SECURITY AND PRIVACY PRESERVATION SCHEME OF FACE IDENTIFICATION AND RESOLUTION FRAMEWORK USING FOG COMPUTING IN INTERNET OF THINGS USING OF PYTHON

P.ARUNAPRIYA,
V.R.KAVITHA,

PRATHYUSHA ENGINEERING COLLEGE,
ARANVOYAL KUPPAM,
POONAMALLEE,
THIRUVALLUR ROAD,
THIRUVALLUR-602025.

***Abstract*—Numerous applications are using face detection techniques to capture the facial images of the user as a sign of authorization. As the number of applications is increasing the images captured are also stored in a huge amount. These images are usually stored in a cloud-basedservice where the analyzing and processing of information for a particular application takes a lot of time. In this paper, we have brought a solution to this challenge by storing the informationand images using Fog computing in an IoT based environment. IoT is being used in many fields and it becomesthe prime responsibility to secure all the information being a store. The proposed framework provides a security and privacy preservationscheme using Fog computing which is used intensively for face identification applications. This minimizes the storage space required in the cloud and hence balances the load between various fog layers. In existing model, they didn't achieve the security level and efficiency level. Also there is no any hybrid security given with combinational. The experimental results determine that the proposed model has obtained an accuracy level of about 90% by offering minimal latency in the entire network.**

Keywords—***IoT, Fog Computing, Face Detection, Privacy Preservation, Security, Efficiency, Load Balancing, Storage***

INTRODUCTION

Numerous applications are being used that captures the images of the users to make it a way of authorizing the application. Lots of information are stored when an application is deployed in the realworld. Storing all these information needs a secured lace. Most of the companies rely on the traditionalcloud-based environment. Cloud is used by numerous application and it needs an alternative to balance the load between various nodes from where it is obtaining the data. An alternative to the cloud-based system is the Fog based computing where the data received from each node in the cloud environment are processed in separate layers of fog instead of being computed in the cloud environment. In this current approach, we have designed a model that could be used in real-world to maintain the privacy of the face detection images and the overallefficiencyofthe current use of fog is observed. Instead of storing the entire data in the cloud and processing it makes the poor cloud environment as it is not feasible to process the entire tons of data that is being accumulated in it. While using Fog computing, each Fog node has the datareceived from unique nodes in the cloud environmentthatmakes it

very easy for processing and hence increases the load balancing. The load is balanced between the various nodes in the fog layers. The computation time of processing the data is reduced whereas the delay time is also minimal. The architecture of how the information is processed in a fog computing environment is depicted in Fig. 1.

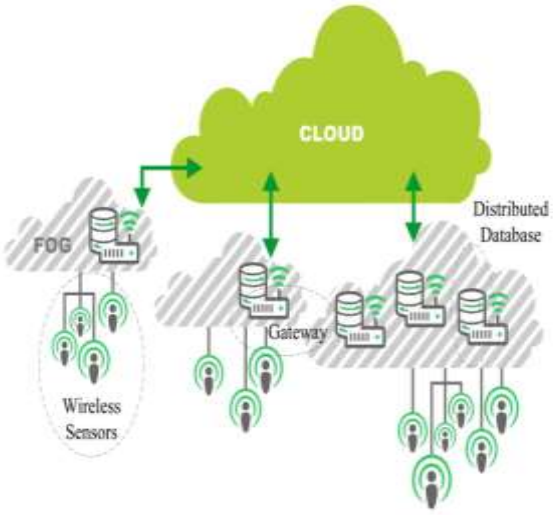

Fig. 1Architecture of Fog Computing

The analysis of the experimental results shows that the proposed model performs well in achieving a high degree of sensitivity on the point of that once it is been exploited to a straight threshold approach whereas it also additionally achieves a high degree of specificity on the point of that once exploitation the training techniques. The entire architecture of the proposed model is designed and explained how the model works. When compared with the existing model, the proposed approach seems to have good efficiency. The remaining of the paper consists of the section as follows:Section II consists of Literature Survey, section III consists of the methodology used in the paper and section III consists of various results obtained. The paper is concluded in the last by mentioning the relevant future works that could be applied or added to the proposed work.

