ENHANCING DATA SECURITY IN IOT HEALTHCARE SERVICES USING OF FOG COMPUTING

Dr. B. Sravan Kumar, Assistant Professor, CSE(AI & ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal(Mandal), Warangal Urban-506005(T.S), India
Mrs.Ch.Sruthi,Assistant professor, CSE(AI&ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal (Mandal), Warangal Urban – 506005(T.S), India
Thriveni. I (21645A6611), UG Student, CSE(AI &ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal(Mandal),Warangal Urban-506005(T.S,)India
K. Ajay Kumar (21645A6612), UG Student, CSE(AI &ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal(Mandal),Warangal Urban-506005(T.S), India
Sumeet Maley (21645A6620), UG Student, CSE(AI &ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal(Mandal),Warangal Urban-506005(T.S), India
D. Punnam Chander (20641A66E1), UG Student, CSE(AI &ML), Vaagdevi College of Engineering (Autonomous), Bollikunta, Khila Warangal(Mandal),Warangal Urban-506005(T.S),

ABSTRACT
Internet of factors (IoT) is the interconnection of bodily objects or gadgets which can transmit and obtain facts via the net with out human involvement. With the advancement in IoT gadgets particularly in healthcare region, massive quantity of statistics is collected from one-of-a-kind sensors and all this facts are transferred and saved in cloud. It will become difficult to handle such huge quantity of statistics in cloud especially the healthcare facts wherein it requires actual time information computation and storage. safety of the statistics is also predominant mission in cloud. Fog computing is the solution to triumph over the demanding situations. Fog nodes works at the edge side and enhances facts protection, accuracy, consistency and reduces the latency rate that is an important issue for application like scientific statistics. Implementation paintings is likewise defined inside the paper in which a digital human temperature sensor device is built the use of DS18B20 temperature sensor. The records gathered from it's far being encrypted in fog node the use of strengthen Encryption popular(AES) algorithm and it's miles send to cloud. therefore, the security of the fitness care data is more suitable the usage of Fog computing.

1.INTRODUCTION
In the world of technology where we are living in, almost all the devices are connected to internet. The number of IoT devices are increasing in an exponential rate and all these devices are relying on cloud computing system for data computation and storage. It becomes a bottle neck problem when it comes to realtime data operation which is the major drawback in the existing IoT healthcare system [1]. In order to overcome the problem Fog Computing concept has been introduced. Fog Computing [2] in an archetype that extends the cloud computing platform. Fog acts as a middle layer between the cloud server and the end devices. It is not the complete replacement of cloud, rather it Fig1: Fog Computing Architecture [3] complements the functionality of cloud. Fog works closer to the edge devices and provides computing resources to these devices. Fog computing overcomes the scalability and reliability issues which is there in the traditional IoT-cloud architecture. Since Fog nodes works at the edge side and more geographically distributed as in (Fig:1), it enhances data security [4][5], accuracy, consistency and reduces the latency rate which is an important factor for application like medical data. As well as the overall bandwidth to cloud is saved, thus achieving better quality of service(QoS) [6].

ISSN: 2278-4632
Vol-14, Issue-5, May: 2024

2.LITERATURE SURVEY

Security of the data is also major challenge in cloud. Fog computing is the answer to overcome the challenges. Fog node works at the edge side and enhances data security, accuracy, consistency and reduces the latency rate which is an important factor for application like medical data. In this paper we will detect the heart disease by using sensors and pulse rate. The data detected will be stored in the fog node .The result would be display by the system as well as report will be sent through mail to the patient. The data collected from it is being encrypted in fog node using Advance Encryption Standard (AES) algorithm and it is send to cloud. Therefore, the security of the health care data is enhanced using Fog computing [7].

An equipment corporation does not, however, except an IoT based Healthcare Corporation from complying with the laws appropriate to its operating section which safeguard individual data. The final outcome is in healthcare solutions needing protection and solitude [8]. There are many advanced mechanisms addressing these concerns, but they have been built in the background of integrated hospitals and care contributors, where resources, computing capacity, announcements and electrical power are available to ensure exceedingly vigorous health. Which include technological (low processing speed, restricted resources, sporadic communication) organizational. It then provides an indication of some of the major frameworks, followed by a measurement of how this is restricted within an IoT based Healthcare systems [9].

The history of human development has proven that medical and healthcare applications for humanity always are the main driving force behind the development of science and technology. The advent of Cloud technology for the first time allows providing systems infrastructure as a service, platform as a service and software as a service. Cloud technology has dominated healthcare information systems for decades now. However, one limitation of cloud-based applications is the high service response time [11]. In some emergency scenarios, the control and monitoring of patient status, decision-making with related resources are limited such as hospital, ambulance, doctor, medical conditions in seconds and has a direct impact on the life of patients. To solve these challenges, optimal computing technologies have been proposed such as cloud computing, edge computing, and fog computing technologies [12]. In this article, we make a comparison between computing technologies [13]-[14]. Then, we present a common architectural framework based on fog computing for Internet of Health Things (Fog-IoHT) applications. Besides, we also indicate possible applications and challenges in integrating fog computing into IoT Healthcare applications [15]. The analysis results indicated that there is huge potential for IoHT applications based on fog computing. We hope, this study will be an important guide for the future development of fog-based Healthcare IoT applications [16].

