International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 02, 2021

Biometric Cryptosystem Providing Data Protection In Fog Computing

P. Arul [1], N. Shanmugapriya [2]

[1]Research Supervisor, Assistant Professor, Department of Computer Science, Government Arts College
(Affiliated to Bharathidasan University, Trichy-24), Tiruchirappalli-620022, Tamil Nadu, India.
[2]Assistant Professor, Department of Computer Science, Government Arts College
(Affiliated to Bharathidasan University, Trichy-24), Tiruchirappalli-620022, Trichy, Tamil Nadu, India.

E_mail:[1]phdarul2004@yahoo.com, [2]shanmugapriyaragu@yahoo.com

ABSTRACT** – Over the recent decade, data processing transferred from cloud computing to the local processing environment named Fog computing. Fog computing is an extension of cloud computing, which process data nearby device instead of sending to the cloud this will reduce the burden from the Internet and quick processing.. In spite of the wide utilization of cloud computing, some applications and services still cannot benefit from this popular computing model due to innately problems of cloud computing such as undesirable latency, lack of mobility support and location awareness. As a result, Fog Computing is currently entice many researchers as it brings cloud services closer to the end users. The Internet of Things (lOT), current digitized intelligent connectivity domain, demands real time response in many applications and services. This furnish Fog Computing a suitable platform for achieving goals of autonomy and efficiency. Fog computing is still emit paradigm that demands further research. Among all the other issues customary in fog computing, security is the one of the blazing issues. The fog, existence closer to the end user, is more vulnerable than the cloud. The Biometric cryptography key is used to secure the scrambled data in the fog environment. The Biometric cryptography technique uses fingerprint, voice or iris as a key factor to secure the data encryption and decryption in the cloud server. Advanced biometrics are used to safeguard sensitive documents and valuables. A more instantaneous problem is that databases of personal information are targets for hackers. Biometric technology offers very constrain solutions for security. In the face of risks, the systems are convenient and hard to duplicate. Additionally, these systems will continue to develop for a very long time into the future.

IndexTerms - Fog Computing, Cloud Computing, Biometric, Internet of Things.

1. INTRODUCTION

The term “fog” arrived from the meteorological sector which brings the cloud near to the earth. Like this, Fog nodes bring down the resources of cloud computing to the edge nodes. This term “fog” is connected with the Cisco company, and the term was framed by the

Company's manager, Ginny Nichols and listed as "Cisco Fog Computing" and it is called by the common people as Fog computing. A Fog Computing

framework is distributed over the network with a variety of the different number of devices. These devices universally attached at the terminal of the network to provide adaptable communication, storage services, collaboratively variable and computation. Fog Computing gives many advantages in different areas such as real time, low latency, high response time, and especially healthcare applications. It is somewhere in-between the cloud data centers and user devices located at the ground (or at the base level).The topologies of FC are the main characteristics which differentiate it from the other technologies. In Fog Computing, the nodes are geographically distributed,
perform computations, and provide better storage space and better network services[1]. However, due to high latency and privacy gap in CC, FC came into the picture to solve these health-related issues.

Fog computing provides all the provisions to the end-users to use the services and resources of cloud computing. It permits to do temporary computations at the edge layer. Whereas edge nodes and sensors (IoT devices) are the data producers present at the ground level and the fog nodes are deployed closer to the edge nodes to limit the network traffic between the end devices and the cloud servers. Due to this limited distance, fog nodes are exposed to attackers. Once the fog nodes are compromised, then the privacy of the information will get affected [2]. To avoid this some security mechanisms like encryption is required. To avoid this some security mechanisms like encryption is required. In practical, it is hard to process the large volume of data generated by the multiple IoT devices which sends the same to the fog nodes. At this stage, data aggregation technique with homomorphic encryption is incorporated to avoid network traffic [3]. This will reduce the communication overhead when the data are sent to the cloud control center via the fog nodes. When using this technique, security and privacy issues also tackled with high extension. Also, this technique will help you to decrease the utilization of network bandwidth [4].

2. NEED FOR SECURITY PROTECTION IN FOG COMPUTING

As mentioned above, the increasing use of fog technology in the various walks of social and industrial areas has increased the pressure on the developers to create a safe threat proof system for a more efficient and reliable network for data storage and processing. With the rise in cyber threat and other malwares, this task is proving to be more difficult, as the traditional fog node creation does not include an inbuilt security protocol as these secure measures are added on later in the devices [9]. However, in view of the new trend, the developers have initiated the inclusion of preprocessed security protocols to furnish a stronger and safer fog computing unit for its use. This was achieved by shifting the focus from better storage and processing system to a security centric device generation.