I. RELATED WORK

Numerous researchers have been workingon Fog Computing to improve various parameters. When it comes to Fog computing,the veryfirst connected space that could be used for the analysis purpose is literally called fog computing [1,2,3,4]. In fog computing, the cloud is made to move from the network and is also a way where the routers can be used to become one of the virtualizationinfrastructures. One way of enhancing to extend the cloud wherefog computing could be used to offer various cloud infrastructures and also some of the smart-items in the infrastructures.Osadchy et al. [5] proposed an efficient system that are mainly intended to secure the overall privacy of the face identification system. Here a novel protocol was designed to secure a facial image that makes use of the homomorphism encryption. Huang et al. [6] proposed a technique that designed an efficient protocol for biometric identification. In this protocol, the ciphertexts used made extensive use of Euclidean distances comprising of vectors. The computational cost of the overall communication was observed to be high as the size of the database increases.

Haghighat et al. [7] proposed a cloud-based biometric identification technique that largely relied on confidential information processing. The stored information was encrypted and the scheme also met all the necessary demands that were needed for storing processing the data. The model made use of encrypted search query for searching the k-d structure in the encrypted data. Bommagani et al. [8] modeled a secure face recognition framework that was entirely based on processing multiple tasks in parallel. It was dependent on processing local binary pattern traditionally called as the LBP. Yuan and Yu [9] securely moved all the operations to cloud servers to maintain and preserve the privacy of the biometric identification framework. Xia et al. [10] made use of sensitive images such as personal images for preserving privacy. It made use of the K-NN algorithm for extracting the features of the images and then encrypting the pixels of the image to preserve it from malicious users. Lee et al. [11] proposed a method that analyzed and also surveyed all the other security-related problems that are faced and the challenges pertaining to fog computing. But

the paper ailed to elaborate on the solutions that could eradicate the problems being discussed.

II. PROPOSED APPROACH

The Proposed architecture designed in this paper is that uses Fog Computing is depicted in Fig. 2. The figure shows that the user or particular individual access the entire information by making use of his smartphones. The smartphones act as the fog nodes that consists of the entire cloud information in an information center. It also consists of the data center and the resolution server.

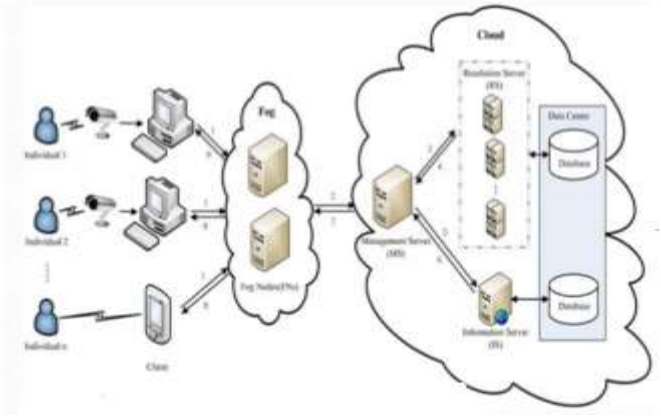

Fig. 2 Architecture of Proposed Model

The cloud information center is used to track all the information of a user and also to store the images that are captured for analyzing and processing of information. The datacenter is the server of servers. When a single server fails, the entire systems don't crash, the other server comes up without any delay. It is the prime responsibility of the datacenter to maintain all the servers and analyze them. The Resolution server is used to detail the resolution of the images in which they are captured. The pixels play a vital role in making a perfect resolution of facial detection. All the features need to be extracted for proper facial identification and detection. The resolution server is where even the low-quality images are transformed into high-quality images so that the features can be well extracted and also the model could perform a better facial detection and identification.

