Journal of Cardiovascular Disease Research

ISSN: 0975-3583, 0976-2833 VOL14, ISSUE 10, 2023

Efficient Privacy-Preserving Medical Diagnosis on Edge Computing Platforms

Subba Reddy Borra[1], B Gayathri[2], B Rekha[2], B Akshitha[2], B. Hafeeza[2]

[1]Professor and Head, Department of Information Technology, Mallareddy Engineering College for Women, (UGC-Autonomous), Hyderabad, India, bvsr79@gmail.com.

[2]Student, Department of Information Technology, Mallareddy Engineering College for Women, (UGC-Autonomous), Hyderabad, India.

Abstract

Edge computing has emerged as a potential solution to some of the challenges in healthcare. It involves processing data closer to the source, such as medical devices and sensors, rather than relying solely on centralized data centers or cloud computing. This approach offers advantages like reduced latency, real-time decision-making, and enhanced privacy protection. Efficient privacy-preserving medical diagnosis on edge computing platforms is a concept deeply rooted in the intersection of healthcare and technology. Over the years, medical diagnosis has increasingly relied on machine learning algorithms to analyze vast amounts of patient data. These algorithms can predict diseases, identify anomalies in medical images, and offer personalized treatment recommendations. However, a significant challenge in this domain is the protection of patient data privacy. Healthcare data is incredibly sensitive, and data breaches or unauthorized access can result in severe consequences, including identity theft and discrimination. Therefore, this research work tackles several key issues. First and foremost, it aims to ensure the privacy of medical data throughout the diagnosis process. This means developing machine learning models and algorithms that can make accurate predictions while safeguarding the sensitive information contained in patient records. Additionally, these models must be highly efficient to operate effectively within the resource-constrained environment of edge computing platforms. Further, real-time processing is a critical requirement in healthcare, especially for conditions that demand immediate attention. Hence, this work strives to provide timely results to healthcare providers. Furthermore, the models must maintain a high level of accuracy and reliability to instil trust in the medical community and ensure that patients receive the best possible care. Ultimately, this research aligns with the goal of patient-centric care. It empowers patients to have more control over their data, share it securely with healthcare providers, and receive real-time decision support, all while preserving their privacy and the integrity of their medical information.

1. Introduction

The Internet of Things (IoT)-based applications and services include sensor networks, healthcare systems, transportation, smart industry, communication systems, smart cities, and manufacturing [1]. The Industrial Internet of Things (IIoT) has been proposed to dramatically enhance qualities of traditional industries, break regional limitations to achieve remote monitoring, perform autonomous production, and provide real-time information to users [2,3,4]. The Internet of Thing (IoT) will deliver about 85% of all IoT devices in healthcare by 2025 [1]. According to Tractia, an intelligent organization, annual earnings in this sector using blockchain technologies would reach USD 9 billion by 2025 [2]. IoT devices are widely used in healthcare to give real-time services to patients and physicians [3]. IoMT-based medical device applications include medical institutions and businesses. However, as the number of internet-connected medical devices (IoMT) increases, greater volumes and inconsistency of data will be generated. With centralized cloud-based characteristics, handling significant data traffic in IoT (IoMT) has now become a severe problem and reason for concern [4]. As a result, patient safety and confidentiality concerns have grown while data collection, data ownership, location privacy, etc., will be at risk. By copying data and changing the identification of healthcare equipment, intruders and hackers can easily target the 5G-enabled IoMT network. IoMT-Cloud currently has a single point of failure, malicious attacks, and privacy leaks, as shown in Figure 1. To ensure network security and secure PHR transmission, data transfer between IoMT and Cloud requires trust, device identification, and user authentication (UA). With the traditional Central Cloud service, however, due to the round-the-clock networking of nodes in this IoT network, it is vulnerable to various security issues, such as message tampering, eavesdropping, and denial-of-service

ISSN: 0975-3583, 0976-2833 VOL14, ISSUE 10, 2023

attacks [5]. In the industrial industry, this raises major security issues as the misuse of data can result in the incorrect diagnosis and can cause life-threatening scenarios for the patients under observation [6,7].