3. RELATED WORK:

In 2016 Vishwanath et al, implemented the AES algorithm with various datasets to ensure the data security in the fog computing. This research makes another level of security and creates difficulty for the attackers to get the data. Also, various performance measures of the encryption technique are analyzed to ensure the accuracy of the entire data present in the

datasets. These provide more advantage to the deployed system. But the weakness is AES key size is limited to a fixed size [10].

In 2018 Zang et al. describes the various architectures of Fog computing and identify the possible security and trust issues. Also investigate the solutions to overcome those issues and specify the real challenges present in security and trust in Fog Computing. In this paper, the drawback is it needs some new protocols and interfaces to ensure the security and trust, but it is very poor to automate the identification of security and trust vulnerabilities. [11]

In 2018 Zang et al. proposed a method named as pallier encryption scheme for protecting the privacy of the data. This scheme ensures that the data inserted is only from genuine IoT devices. Also, it ensures the data packets are not disclosed to any others. It is observed that the data gathering from IoT devices are not affected even if some fog nodes are failed to transmit the data. This is a major advantage of this method. And the problem is, these security results are not enough to protect the CIA of fog platform[11].

In 2019 Shen et al proposed a scheme to protect the privacy and collusion opposing data aggregation for dynamic groups. Also develop a strong data encryption, aggregation and decryption schemes in fog computing. The demerit of this scheme is it requires a third party assistance for data aggregation. [14].

Data security is one of the key challenges in the big data era [15]. In this context, securing the data in cloud computing invoked the efforts of crypt-analysts, network security experts, software security engineers, and many others, and data breaches are still occurring within cloud computing [16]. In fact, the data security issue is aggravated in the case of fog computing [17].

Delivering Security as-a-Service (SECaaS) was proposed to ensure end to-end system security including fog nodes, network, and data security. This method senses the amount of energy about a linked node and also takes the highest-energy route to transmit data to the surface location node. In the event that surface position node is occupied with contacts, an update instruction will be given to the successor sub-aquatic neighbor to take a replacement surface position node to avoid data loss [18]. First, the fingerprint data is exploited to cancelable transformation to generate a bit-string. The derived bit-strings are then used for mutual locker and personalized locker generation. Further, the cryptographic keys are secretly exchanged using these lockers. Panchal et al. (2017).

Jagadeesan et al. [19] proposed an efficient approach based on multimodal biometrics such as Iris and fingerprint for generating a secure cryptographic key. First of all the features, minutiae points and texture properties are extracted from the fingerprint and iris images respectively. second, the extracted features are fused at the feature level to obtain the multi-biometric template. At last,a multi-biometric template is used for generating a 256-bit cryptographic key. After simulation, experimental results have showed that the 1 / 5 Cryptographic Key Generation from Multiple Biometric Modalities. Fusing Minutiae with Iris Feature generated 256-bit cryptographic key is said to be capable of providing better user authentication and better security.

4. PROBLEM STATEMENT

Fog computing paradigm extends the storage, networking, and computing facilities of the cloud computing toward the edge of the networks while offloading the cloud data centers and reducing service latency to the end users. In the manner, the characteristics of fog computing arise new security and privacy challenges. The conventional cloud-based security mechanisms include the use of heavyweight cryptosystems, which are not suitable for direct application in the fog computing. Fog computing is vulnerable to security attacks because it is designed upon traditional networking component. Therefore, it has become indispensable to address the fog security and privacy issues. The proposed solution aims fog devices that are computationally constrained and thus, not capable of preforming intense computations; they are capable of performing very basic operations and lightweight encryption.
Biometrics is the most appropriate means of identifying and verifying individuals in a reliable and fast way through unique biological characteristics. We proposed an efficient approach based on multimodal biometrics such as Iris and fingerprint for generating a secure cryptographic key.

