fog computing: A survey", In International conference on wireless algorithms, systems, and applications , Springer, Cham. pp. 685-695
10. Hussein, N.H. and Khalid, A. "A survey of cloud computing security challenges and solutions". International Journal of Computer Science and Information Security, 2016, 14(1), p.52.
11. Yi X, Rao FY, Bertino E, Bouguettaya A. "Privacy-preserving association rule mining in cloud computing". In Proceedings of the 10th ACM symposium on information, computer and communications security 2015, Apr 14, ACM. pp. 439-450.
12. Hejazi M, Al-Haddad S.A, Singh Y.P, Hashim SJ, Aziz A.F. "ECG biometric authentication based on non-fiducial approach using kernel methods", Digital Signal Processing. 2016 May 1;52, pp72-86.
13. Lu Y, Li L, Peng H, Yang Y. "An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem", Journal of medical systems. 2015 Mar 1;39(3),pp:32.
14. Jagadiswary D, Saraswady D. "Biometric authentication using fused multimodal biometric". Procedia Computer Science. 2016 Jan 1;85: pp109-16.
15. Chaudhry S.A, Khan M.T, Khan M.K, Shon T. "A multiserver biometric authentication scheme for tmis using elliptic curve cryptography". Journal of medical systems. 2016 Nov 1;40(11) pp:230.

16. Murillo-Escobar, M.A., Cruz-Hernández, C., Abundiz-Pérez, F. and López-Gutiérrez, R.M, "A robust embedded biometric authentication system based on fingerprint and chaotic encryption", Expert Systems with Applications, 42(21), 2015, pp.8198-8211.
17. Nakamura, T., Goverdovsky, V. and Mandic, D.P. "In-ear EEG biometrics for feasible and readily collectable real-world person authentication". IEEE Transactions on Information Forensics and Security, 13(3),2017 pp.648-661.
18. Gupta, P., Srivastava, S. and Gupta, P. "An accurate infrared hand geometry and vein pattern based authentication system. Knowledge-Based Systems, 103, 2016. pp.143-155.
19. Mohsin, A.H., Zaidan, A.A., Zaidan, B.B., bin Ariffin, S.A., Albahri, O.S., Albahri, A.S., Alsalem, M.A., Mohammed, K.I. and Hashim, M. "Real-time medical systems based on human biometric steganography: A systematic review", Journal of medical systems, 42(12), 2018. p.245.
20. Drygajlo, A. and Haraksim, R., "Biometric Evidence in Forensic Automatic Speaker Recognition". In Handbook of Biometrics for Forensic Science, Springer, Cham.2017, pp. 221-239.
21. Haghighat, M., Abdel-Mottaleb, M. and Alhalabi, W. "Discriminant correlation analysis: Real-time feature level fusion for multimodal biometric recognition". IEEE Transactions on Information Forensics and Security, 11(9),2016, pp..1984-1996.