IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 11, Issue 6, November-December 2024

Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106039

Obtain Patient Health Data Priority Classification in a Remote E-Healthcare System while Maintaining Privacy

Mr.G.Lakpathi[1], Mr.B.Venkata Abhinav[2], Ms. D.Sai Kalpana[3], Ms.D.Srilatha[4]

Assistant Professor, Department of Computer Science & Engineering, Guru Nanak Institute of Technology, Telangana, India[1]

Student, Department of Computer Science & Engineering, Guru Nanak Institute of Technology, Telangana, India[2,3,4]

ABSTRACT: The Wireless Body Area Network (WBAN) has attracted considerable attention and become a promising approach to provide a 24-hour on-the-go healthcare service for users. However, it still faces many challenges on privacy of users' sensitive personal information, confidentiality of healthcare center's disease models. For this reason, many privacy-preserving schemes have been proposed in recent years. However, the efficiency and accuracy of those privacy-preserving schemes become a big issue to be solved. In this paper, we propose an efficient and privacy-preserving priority classification scheme, named PPC, for classifying patients' encrypted data at the WBAN-gateway in a remote eHealthcare system. Specifically, to reduce the system latency, we design a non-interactive privacy-preserving priority classification algorithm, which allows the WBAN-gateway to conduct the privacy-preserving priority classification for the received users' medical packets by itself and relay these packets according to their priorities (criticalities). Detailed security analysis shows that the PPC scheme can achieve the priority classification and packets relay without disclosing the privacy of the users' personal information and confidentiality of the healthcare center's disease models. In addition, the extensive experiments with an android app and two java server programs demonstrate its efficiency in terms of computational costs and communication overheads.

I. INTRODUCTION

Remote eHealthcare systems using WBANs and smartphones enable efficient physiological data collection and transmission. Sensors send raw data to smartphones for preprocessing, which is then forwarded to WBAN-gateways and healthcare centers. However, sharing sensitive data like medical history and healthcare centers' disease models raises privacy concerns. Attackers may exploit smartphones or gateways to steal data or intellectual property, necessitating privacy-preserving measures.

Key challenges include ensuring security through robust encryption resistant to ciphertext-only and known-plaintext attacks. Accuracy is critical, as standardization and randomization methods (e.g., differential privacy) can compromise medical outcomes. Efficiency remains an issue, with computationally intensive techniques like homomorphic encryption causing delays. Effective solutions must balance privacy, accuracy, and efficiency for reliable remote eHealthcare systems.

II. LITERATURE SURVEY

C. A. Otto et. al(2006)This paper describes a prototype system for continual health monitoring at home. The system consists of an unobtrusive wireless body area network (WBAN) and a home health server. The WBAN sensors monitor user's heart rate and locomotive activity and periodically upload time-stamped information to the home server. The home server may integrate this information into a local database for user's inspection or it may forward the information further to a medical server. The prototype may be used for ambulatory monitoring of patients undergoing cardiac rehabilitation or for monitoring of elderly at home by informal caregivers.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106039

I. Goienetxea(2016)We investigated different encryption algorithms for sport wearable devices by utilizing a newly developed data generator for the testing purposes. Additionally we investigated different data encryption algorithms for a NoSQL DBMS. Testing results for data generator, data encryption and NoSQL database stress testing are presented and discussed as well. The research project was conducted in support of NSERC grant "GAUGE: Exact Positioning Systems for Sport and Healthcare Industries".**:**

Z. Chen(2017)Wearable devices such as smart watch and bracelets continually broadcast Bluetooth Low Energy (BLE) signals, which can be easily captured by monitoring devices such as WiFi routers and Bluetooth scanners. As more and more wearable devices emerge, unauthorized monitoring and tracking by adversary becomes great privacy threats not only in the cyberworld, but also in the physical world. To protect location privacy, this paper presents a real-life location monitoring system that is based on BLE privacy feature that changes the device physical address periodically. To enable users to better control their privacy level while still providing monitoring and tracking service to authorized parties (e.g., for child and elderly care), we extend BLE privacy by enriching its privacy semantics with a comprehensive set of metrics, such as simple opt-in/out, k-anonymity, and granularity-based anonymity. The system has been implemented and evaluated in terms of accuracy and user study.

S. Rezvani and S. A. Ghorashi.(2013)Integration of miniature sensors composes a wireless body area network (WBAN), which enables remote health monitoring. To make this technology widely acceptable in the society, some studies suggest commonly used gadgets such as cell phones or laptops as a hub for WBANs. In these cases, envisaged medical and non-medical applications of WBANs must have the same priority unless in emergency situations. Also, medical applications of WBANs need some strict requirements that are not that important for non-medical applications, such as very low-power consumption or reliability. In addition, channel condition may change in WBANs because of fading effects and this causes packet loss. Therefore proper traffic prioritization, high reliability and efficient channel utilization are vitally important issues in these networks. In this study, the authors improve the performance of the medium access control (MAC) protocol of WBANs using an adaptive resource allocation and traffic prioritization according to the medical situation of user and channel condition. Through adaptively separating and managing the possible traffics of WBANs, the heterogeneous requirements of different applications are provided. Analytical and simulation results show that the proposed MAC protocol outperforms IEEE 802.15.4 and IEEE 802.15.6 MAC protocols in terms of power consumption as well as the channel utilization and reliability.