3.PROBLEM STATEMENT

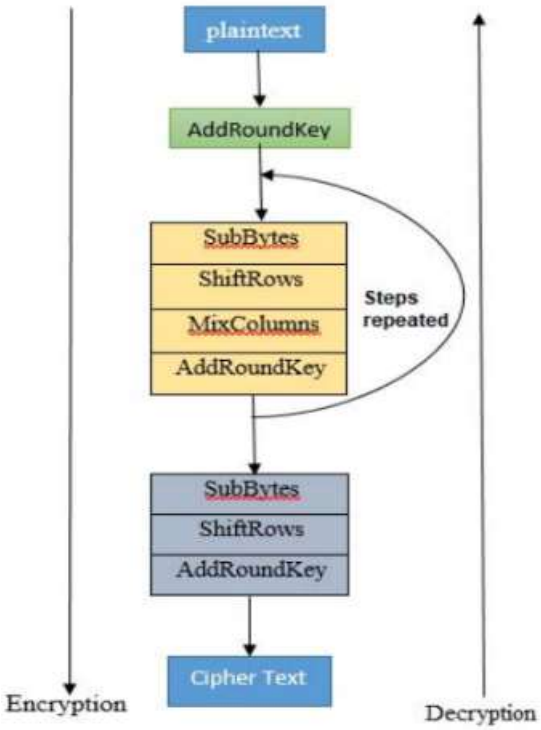
Currently fog uses the Decoy system [10][11] as a security service from malicious attacker. Like in Cloud, Fog uses this method to trick the attacker by providing fake data when they try to extract the data. In the decoy system the user has to sign up then login, while logging in the system will ask security questions related to information given while signing up. So when an attacker tries to login her/she will be trapped with the question and the system will give back spurious file which is very such similar to the original file and when the attacker tries to download it will turn out to be a fake data. But there is chance that the attacker might guess the questions right. Therefore, this system is not a very good way of securing data[17]

ISSN: 2278-4632
Vol-14, Issue-5, May: 2024

4.PROPOSED SYSTEM

In the proposed system a three tier architecture [18] [19] model is considered as in fig2. First layer will be the Edge devices which will collect the data and this data will be transferred to the middle layer. The middle layer will be the fog layer; encryption process of the collected data will be performed in this layer. The encrypted data from the middle layer will then be send to the third layer which is the cloud layer. In the cloud the final encrypted data will be permanently stored.

5. SYSTEM ARCHITECTURE



6.IMPLEMENTATION

6.1 Data Encryption Module: This module focuses on encrypting sensitive data transmitted between IoT devices and fog nodes, as well as fog nodes and cloud servers. Encryption ensures that even if the data is intercepted, it remains unintelligible to unauthorized users.

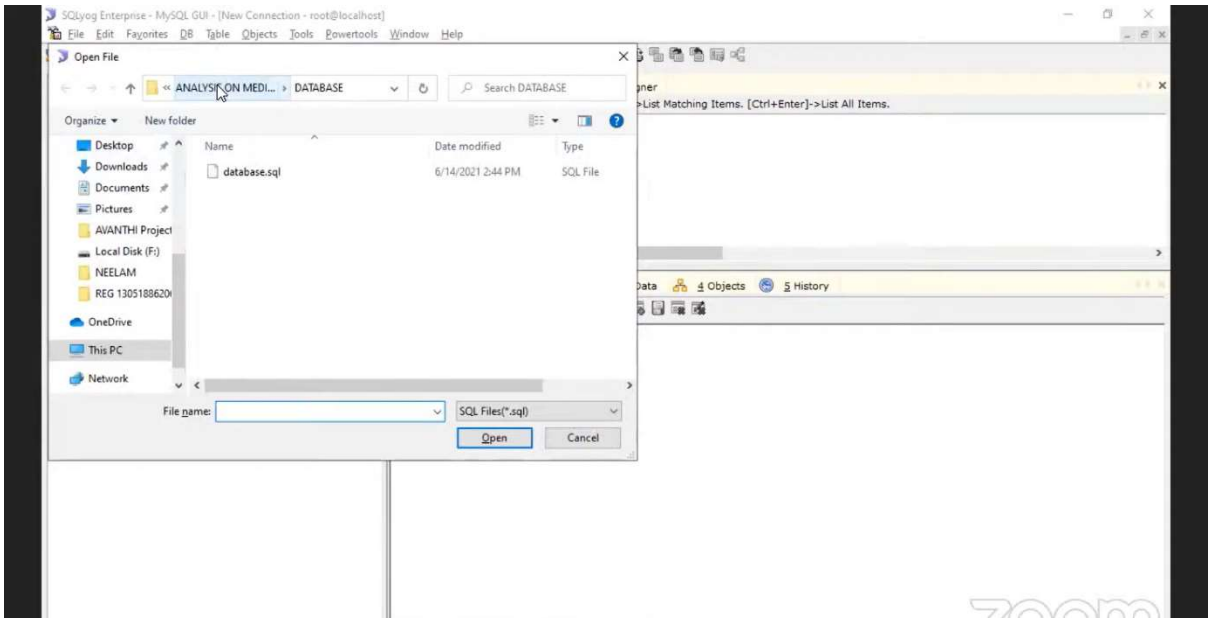
6.2 Access Control Module: This module manages access permissions to IoT healthcare services and data. It enforces role-based access control (RBAC) or other access control mechanisms to ensure that only authorized personnel can access specific data and functionalities.