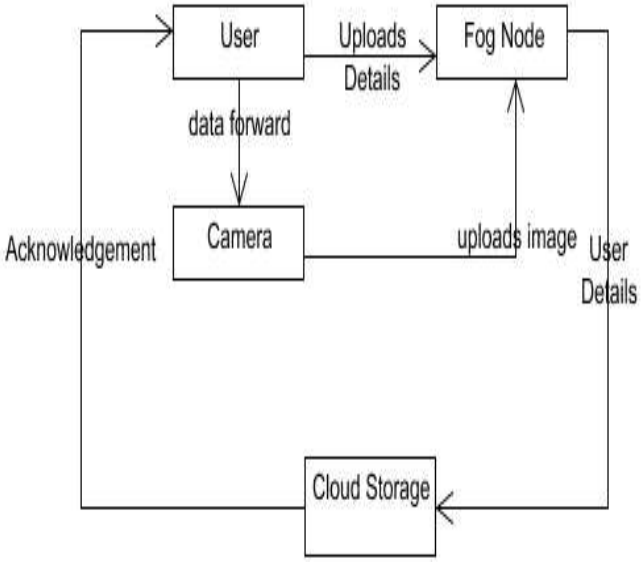

Fig.3 Block Diagram of Proposed Model

The block diagram of the proposed model is depicted in Fig. 3. The figure shows that the user is made to access the fog nodes by uploading his personal details. While doing this, the images of the users are also captured by the camera in the smartphone. All the information about the users isstored in the fog node. The analyzes of the application happen in cloud storage where the user gets the acknowledged whenever his application is accessed or any other new information needs to be informed to the user.

K- nearest neighbor algorithm

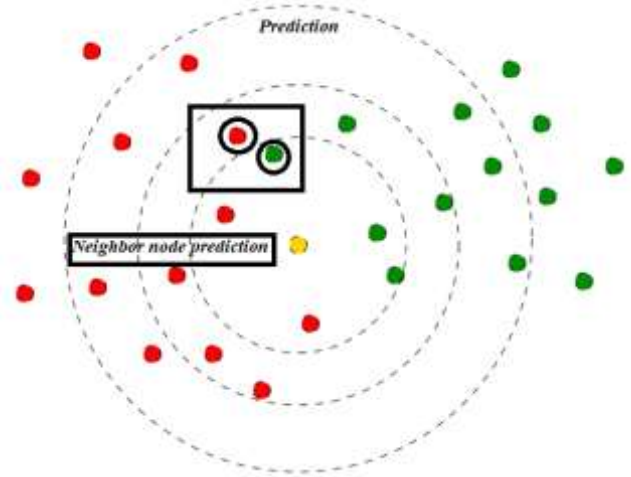

Fig. 4Prediction value

We have used this algorithm for predicting the points in the face. There are more area will be aborbed by the face technology. If the point was set to recognise the face then our application will use this technology for predicting the neighbor values. This algorithm was used to predict the user face values in different areas. It will also show the similarity values, if face is matching the predicted value then it will allow the user to access the data in fog. We have discussed our result in the next section by fixing our screeshots.

IV. EXPERIMENTAL RESULTS

The user details are registeredwitha unique user ID's in the application. While the process of registration, the user is made to enter all his personal information such as his name, age,and address and mobile number. At thisprocess, the application also captures the image of the user which is further used for facial detection. The face that is captured is stored in the Fog layer and retrieved when necessary. A face recognition scheme is developed that consists of the algorithm for detecting the face of the user when he needs to access the application. When the user initiates a sign in process again in the application, along with the user's credentials the face image of the user is again captured and compared with the image that he has uploaded during the time of registration. When the face is same, the user is able to login the application else the access is denied hence providing a secure and private mechanism for access the application.Various discussions and observations have been done on experimenting with the proposed model. Fig. 5 shows the efficiency of the proposed approach. The computation time for processing and storing the data is done using the simulator.