III. METHODOLOGIES

Modules Name
1. User
2. Data Collect
3. Classify Relay

Modules Explanation
1. **User:**This module provides secure login and registration, requiring a username, password, and email for server access. Registered users can manage upload/download activities via the server.
2. **Data Collect**:In this module, Data Users register/login, search files by name, and download encrypted files. Users send trapdoor requests to the server, get owner permission, and download files in plain text.
3. **Classify Relay**:This is the Second module of this project. In this module Data Owner should register and Login. Data Owner will Uploads the files into the database. Data owner can also send request to the data user.

Existing System Disadvantages
- **Privacy Concerns**: Risk of exposing sensitive personal data.
- **Confidentiality Issues**: Protection of healthcare models remains challenging.
- **Efficiency**: Existing schemes may be slow or resource-intensive.
- **Accuracy**: Trade-offs in preserving privacy can impact system accuracy.

Proposed System
This paper proposes the PPC scheme for efficient, privacy-preserving priority classification of encrypted patient data in WBAN. A non-interactive algorithm enables the WBAN-gateway to classify and relay medical packets based on criticality without compromising user privacy or healthcare model confidentiality. Security analysis ensures privacy preservation, and experiments show its computational and communication efficiency.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

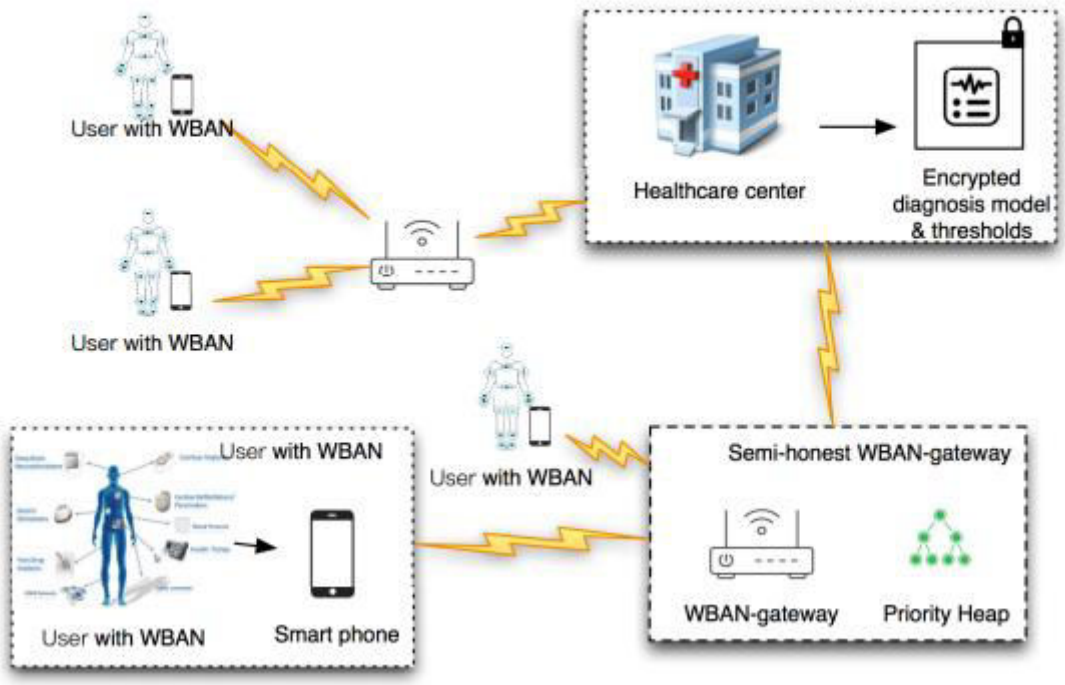
|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106039

Proposed System Advantages

- Efficiency: Reduces system latency with a non-interactive algorithm.
- Privacy Preservation: Protects user data and healthcare model confidentiality.
- Priority Handling: Classifies and relays medical packets based on criticality.
- Scalability: Demonstrates low computational costs and communication overhead.
- Security: Ensures robust privacy through detailed analysis.

System Architecture



Explanation

In this project data owner has a register all details and then login. Data owner can be an upload a document. Data owner can have a send request to the data user. Data user can search a query with uploaded document. The file has also a download it will show an encryption format. Data user also a send a request to the cloud server. Cloud server can a login. It will accept a key approve. Cloud server can also see all the data information's. Cloud server can also see all the user information. Cloud server can see all the stored information. Cloud server can approve a key request from the user. Then data owner has get the request data owner can send a secret key to the user. Then user can also download a file. If the user has given wrong keys it gets warning the user has a block permanently. The file it gets an attacks.

Implementation

The implementation of this project begins with **Data Collection**, where physiological data is gathered using wearable devices integrated into a Wireless Body Area Network (WBAN). Data such as heart rate and body temperature is transmitted securely to a smartphone via Bluetooth or Zigbee. The smartphone preprocesses the raw data and encrypts it using algorithms like AES or RSA to ensure privacy. The encrypted data is then sent to the WBAN gateway for further processing.In the **Dataset** module, the encrypted data is stored in a secure relational database, such as MySQL. The database is structured to accommodate user profiles, encrypted physiological data, and metadata. APIs are developed to facilitate secure access to the data, ensuring proper authentication and data integrity.The **Data Preparation** phase involves cleaning and organizing the data for analysis. Tools like Python's Pandas and NumPy are used to normalize data, handle missing values, and remove outliers. Feature selection techniques identify critical attributes like blood pressure or heart rate for classification, optimizing the dataset for machine learning models.During the **Model Selection** stage, machine learning algorithms such as Decision Trees, Random Forests, or Logistic Regression are trained using libraries like TensorFlow, PyTorch, or scikit-learn. Models are evaluated based on