5. BIOMETRICS AND DATA PROTECTION

The "United Nations Resolution" of 14 December 1990, which sets out guidelines for computerized personal data files regulation, does not have any binding force.
On a more global basis, legal deliberations thus rely mostly on personal data provisions in the broad sense. But such provisions sometimes prove to be poorly adapted to biometrics. On the contrary, the new E.U. regulation replaces the prevailing existing national laws as of May 2018.
The Next Generation Biometrics Market is Segmented by Type of Solution (Face Recognition, Fingerprint Recognition, Iris Recognition, Palm Print Recognition, Signature Recognition), End-user Vertical (Government, Defense, Travel and Immigration, Home Security, Banking and Finance, Consumer Electronics, Healthcare), and Geography.

A.Market Overview
The next generation biometrics market has record a CAGR of 35.53%, during the forecast period (2021 -2026). One of the key trends witnessed within the next generation biometrics market may be a paradigm shift in business discourse toward more privacy and fewer security threats. The end-users are increasingly trying to find integrated solutions, instead of counting on conventional methods.

- The next generation biometric market is expected to grow at a significant growth rate, due to the rising number of terrorist activities, coupled with the increasing theft activities on the a part of crucial data and knowledge that have raised concerns regarding national security. Major points, such as growth in e-passport program, government support, and extensive use in criminal identification, are majorly driving the market.
- The growth in airport security initiatives and attempts to reduce the crime rates have increased the investments in biometric systems, globally. Various government initiatives, like e-passports, e- driving licenses, border management, and national IDs, are being implemented within the developed countries using advanced biometrics
- IRIS recognition is one of the fastest-rising segments among the type of solution. Few benefits of this technology are that it's easy to use, difficult to forge, and is accurate. The iris recognition application within the consumer electronics sector is predicted witness the very

best rate of growth during the forecast period, mainly due to the commercialization of varied iris scan-based electronic devices, like smartphones, tablets, smart watches, notebooks, et al. .

- Nevertheless, factors, such as high deployment costs and fear of privacy intrusion, are expected to hamper the growth of the market.

B.Scope Of The Report

Later generation biometrics are the technologies used to authenticate the identity of individuals through biological characteristics, such as facial expression, voice, palm, fingerprints, signature, iris, vein, and DNA. The biometric techniques are easy to use and therefore the data obtained is in digital format, which is tough to forge or duplicate and rebuild. Moreover, next generation biometrics are available in various sort of solutions which will cater to several end-user verticals consistent with their need.

By Type of Solution

- FACE RECOGNITION
- FINGERPRINT RECOGNITION
- IRIS RECOGNITION
- PALM PRINT RECOGNITION
- SIGNATURE RECOGNITION

C.Key Markek Trends

Banking And Financial Industry To Be The Fastest-Growing Sector

- Major Banks are turn out biometric authentication. JP Morgan Chase, Bank of America and Wells Fargo allow their customers to log in to mobile banking via fingerprint authentication.
- Voice authentication is also installed in bank call centers to identify customers. Next generation biometric authentication can improve customer satisfaction by eliminating the need for passwords and as a result, rise the demand for acquiring of biometrics in the banking sector.
- Wells Fargo is working on a payment solution that will make use of the voice of its customers to authenticate transactions and access services. While other banks and financial institutions still have limited approach toward voice biometrics and use it only to let customers access information, like account balance, etc., Wells Fargo took the step to use voice biometrics to authenticate payments.

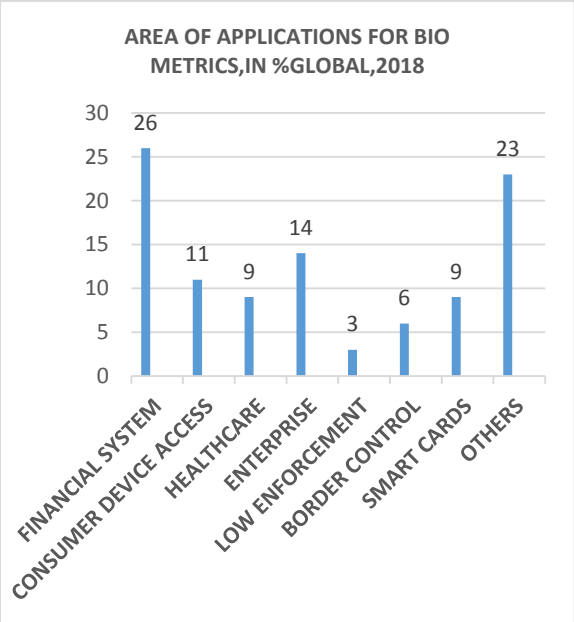

Fig.1 Find Biometrics (Sample Report).