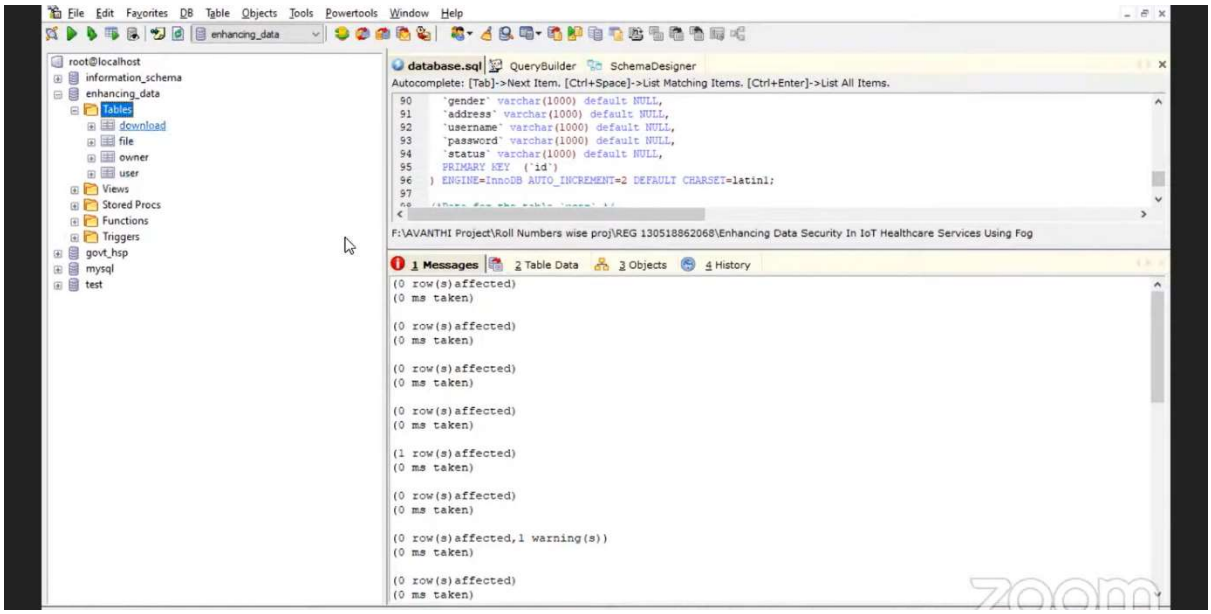
6.3 Authentication Module: The authentication module verifies the identity of users, IoT devices, and fog nodes before granting access to sensitive data or services. It can use techniques like username-password authentication, multi-factor authentication (MFA), or digital certificates.

6.4 Secure Communication Module: This module ensures secure communication channels between IoT devices, fog nodes, and cloud servers. It may implement protocols like HTTPS, SSL/TLS, or other secure communication protocols to protect data during transit.