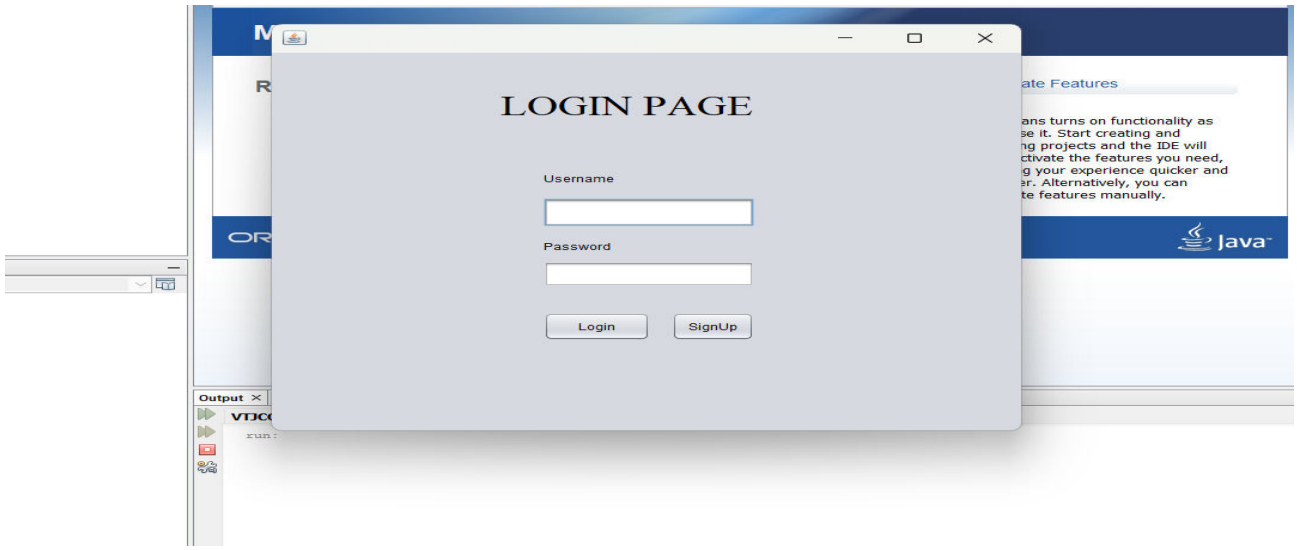
| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

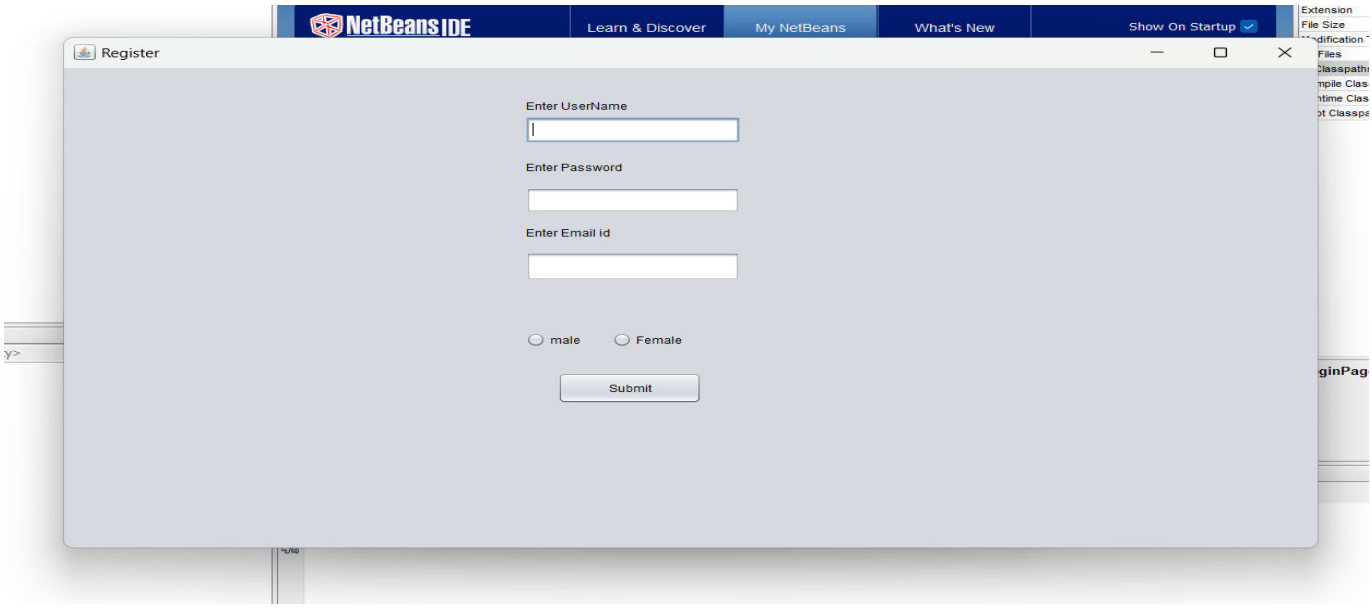
DOI:10.15680/IJARETY.2024.1106039

accuracy, precision, recall, and F1-score, and the best-performing model is saved for deployment using tools like joblib or pickle.In the **Analyze and Prediction** module, the trained model is used to classify encrypted medical data into priority levels. A priority queue algorithm ensures that high-criticality data is relayed to healthcare centers with minimal latency. The classification and relaying logic is integrated into a server-side framework like Flask or Django, with results displayed on a user interface such as an Android app or web application.Finally, in the **Accuracy Testing and Model Saving** module, the model is validated using test datasets and fine-tuned through hyperparameter optimization techniques like grid or random search. The validated model is stored securely in a cloud environment or local server for future predictions. Deployment involves setting up a backend using J2EE or Python, a database for secure data storage, and a user-friendly frontend for interaction.This comprehensive implementation ensures a secure, efficient, and privacy-preserving system for managing and prioritizing healthcare data.