D.Safety And Privacy Levels Of Data

The privacy and security of health data can be ensured by proper authentication using biometric signatures. The authors proposed distinct levels of security for various types of data as shown in Figs. 2, 3. Text passwords and user names represent the lowest level of security. Images and video recordings require the highest level of security features.

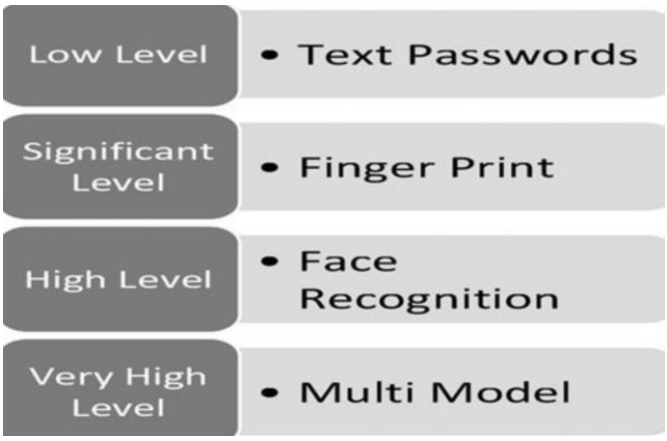

Fig. 2 Security levels and data types

Fig.3 Fog Computing Application for Biometric-Based Secure Access. ..

6. FOG COMPUTING FOR ENHANCING BIOMETRIC SECURITY

The edge computing helps us to solve the difficulties connected with safety and confidentiality of biometric signatures by improving security and privacy of critical patient information. The intrinsic properties of fog computing permit additional advantages of computing features which are essential for ensuring the privacy and security-sensitive data access by computing important data at the fog nodes and transmitting the secure and encoded data to cloud after processing.

A. High Security Of Transition Based Biometric Cryptosystems For Fingerprint Protection

In the worker knowledge base, scale drawing are taken care of with a fingerprint eminent system. Different systems to ensure biometrics layouts, such as biometric encryption, salting, and non-invertible adjustment, are proposed to overhaul authentication to prevent assurance issues in the event that the knowledge base is bartered. Nonetheless, along with protection, range, and revocability, a solitary approach cannot meet all application requirements. Among various physiological biometric traits, the fingerprint
is extensively used as it is convenient to capture, easy to process, and is found to be persistent. Fingerprint-based authentication systems [20,21] mainly rely on the information of minutiae points and singular points. In a fingerprint image, points of ridge bifurcation and ridge ending are the widely used minutiae points.

Further, the core point and the delta point in a fingerprint are used as singular points where the core point is defined as a point where the curvature of the ridges is the most, and the delta point is defined as the point where ridges form a delta shape.

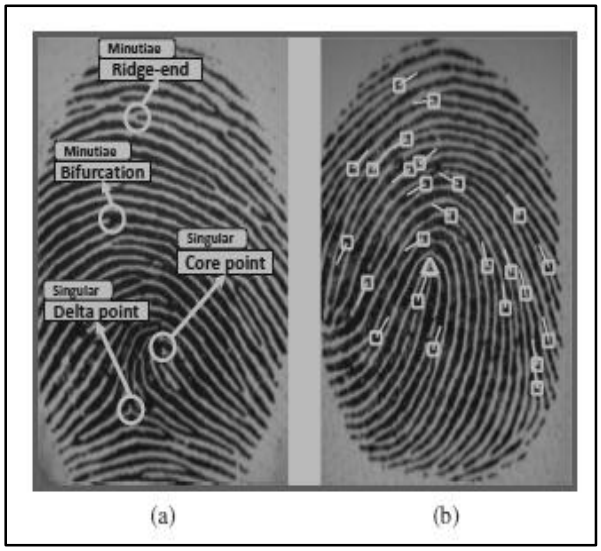

Fig.4 Fingerprint images representing (a) types of feature points in a fingerprint, (b) extracted feature points (minutiae points along with rientation information represented using square) and singular point (represented using triangle)

An example of a fingerprint image with minutiae points and singular points marked on it is shown in Figure 1. In a fingerprint-based authentication system, usually, information of minutiae points (i.e. location of minutiae point and orientation of ridge at minutiae point) is stored in the database to recognize the original fingerprint image by using the information of minutiae points [1, 6]. Moreover, in [7], a method describes that even an original fingerprint can be formed by using the minutiae template of ISO standard. As we know, the fingerprint is a permanent biometric feature associated with a person, and it is not possible to change it if it is compromised in the event of an attack. To protect the information of fingerprint template, many template protection techniques have been proposed, which are mainly classified under two categories: *biometric cryptosystem* [8] and *cancellable biometrics* [3]. The technique proposed here falls under the latter category, which suggests that a biometric template obtained by transforming the original template should be stored in the database instead of the original template to protect it. This transformation should exhibit some essential characteristics, which are given below.