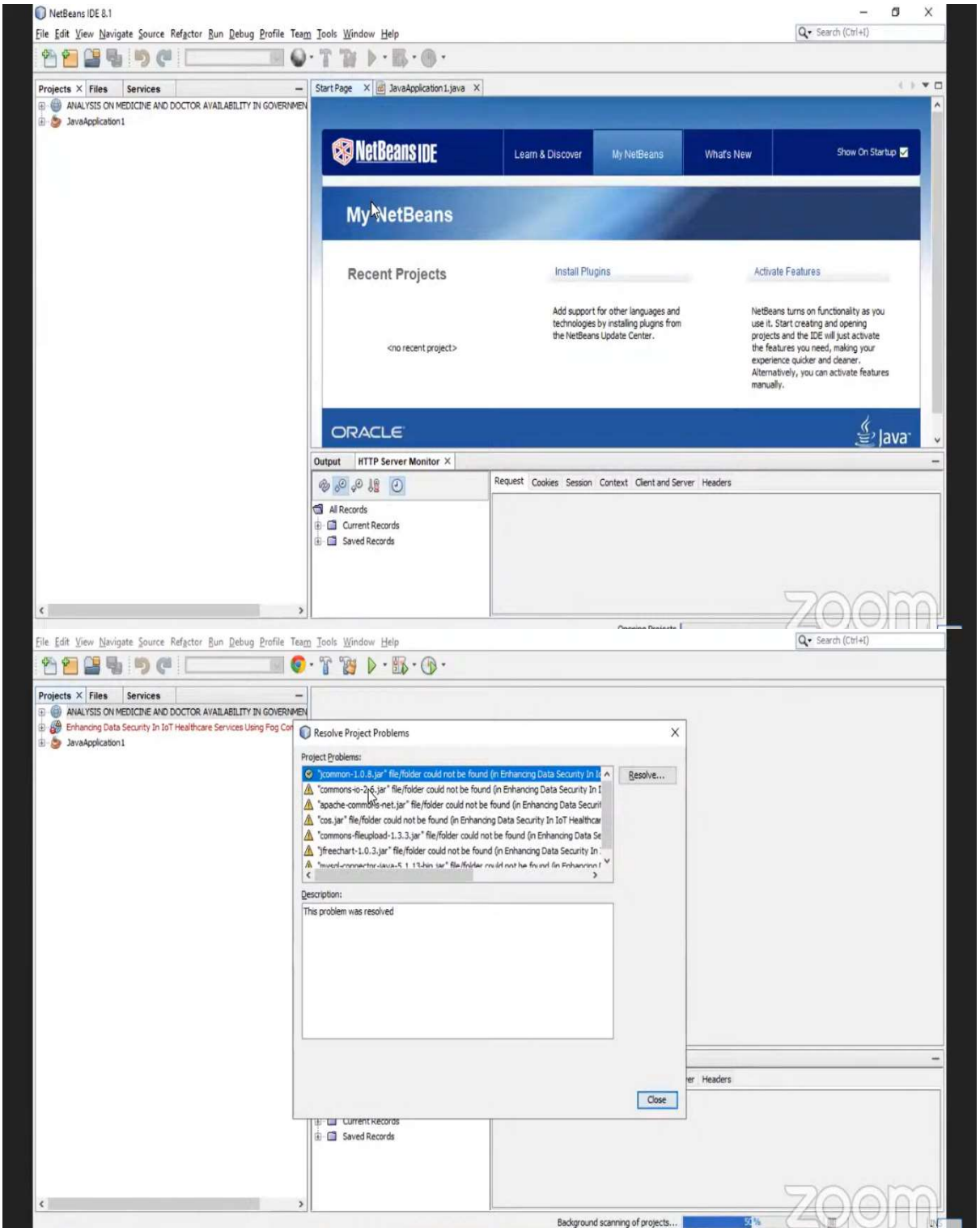
ISSN: 2278-4632
Vol-14, Issue-5, May: 2024