Experimental Results



Login Page



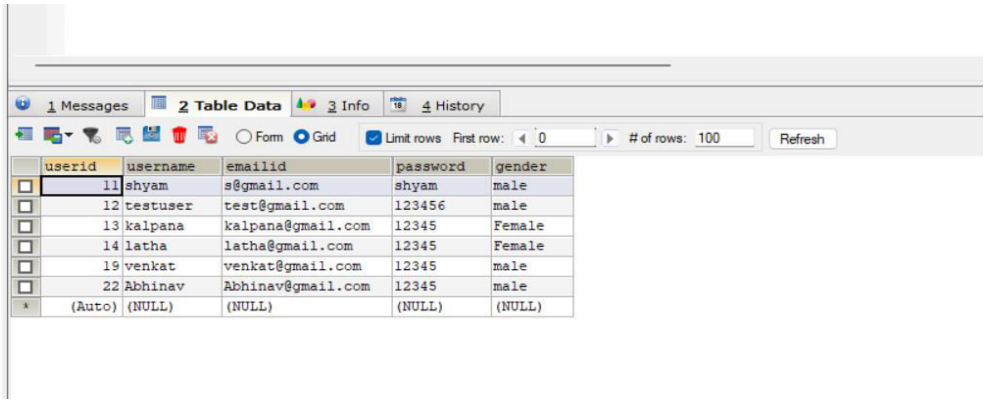
Registration Page

International Journal of Advanced Research in Education and TechnologY(IJARETY)

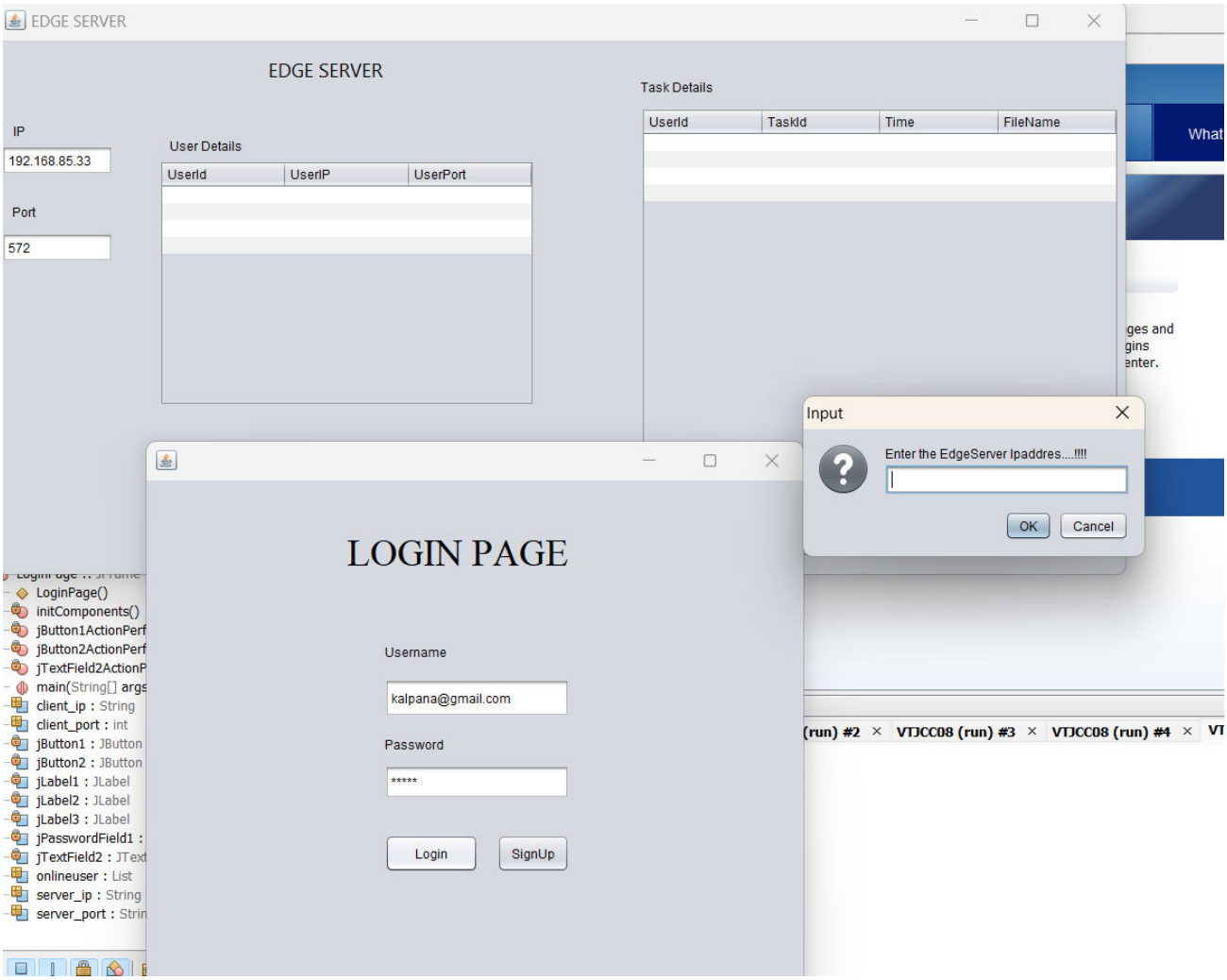
| ISSN: 2394-2975 | www.ijarety.in | | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106039