- **Renewability:** Renewability requires that it must be possible to generate an entirely new template using the same biometric data if the stored template is compromised.
- **Unlinkability:** It states that the templates which are generated by utilizing the different parameters of the transformation function should be unlinkable with each other. Due to the unlinkability of a user template, a stored template can easily be replaced by another one in the event of an attack on the database.
- **Security:** If a template which is constructed after performing a transformation on an original template is compromised, then intruder should not be able to reconstruct the original biometric image by utilizing it. This ensures that the transformation technique is strong enough to protect the privacy of users and prevent unauthorized access in the biometric system.

- **Recognition rate:** Recognition rate or matching performance of a biometric system should not be degraded due to the transformation used to protect the original biometric template.

A new technique to protect fingerprint templates is presented. The proposed technique satisfies all the characteristics listed above and is shown to be robust to attacks. The significant contributions of this research work are mentioned below.

1. The proposed technique generates a non-invertible 3D user template which ensures the security of fingerprint data of a user stored in the database.
2. As alignment is a crucial step in a fingerprint-based system, an alignment technique utilizing the principal component analysis (PCA) is proposed, which does not store any auxiliary information into the database for alignment during verification.
3. A large number of distinct user templates can be constructed from the same biometric data using different values of keysets. This makes the templates fully unlinkable and renewable.
4. The transformed user templates are highly secure as it is infeasible to restore the original fingerprint data from the transformed template even if an adversary gets the information of keyset.
5. The proposed technique has shown good performance even in the case of challenging databases such as FVC2002 DB3, FVC2004 DB1, and FVC2004 DB2. a person. If any attack happens on the database and stored information is compromised, then it is possible to reconstruct.

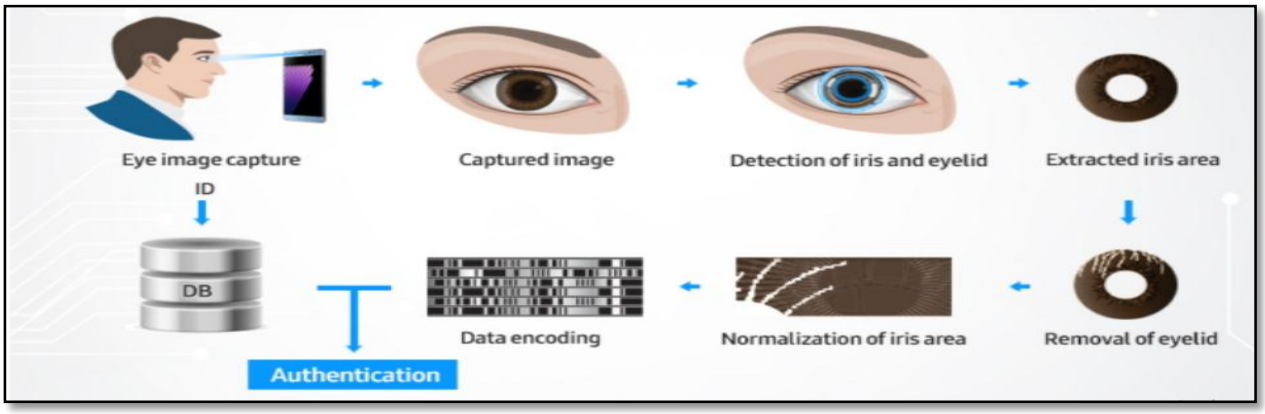

Fig.5 Iris Recognition based biometric security.