7.EXPECTED RESULTS

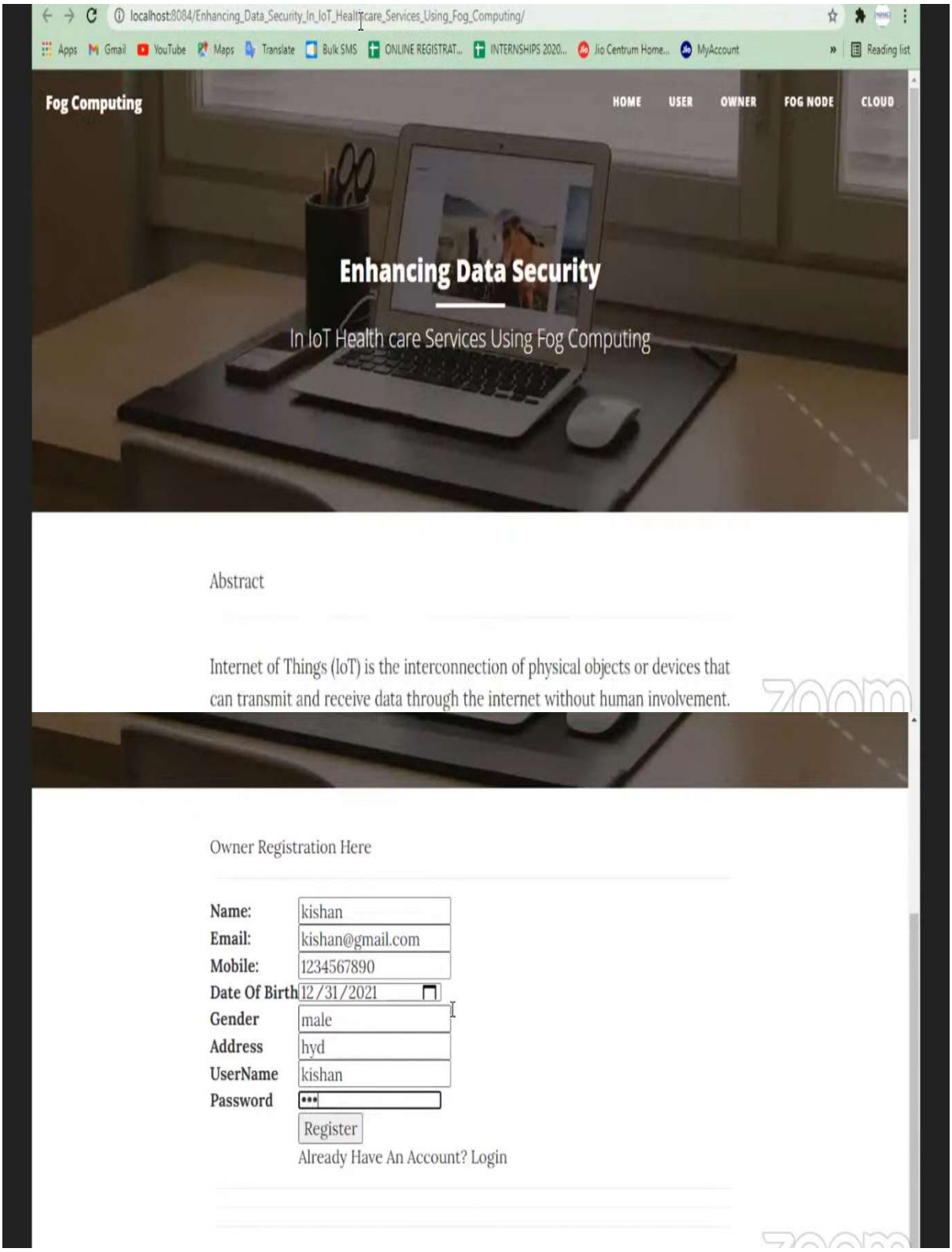




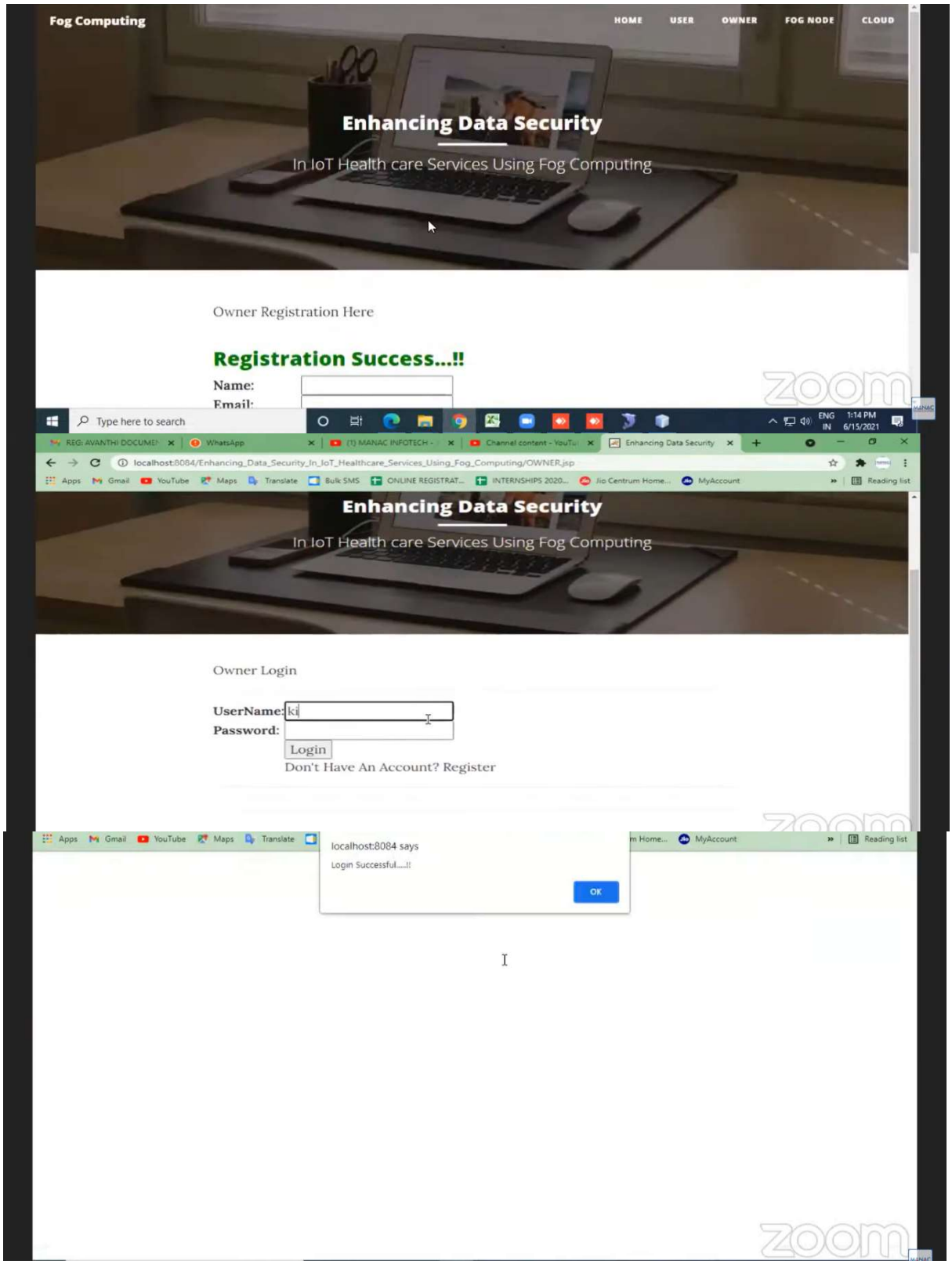
ISSN: 2278-4632
Vol-14, Issue-5, May: 2024