Data stored in database



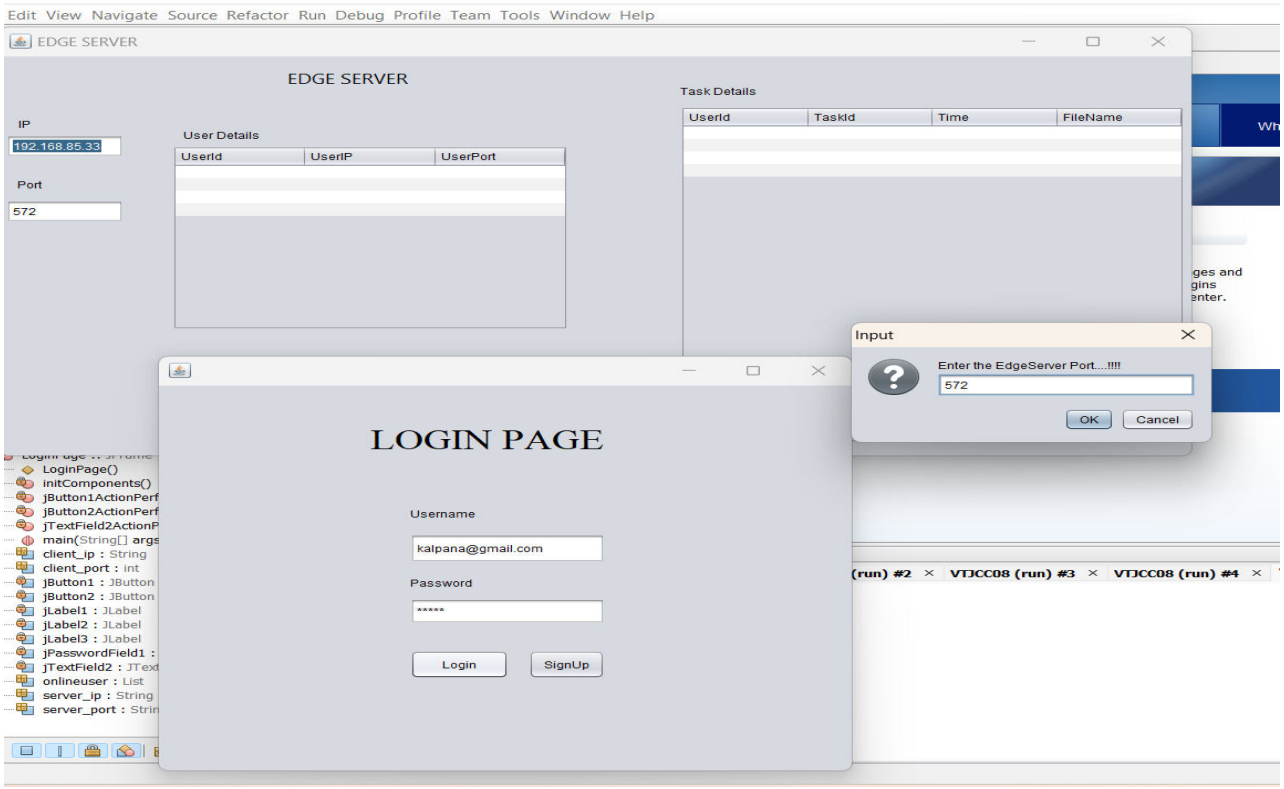
Entering IP Address

International Journal of Advanced Research in Education and TechnologY(IJARETY)

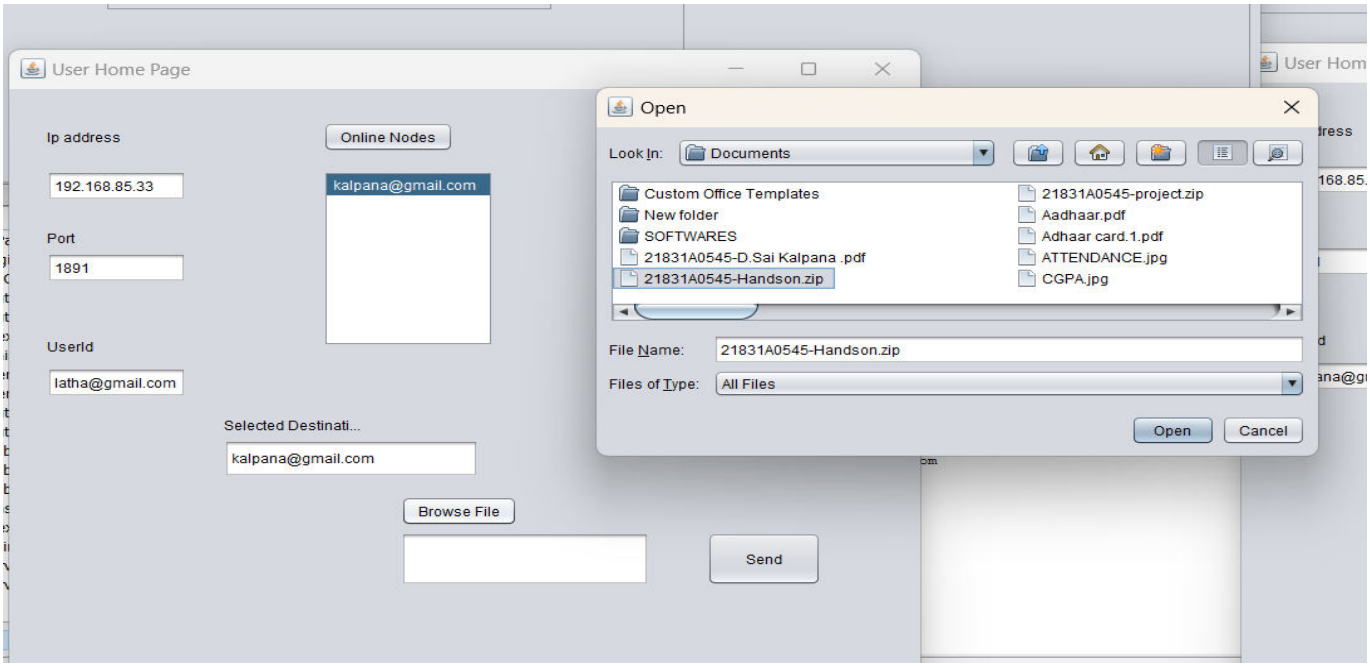
| ISSN: 2394-2975 | www.ijarety.in | | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106039