The edge computing based IoMT is currently a popular topic. Previous research missed important security issues such as: 1. Healthcare IoMT devices send data to cloud servers that are frequently unencrypted and open to manipulation and attack. As a result, sensitive patient information will likely be accessible. This issue leads to security vulnerabilities. 2. To our knowledge, the need to identify IoMT medical devices, which leads to the verification and authentication of health data, is considered very important and sensitive, and it can be accomplished quickly using a blockchain in the FC-IoMT system. Moreover, servers at the network's edge should perform more detailed authentication and verification. BAKMP-IoMT, the new IoMT key agreement technique for blockchain-accessible authentication, was designed by [8]. It is also obtained theoretically from the algorithm's top time complexity and the number of patients.

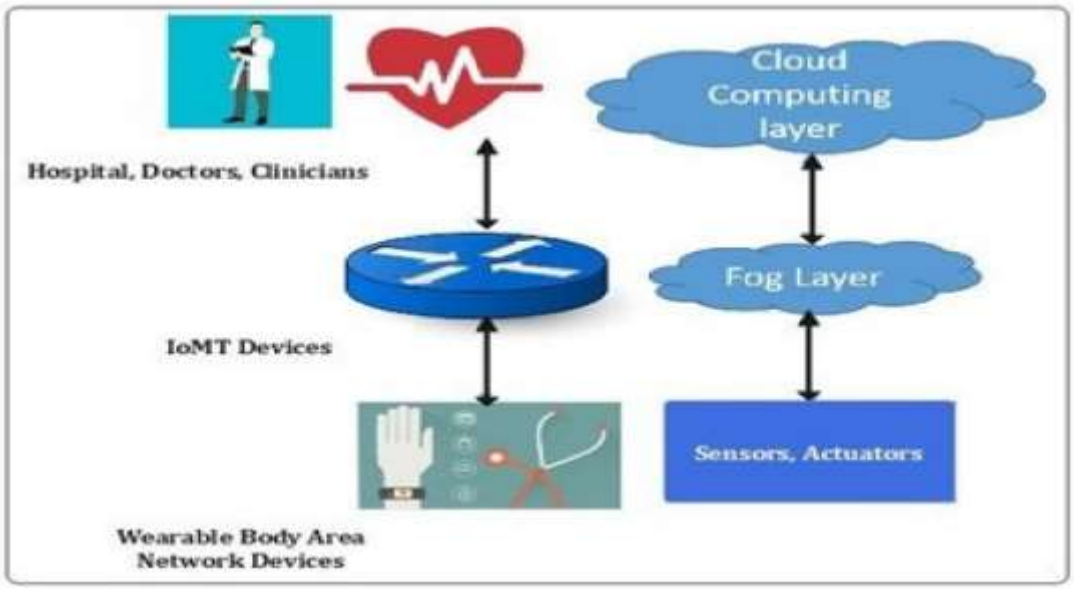


Figure 1. Application of edge computing.

2. Literature Survey

Researcher in a study [9] explored various design research topics on readers' 5G-enabled tactile internet edge computing. In the same way [10] thoroughly examined 5G-assisted smart health of 14 care solutions in the IoT. R. Researchers in a study [11] proposed a multi-cloud cascade architecture, a low-overhead native testing framework, and a medical data storage backup method. This is also something that is examined by researchers [12] proposed a smart authentication (SSA) system to improve patient–physician data security and privacy preservation systems. Ref. [13] designed a node security identity authentication, providing a secure and reliable updating method for authentication keys and session keys. Ref. [14] proposed smart remote healthcare systems that require long working periods, low cost, network resilience, and confidence in highly dynamic network environments. Ref. [15] highlight the rising issues in IIoT information processing storage, querying, and dynamic data collecting. Researchers in a study [16] proposed a case database and the current patient's privacy was protected regardless of whether the abstracts matched or not. Ethereum is a permissionless blockchain that has been widely used by various blockchain enthusiasts. Ethereum follows the standard principles and elements of a blockchain network. Like a84blockchain, it uses the Proof of Work (PoW) consensus process to facilitate validation of blocks of the network by mining nodes before adding the blocks and their transactions into the blockchain. Ethereum can be utilized by connecting nodes to a blockchain with a unique chain-id. This allows all the nodes to participate within the blockchain activities and access blocks and/or transactions. Ethereum can also be implemented as a private blockchain for typical enterprise solutions that restrict access to their trusted assets and personnel [17].