B. Literature on Iris Recognition based Biometric Security

The colored circular section in the human eye is called iris and this can be seen with the normal eye. Iris is comprised of muscles that modify the pupil's size and also controls the quantity of light coming into the eye. Quantity of melatonin pigment contributes to various colors in the formation of iris of humans. The iris muscle foldings covering the ring generate a structure giving a greater level of detail. The creation process of muscle structure is stochastic and it will not follow any specific rules to govern the formation of structure in a human's eye. This muscle structure once created remains permanent throughout the life of the person. Each person's iris is unique and has a distinct pattern for each eye. These properties are considered for individual recognition. A high-quality digital camera can scan the details of iris muscle structures. The iris recognition system uses near-infrared (NIR: 700–900 nm) radiation to capture iris structure. The iris recognition software is installed in a dedicated system to get efficiency and security purposes. A camera captures the image of this structure

of iris muscles and its quality is upgraded by the image enhancement procedures. Every iris formation is unique even the

two iris of a person are not identical and there are variations in iris of twins also [22, 23]. This improved image is processed by the recognition system to identify the distinct features to create a biometric template. Matching the sample current iris data with this stored iris template confirms the identity of the person under consideration.
Iris recognition offers minimum cost of implementation with high security and user friendliness. Iris recognition has been implemented by border control agencies of 15 Fog Computing Application for Biometric-Based Secure Access. . . 361 the United Arab
Emirates at border security checkpoints. All the foreign travelers with visitor visas have to undergo an iris recognition system for entry into UAE. CANPASS Air program based on iris recognition is operational in several Canadian airports. Aadhaar, a citizen identification system from the government of India's program is the unique method, where the biometric signatures are extensively used for citizen identification and linked to all public services. Iris identification of a person using iris is very successful in many applications.

7. PROPOSED SYSTEM

In our proposed cryptographic solution is based on Biometric key-dependent approach, which allows for a good compromise between the security level and computational complexity. In this paper, we proposed various techniques related with Cryptographic key generation based on Biometric parameter such as iris, fingerprint .We proposed an efficient approach based on multimodal biometrics such as Iris and fingerprint for generating a secure cryptographic key. A new key is generate to encrypt the Fog data with help of AES algorithm integrated with biometric data to ensure the data security. Biometrics is rapidly becoming a key piece of the security infrastructure and multifactor authentication – providing quick and easy verification, audit logs, and analysis.
The security is an important aspect several applications where security plays vital role. Cryptographic techniques are widely used in many fields to secure confidential data during its storage and transmission. Authentication can be achieved using shared key which will be compared to a stored template to provide authentication of the individual. In security applications, there are several techniques based on biometrics such as iris recognition, face recognition, fingerprints, hand, voice etc. Among the all the biometric features, iris and fingerprint are the unique biometric identifier and also has high identification accuracy. These systems are authorizing essential as the industry continues to scale and become more complex – and we should expect even bigger things in the years ahead. While biometrics provide non-repudiation and convenience, traditional cryptography provides adjustable levels of security and can be used not just for authentication, but also for encryption. In the proposed solution, the collected data at one fog node is encrypted, and dispersed in a random manner to its n neighbor fog nodes. We also adopt consistent hashing scheme the encrypted data is distributed to another fog node. It can be considered as a insubstantial solution and it can be adapted according to the fog limitations in terms of power, storage, and computations.

8. CONCLUSION AND FUTURE SCOPE

Fog computing is an evident area for IOT applications. However, making full use of the geographically distributed network edge devices, the fog paradigm drive more and more applications and services from cloud to the network edge. It significantly reduces the data transfer time and the amount of network transmission, and effectively meet the demands of real-time or latency sensitive applications and ease network bandwidth bottlenecks. Fog is attractive target for cyber-attackers since the fog contains huge volumes of sensitive data from both Cloud and IOT devices. In this way, futher research is required to improve fog security. In this paper, we focus on the fog computing technology. The architecture, challenges of fog computing and its security issues. Based on the survey, one of the key challenge is data security. We proposed an efficient approach based on multimodal biometrics such as Iris and fingerprint for generating a secure cryptographic key. In this research concluded with new multimodal biometric secret key using AES algorithm to create a secure network where all the IOT data can be privately stored and shared in the current.