Entering Port Number



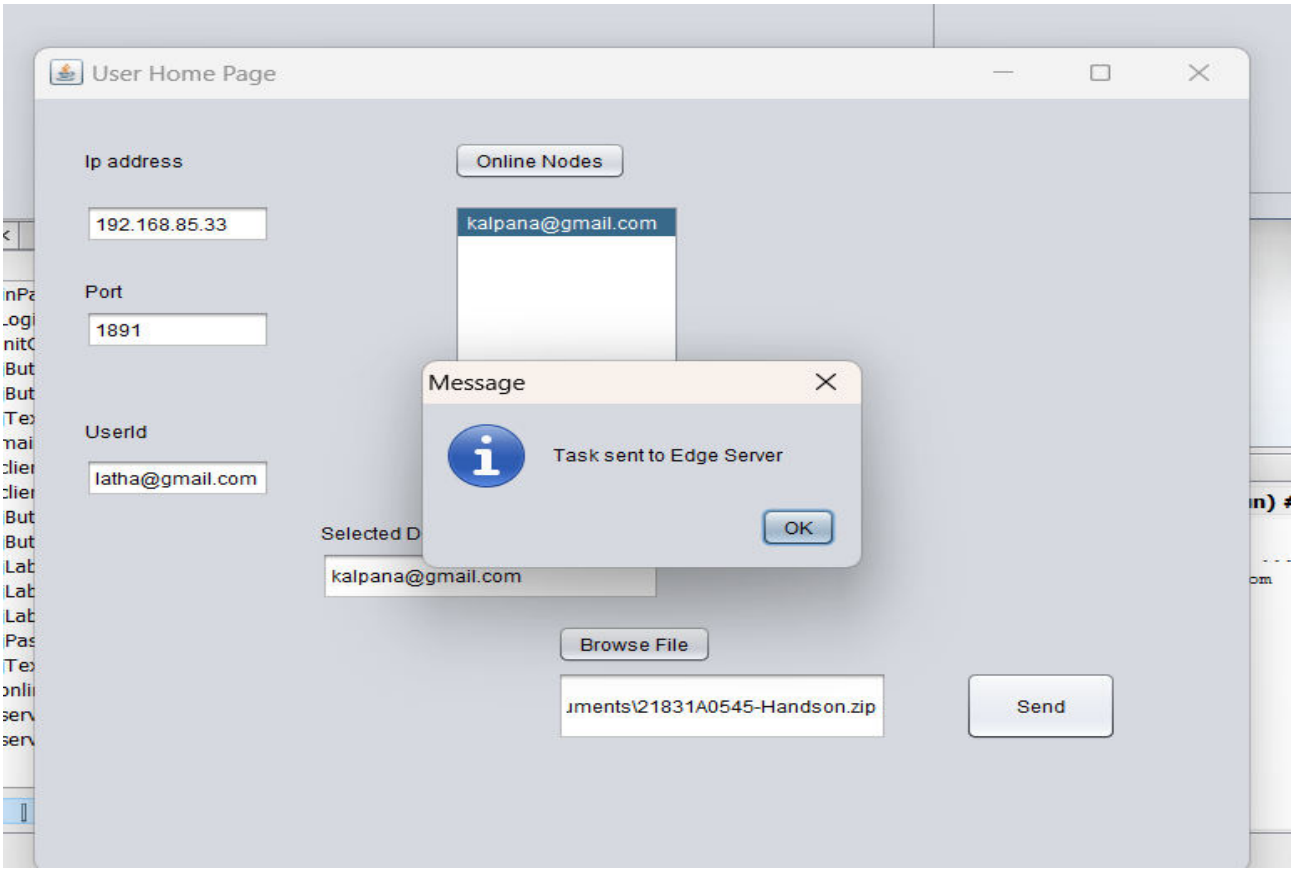
Uploading Data Into Nearby Edge Server

International Journal of Advanced Research in Education and TechnologY(IJARETY)