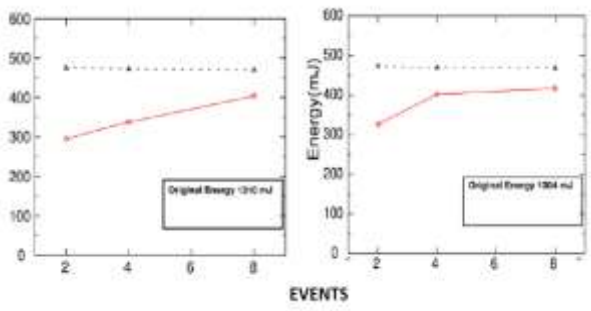

Fig. 5The efficiency of the Proposed Model

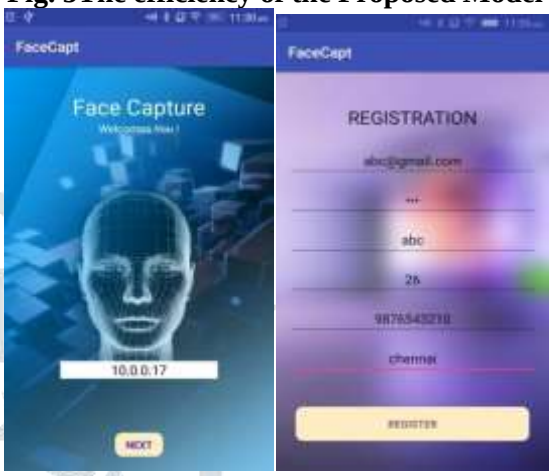

Fig. 6Registration Screen

In Fig.6, we have proposed the application with android plaform. Here, user should register their details like user id, password, age, mobile number and address for the future security. If user has forgot their password then they can change the password using OTP request to our mobile number. In Fig.7, after registration is completed, user need to log in using their user id and password. Finally, user can recognise the face using our application for securing the system.

Fig. 7Log in and face capturing Screen

IV.CONCLUSION

Fog computing is primarily used as an alternate or along with cloud computing for processing and analyzing the information in a separate node rather than saving it in the entire cloud-based server. In this paper, we have proposed a secured and privacy preservation framework for face identification using FOgComputing. The model is used to capture the faces of the users at the time of registration and at every sign in the applications captures the images of the user trying to access that application. The comparison if the face is done at each and every sign-in. Once the faces are similar the user is allowed to enter the application else his access is denied. The overall specificity of the algorithm proved to be effective when compared to other traditional algorithms. The distributed analytics and edge intelligence planned in our system utilized each smartphone and cloud services. The experiments show that the proposed model is able to do an occasional miss rate and an occasional false positive rate compared against the progressive systems. The future works might include some security add-ons to make the information more secure.

References

[1] L. M. Vaquero and L. Rodero-Merino. Finding youthe way in the definition fog: Towards a comprehensive offog computing. ACM SIGCOMM COMPUTERCOMMUNICATION REVIEW, 44(5):27{32, 2014.

[2] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu. Fogcomputing: A platform for the internet of things andanalytics. In Big Data and Internet of Things: A Roadmap for Smart Environments, pages 169 186. Springer, 2014.

[3] V. Stantchev, A. Barnawi, S. Ghulam, J. Schubert,and G. Tamm. Smart items, fog,and cloud computingas enablers of servitization in healthcare. 2015.

[4] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli. Fogcomputing and its role in the internet of things.InProceedings of the first edition of the MCC workshopon Mobile cloud computing, pages 13{16. ACM, 2012.

[5] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich, "SCiFI—A system for secure face identification," in Proc. IEEE Symp. Security Privacy, Oakland, CA, USA, 2010, pp. 239–254.

[6] Y. Huang, L. Malka, D. Evans, and J. Katz, "Efficient privacy-preserving biometric identification," presented at the Netw. Distrib. Syst. Security Symp. (NDSS), San Diego, CA, USA, 2011, pp. 421–434.

[7] M. Haghighat, S. Zonouz, and M. Abdel-Mottaleb, "CloudID: Trustworthy cloud-based and cross-enterprise biometric identification," Expert Syst. Appl., vol. 42, no. 21, pp. 7905–7916, 2015.

[8] A. S. Bommagani, M. C. Valenti, and A. Ross, "A framework for secure cloud-empowered mobile biometrics," in Proc. IEEE Mil. Commun. Conf. (MILCOM), Baltimore, MD, USA, 2014, pp. 255–261.

[9] J. Yuan and S. Yu, "Efficient privacy-preserving biometric identification in cloud computing," in Proc. IEEE INFOCOM, Turin, Italy, 2013, pp. 2652–2660.

[10] Z. Xia et al., "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

[11] K. Lee, D. Kim, D. Ha, U. Rajput, and H. Oh, "On security and privacy issues of fog computing supported the Internet of Things environment," in Proc. 6th Int. Conf. Netw. Future (NOF), Montreal, QC, Canada, 2015, pp. 1–3