9. REFERENCES:

[1] Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012, August). Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on mobile cloud
[2] computing (pp. 13–16). New York: ACM.
[3] Jia, W., Zhu, H., Cao, Z., Dong, X., & Xiao, C. (2013). Human-factoraware privacy-preserving aggregation in smart grid. IEEE Systems
[4] Journal, 8(2), 598-607.
[5] Wang X, Wang L, Li Y, Gai K(2018) Privacy-Aware Efficient Fine-Grained Data Access Control in Internet of Medical Things Based Fog Computing. IEEE Access 6(1):47657–47665.
[6] Bouzefrane, S., Mostefa, A.F.B., Houacine, F., Cagnon, H.: Cloudlets authentication in nfc-based mobile computing. In: MobileCloud. IEEE(2014).
[7] Hu, P., Dhelim, S., Ning, H., & Qiu, T. (2017). Survey on fog computing: architecture, key technologies, applications and open issues. Journal of network and computer applications, 98, 27-42.
[8] O. Salman, I. Elhajj, A. Chehab, and A. Kayssi,"Iot survey: An sdn and fog computing perspective,"
[9] Computer Networks, vol. 143, pp. 221 – 246, 2018 .
[10] article/pii/S1389128618305395
[11] C. B. Tan, M. H. A. Hijazi, Y. Lim, and A. Gani,"A survey on proof of retrievability for cloud data
[12] integrity and availability: Cloud storage state-of-the-art,issues, solutions and future trends," Journal of Network and Computer Applications, vol. 110, pp. 75 – 86, 2018.
[13] [Online]. Available: http://www.sciencedirect.com/science/
[14] article/pii/S1084804518301048
[15] Y. Guan, J. Shao, G. Wei, and M. Xie, "Data security and privacy in fog computing," IEEE Network, vol. 32, no. 5, pp.106–111, September 2018.
[16] ETSI: Mobile-edge computing. http://goo.gl/7NwTLE (2014).
[17] Vishwanath, A., Peruri, R., & Jing (Selena) He. (2016). Security in fog computing through encryption. DigitalCommons@ Kennesaw State University.

[18] Zhang, P., Zhou, M., & Fortino, G. (2018). Security and trust issues in Fog computing: A survey. Future Generation Computer Systems, 88, 16-27.
[19] Zhang, Y., Zhao, J., Zheng, D., Deng, K., Ren, F., Zheng, X., & Shu, J.(2018). Privacy-preserving data aggregation against false data injection attacks in fog computing. Sensors, 18(8), 2659.
[20] Shen, X., Zhu, L., Xu, C., Sharif, K., & Lu, R. (2020). A privacy preserving data aggregation scheme for dynamic groups in fog computing. Information Sciences, 514, 118-130.
[21] B. A. Martin, F. Michaud, D. Banks, A. Mosenia, R. Zolfonoon, S. Irwan, S. Schrecker, and J. K. Zao, "Openfog security requirements and approaches," in 2017 IEEE Fog.
[22] Cao, N., Wang, C., Li, M., Ren, K., Lou, W.: Privacy-preserving multi keyword ranked search over encrypted cloud data. TPDS 25 (2014)
[23] Wei J, Wang X, Li N, Yang G, Mu Y(2018) A Privacy-Preserving Fog Computing Framework for Vehicular Crowdsensing Networks. IEEE Access 6(1):43776–43784.
[24] https://www.sam-solutions.com/blog/fog-computing-vs-cloudcomputing-for-iot-projects/World Congress (FWC), Oct 2017, pp. 1–6.
[25] Kashish Shakil, A., Farhana Zareen, J., Alam, M., Jabin, S., & BAMHealthCloud. (2017). A biometric authentication and data management system for healthcare data in Cloud, Journal
[26] of King Saud University. Computer and Information Sciences, 32, 57. https://doi.org/10.1016/j.jksuci.2017.07.001.
[27] Jagadeesan, T.Thillaikkarasi, Dr.K.Duraiswamy "Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature" International Journal of Computer Applications, 2010 .
[28] Maltoni, D., et al.: Handbook of Fingerprint Recognition, 2nd ed. Springer Publishing Company, Incorporated, London (2009)
[29] Uz, T., et al.: Minutiae-based template synthesis and matching for fingerprint authentication. Comput. Vis. Image Underst. 113(9), 979–992 (2009).
[30] Ali Alheeti, K. M. (2011). Biometric Iris recognition based on hybrid technique. International
[31] Journal on Soft Computing (IJSC), 2(4). https://doi.org/10.5121/ijsc.2011.24011.
[32] Shubhika Ranjan, Prabu S, Swarnalatha P, Magesh G, Ravee Sundararajan, Iris Recognition
[33] System, International Research Journal of Engineering and Technology (IRJET), e-ISSN:
[34] 2395–0056, Vol: 04, Issue: 12, (2017). Retrieved from https://www.ijeat.org/wp-content/
[35] uploads/papers/v8i5S3/E11030785S319.pdf