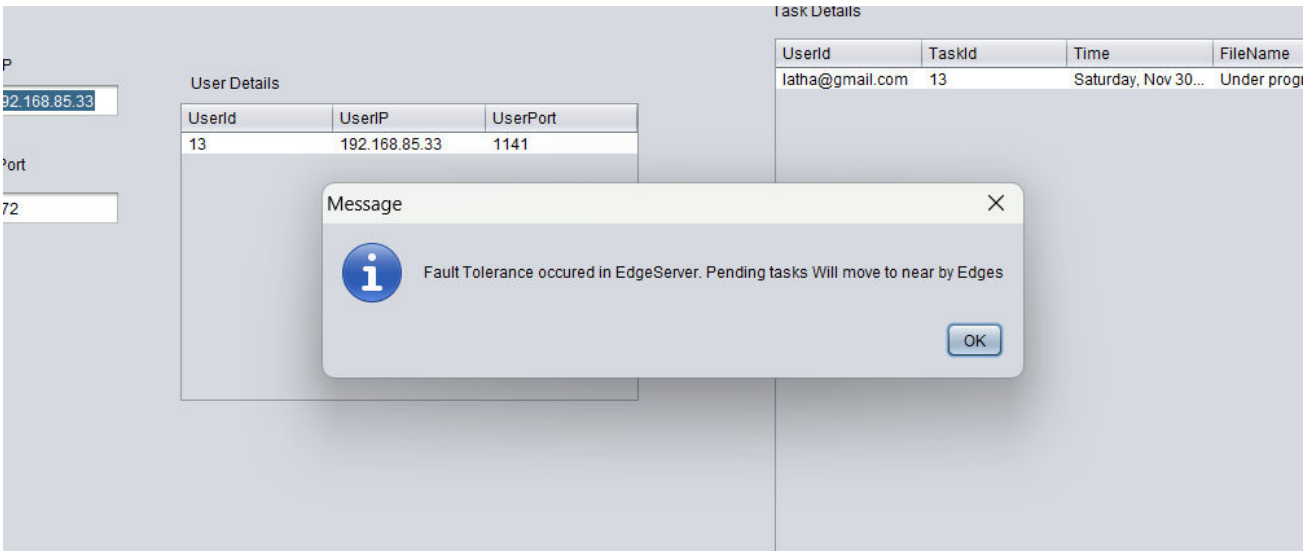
| ISSN: 2394-2975 | www.ijarety.in | | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106039



Data Stored In Nearby Edge Server Successfully



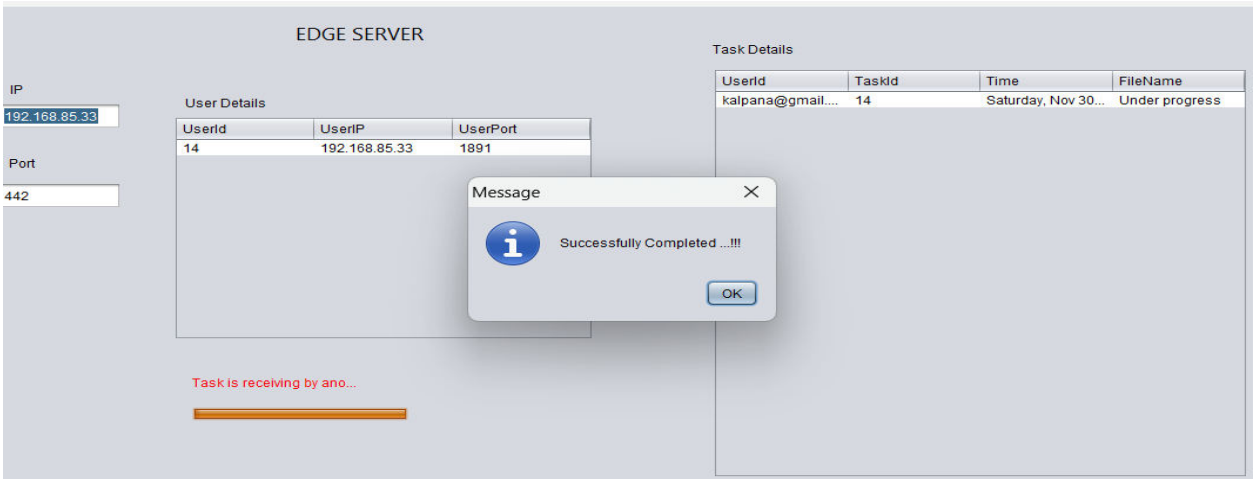
Fault Tolerance Occurred In Edge Server

International Journal of Advanced Research in Education and TechnologY(IJARETY)

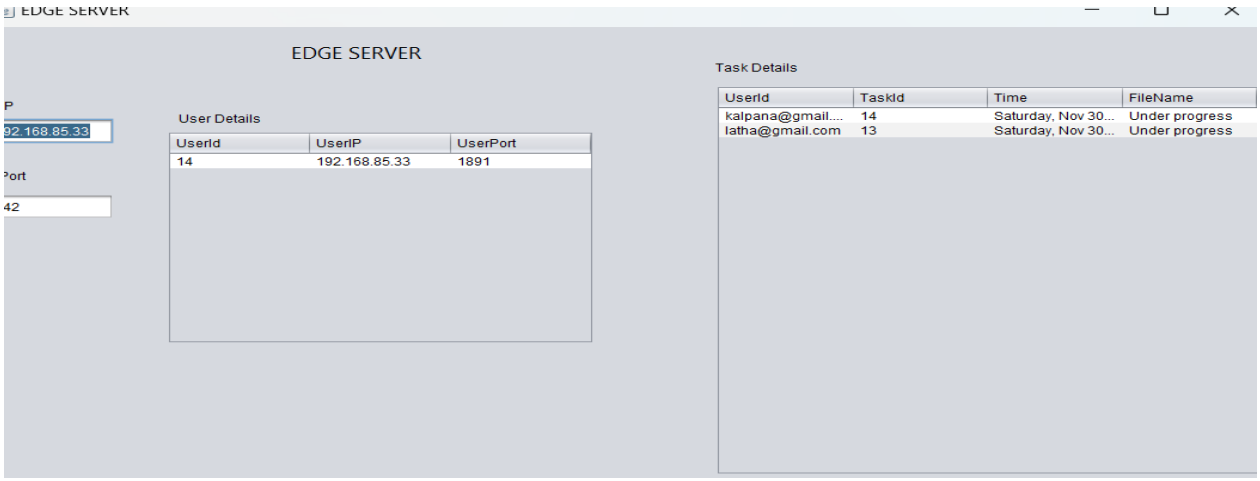
| ISSN: 2394-2975 | www.ijarety.in | | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106039