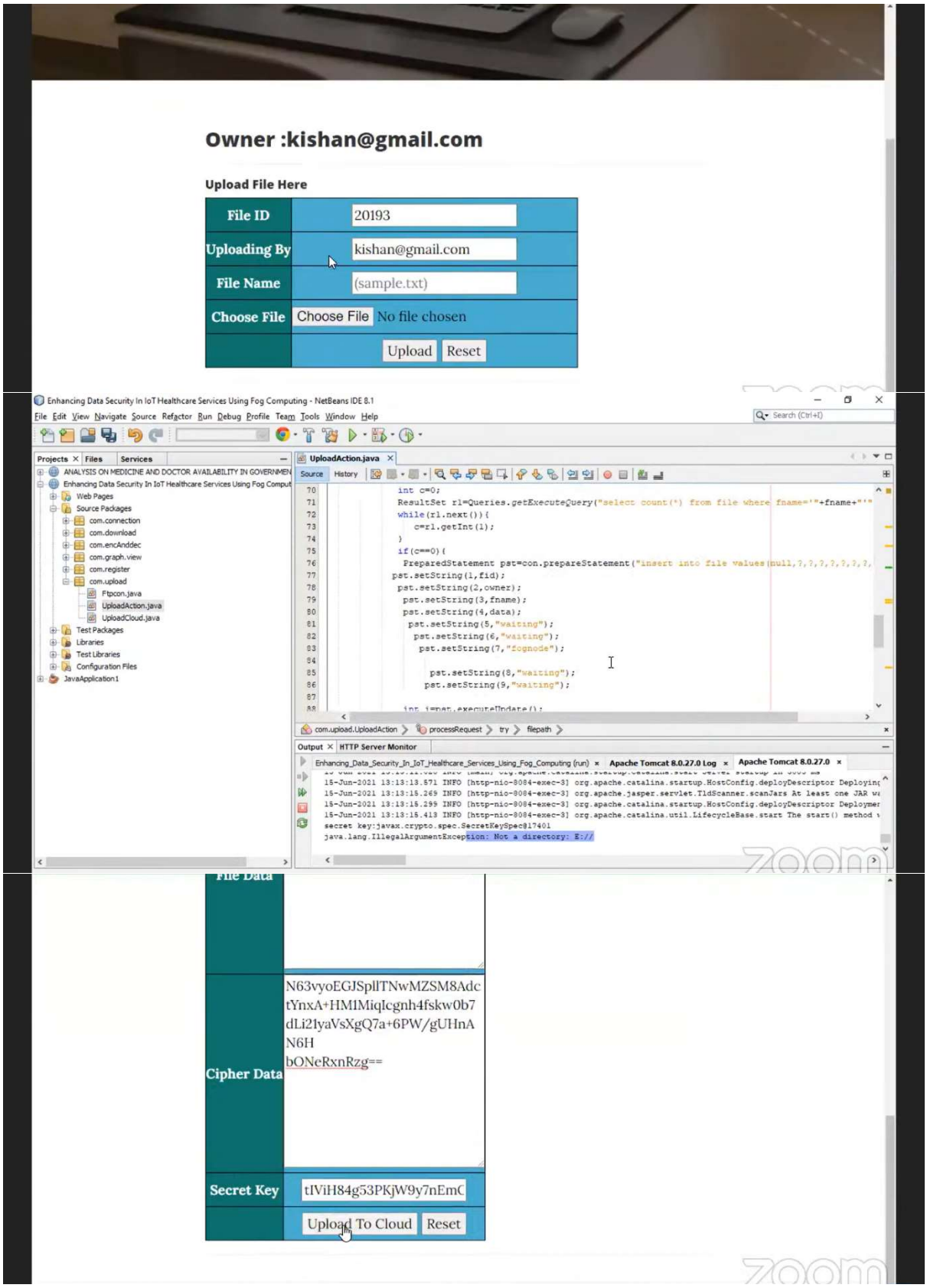
ISSN: 2278-4632
Vol-14, Issue-5, May: 2024