Data Sent to Nearby Edge Server Securely



Data Stored In edge Server

IV. CONCLUSION

This project, we have proposed an efficient privacy preserving priority classification(PPC) scheme on patient healthcare data in remote E-Healthcare system. The proposed PPC scheme achieves the priority classification and packets relay tasks, while preserving the privacy of the users and the confidentiality of the health care center's disease models. Because it is an on-interactive procedure, the communication cost is low. We have also implemented an android app and two java programs to demonstrate that our PPC scheme is efficient in computational cost and communication overhead

V. FUTURE ENHANCEMENT

Future work on the PPC scheme includes integrating advanced techniques like federated learning for better accuracy and real-time processing for critical scenarios. Scaling with edge computing, IoT integration, and blockchain ensures adaptability, security, and continuous monitoring. Personalized healthcare recommendations and compliance with regulations (e.g., GDPR, HIPAA) aim for universal applicability. Cross-platform access and optimized protocols enhance usability and efficiency.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106039

REFERENCES

1. K. Bilal, S. U. Khan, L. Zhang, H. Li, K. Hayat, S. A. Madani, N. Min-Allah, L. Wang, D. Chen, M. Iqbal, C. Z. Xu, and A. Y. Zomaya, "Quantitative comparisons of the state of the art data center architectures," Concurrency and Computation: Practice and Experience, Vol. 25, No. 12, 2013, pp. 1771-1783.
2. K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Zomaya, "On the characterization of the structural robustness of data center networks," IEEE Transactions on Cloud Computing, Vol. 1, No. 1, 2013, pp. 64-77.
3. D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, "Energy-efficient data replication in cloud computing datacenters," In IEEE Globecom Workshops, 2013, pp. 446-451.
4. Y. Deswarte, L. Blain, and J-C. Fabre, "Intrusion tolerance in distributed computing systems," In Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy, Oakland CA, pp. 110-121, 1991.
5. B. Grobauer, T.Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," IEEE Security and Privacy, Vol. 9, No. 2, 2011, pp. 50-57.
6. W. K. Hale, "Frequency assignment: Theory and applications," Proceedings of the IEEE, Vol. 68, No. 12, 1980, pp. 1497-1514.
7. K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, Vol. 4, No. 1, 2013, pp. 1-13.
8. M. Hogan, F. Liu, A.Sokol, and J. Tong, "NIST cloud computing standards roadmap," NIST Special Publication, July 2011.
9. W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," In 44th Hawaii IEEE International Conference onSystem Sciences (HICSS), 2011, pp. 1-10.
10. A. Juels and A. Opera, "New approaches to security and availability for cloud data," Communications of the ACM, Vol. 56, No. 2, 2013, pp. 64-73.
11. G. Kappes, A. Hatzieleftheriou, and S. V. Anastasiadis, "Dike: Virtualization-aware Access Control for Multitenant Filesystems," University of Ioannina, Greece, Technical Report No. DCS2013-1, 2013.
12. L. M. Kaufman, "Data security in the world of cloud computing," IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.
13. S. U. Khan, and I. Ahmad, "Comparison and analysis of ten static heuristics-based Internet data replication techniques," Journal of Parallel and Distributed Computing, Vol. 68, No. 2, 2008, pp. 113-136. [14] A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, "Towards
14. Secure Mobile Cloud Computing: A Survey," Future Generation Computer Systems, Vol. 29, No. 5, 2013, pp. 1278-1299.
15. A. N. Khan, M.L. M. Kiah, S. A. Madani, and M. Ali, "Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing, The Journal of Supercomputing, Vol. 66, No. 3, 2013, pp. 1687-1706 .
16. T. Loukopoulos and I. Ahmad, "Static and adaptive distributed data replication using genetic algorithms," Journal of Parallel and Distributed Computing, Vol. 64, No. 11, 2004, pp. 1270-1285.
17. A. Mei, L. V. Mancini, and S. Jajodia, "Secure dynamic fragment and replica allocation in large-scale distributed file systems," IEEE Transactions on Parallel and Distributed Systems, Vol. 14, No. 9, 2003, pp. 885-896.
18. L. Qiu, V. N. Padmanabhan, and G. M. Voelker, "On the placement of web server replicas," In Proceedings of INFOCOM 2001, Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 3, pp. 1587-1596, 2001.
19. D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing environments," Procedia Engineering, Vol. 15, 2011, pp. 2852 2856.
20. Y. Tang, P. P. Lee, J. C. S. Lui, and R. Perlman, "Secure overlay cloud storage with access control and assured deletion," IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 6, Nov. 2012, pp. 903-916.
21. M. Tu, P. Li, Q. Ma, I-L. Yen, and F. B. Bastani, "On the optimal placement of secure data objects over Internet," In Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium, pp. 14-14, 2005.
22. D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, Vol. 28, No. 3, 2012, pp. 583-592.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com