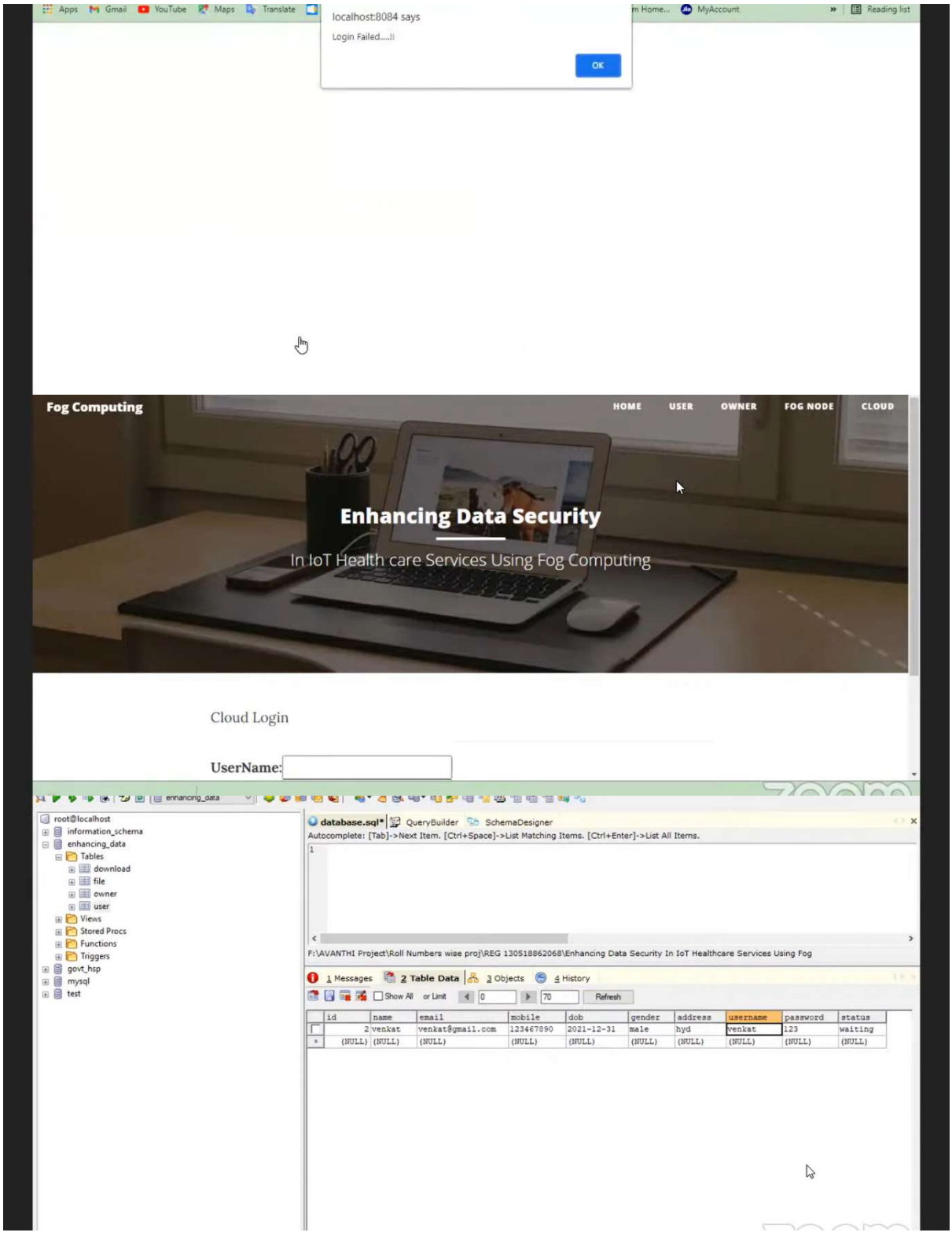
ISSN: 2278-4632
Vol-14, Issue-5, May: 2024



ISSN: 2278-4632
Vol-14, Issue-5, May: 2024



ISSN: 2278-4632
Vol-14, Issue-5, May: 2024



8.CONCLUSION

Fog computing architecture is able to overcome the security challenges of the traditional IoT cloud architecture to some extent. By introducing fog as a middle layer and performing at the edge side it enhances data security, accuracy, consistency, reduces the latency rate and enhances the overall quality of service. In the near future IoT-Fog-cloud architecture will be widely used as more and more IoT devices are developed and the increasing demand for fast computation. The implementation can be enhanced in future by developing a reliable real time data monitoring system application with the mentioned architecture as a core. And to give a computational prove of how much fog can enhance the traditional IoTCloud architecture.

9.FUTURE WORK

Fog computing architecture is able to overcome the security challenges of the traditional IoT cloud architecture to some extent. By introducing fog as a middle layer and performing at the edge side it enhances data security, accuracy, consistency, reduces the latency rate and enhances the overall quality of service. In the near future IoT-Fog-cloud architecture will be widely used as more and more IoT devices are developed and the increasing demand for fast computation. The implementation can be enhanced in future by developing a reliable real time data monitoring system application with the mentioned architecture as a core. And to give a computational prove of how much fog can enhance the traditional IoTCloud architecture.

10. REFERENCES

1. Kraemer, Frank Alexander, Anders Eivind Braten, NattachartTamkittikhun, and David Palma. "Fog Computing in Healthcare–A Review and Discussion." IEEE Access 5 (2017): 9206-9222.

2. Khan, Saad, Simon Parkinson, and Yongrui Qin. "Fog computing security: a review of current applications and security solutions." Journal of Cloud Computing 6, no. 1 (2017): 19.

3. Fog Computing Architecture, https://www.slideshare.net/saisharansai/fogcomputing-46604121, July 2018.

4. Al Hamid, Hadeal Abdulaziz, Sk Md Mizanur Rahman, M. Shamim Hossain, Ahmad Almogren, and Atif Alamri. "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): 22313-22328. 5. Alrawais, Arwa, Abdulrahman Alhothaily, Chunqiang Hu, and Xiuzhen Cheng. "Fog computing for the internet of things: Security and privacy issues." IEEE Internet Computing 21, no. 2 (2017): 34-42.

6. Elminaam, Diaa Salama Abdul, Hatem Mohamed Abdul Kader, and Mohie Mohamed Hadhoud. "Performance evaluation of symmetric encryption algorithms." IJCSNS International Journal of Computer Science and Network Security 8, no. 12 (2008): 280-286.

7. Coppersmith, Don, Donald Byron Johnson, and Stephen M. Matyas. "A proposed mode for triple-DES encryption." IBM Journal of Research and Development 40, no. 2 (1996): 253-262.

8. Gia, Tuan Nguyen, Mingzhe Jiang, AmirMohammad Rahmani, Tomi Westerlund, Pasi Liljeberg, and Hannu Tenhunen. "Fog computing in healthcare internet of things: A case study on ecg feature extraction." In Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on, pp. 356-363. IEEE, 2015.

9. Mukherjee, Mithun, Rakesh Matam, Lei Shu, Leandros Maglaras, Mohamed Amine Ferrag, Nikumani Choudhury, and Vikas Kumar. "Security and privacy in fog computing: Challenges." IEEE Access 5 (2017): 19293- 19304.

10. Shrestha, N. M., Abeer Alsadoon, P. W. C. Prasad, L. Hourany, and A. Elchouemi. "Enhanced e-health framework for security and privacy in healthcare system." In Digital Information Processing and Communications (ICDIPC), 2016 Sixth International Conference on, pp. 75-79. IEEE, 2016.
11. Wang, Qixu, Dajiang Chen, Ning Zhang, Zhe Ding, and Zhiguang Qin. "PCP: A PrivacyPreserving Content-Based Publish–Subscribe Scheme With Differential Privacy in Fog Computing." IEEE Access 5 (2017): 17962- 17974.
12. Wanve, Balu, Rahul Kamble, Sachin Patil, and Jayshree Katti. "Framework for client side AES encryption technique in cloud computing." In Advance Computing Conference (IACC), 2015 IEEE International, pp. 525-528. IEEE, 2015.
13. Vishwanath, Akhilesh, Ramya Peruri, and Jing (Selena) He. Security in fog computing through encryption. DigitalCommons@ Kennesaw State University, 2016.
14. Sadikin, Mohamad Ali, and Rini Wisnu Wardhani. "Implementation of RSA 2048-bit and AES 256-bit with digital signature for secure electronic health record application." In Intelligent Technology and Its Applications (ISITIA), 2016 International Seminar on, pp. 387-392. IEEE, 2016.
15. Shao, Fei, Zinan Chang, and Yi Zhang. "AES encryption algorithm based on the high performance computing of GPU." In Communication Software and Networks, 2010. ICCSN'10. Second International Conference on, pp. 588-590. IEEE, 2010.
16. Shao, Fei, Zinan Chang, and Yi Zhang. "AES encryption algorithm based on the high performance computing of GPU." In Communication Software and Networks, 2010. ICCSN'10. Second International Conference on, pp. 588-590. IEEE, 2010.
17. Umamaheswari E, Ajay DM, Umang Sindal, Scope of Internet of Things: A Survey, Asian Journal of Pharmaceutical and Clinical Research, April 2017
18. D M Ajay, Umamaheswari.E, an initiation for testing the security of a cloud service provider. Smart Innovation, Systems, Technologies. Switzerland: Springer Publications; 2016. p. 35- 41.
19. D M Ajay, Umamaheswari.E, Why, how cloud computing- How not and cloud security issues. Global Journal of Pure and Applied Mathematics (GJPAM) 2016;12(1):1-8 20. D M Ajay, Umamaheswari E, Evaluating the Efficiency of Security Mechanisms in Cloud Environments, International Journal of Control Theory and Applications, Vol. 9, No.51, 2016