A recent study conducted by Dorri et al. [18] reviewed the main challenges of edge computing and IOT. The study concluded the recent trends of IOT algorithms and the main challenges in edge computing, which works

ISSN: 0975-3583, 0976-2833 VOL14, ISSUE 10, 2023

as a middle layer between data centers in the cloud and IOT networks. Hang et al. [19] developed a new scheme that captures the most significant features of the DBMS environment, including relational, graph-based, key-value, tree-like, etc., query languages, platforms (servers), plus running environments (desktop, Web, cloud), and specific contexts—i.e., focusing on optimizing queries, redundancy, security, performance, as compared with other schema-less approaches, programming languages/paradigms, and others. Yu et al. [20] focused on Quality of Service (QoS) in IOT utilization. They performed an analysis review on QoS techniques developed in the literature for IoT applications and investigated current research trends. They found that the most popular QoS metrics are Network Usage, Throughput, Reliability, and Latency.

The classical distributed consensus mechanism is the consensus mechanism used in the traditional distributed network, which realizes the distributed consensus through the state machine replication between network nodes. Hameed et al. [21] proposed the Byzantine Generals Problem and studied how non-fault nodes reach agreement on specific data in the case of possible failure nodes or malicious attacks, which became the basis for the research on consensus mechanisms. Dwivedi et al. [22] proposed a Paxos algorithm to solve the Byzantine Generals Problem. This algorithm can tolerate the collapse of a certain number of nodes in the network, so as to reach an agreement on a specific value in the distributed system. Daraghmi et al. [23] proposed the Practical Byzantine Fault Tolerance (PBFT). As a solution to the Byzantine Generals Problem, PBFT could achieve the final consensus among honest nodes while the number of enemies was no more than 1/3 of the total number of nodes. Jung et al. [24] proposed a new common algorithm: Mixed Byzantine Fault Tolerance (MBFT). Functionally, MBFT partitions the nodes participating in the consensus process and improves scalability and efficiency without sacrificing security. MBFT also introduces a random node selection mechanism and a credit mechanism to improve security and fault tolerance. Esposito et al. [25] proposed a dynamic reputation practical Byzantine fault tolerance algorithm. The dynamic reputation practical Byzantine fault tolerant algorithm adopts the consensus election method based on credit. The monitoring node divides the remaining nodes into two types of nodes according to their reputation values: consensus nodes and auxiliary nodes, which participate in different stages of the block generation process, respectively, and dynamically update the consensus nodes with low reputation scores.

3. Proposed System Model

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. The goal is for UML to become a common language for creating models of object-oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML. The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems. The UML is a very important part of developing objects-oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

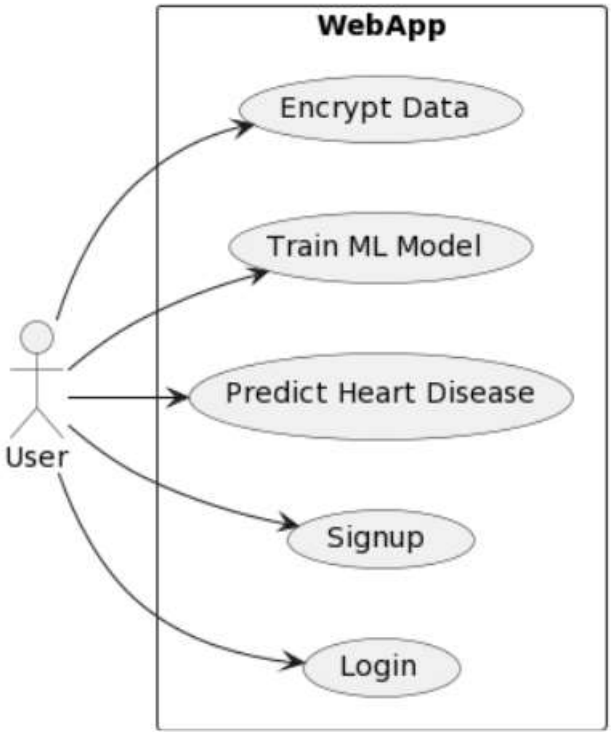
GOALS: The Primary goals in the design of the UML are as follows:

- Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
- Provide extendibility and specialization mechanisms to extend the core concepts.
- Be independent of particular programming languages and development process.
- Provide a formal basis for understanding the modeling language.
- Encourage the growth of OO tools market.
- Support higher level development concepts such as collaborations, frameworks, patterns and components.
- Integrate best practices.

ISSN: 0975-3583, 0976-2833 VOL14, ISSUE 10, 2023

Use Case Diagram

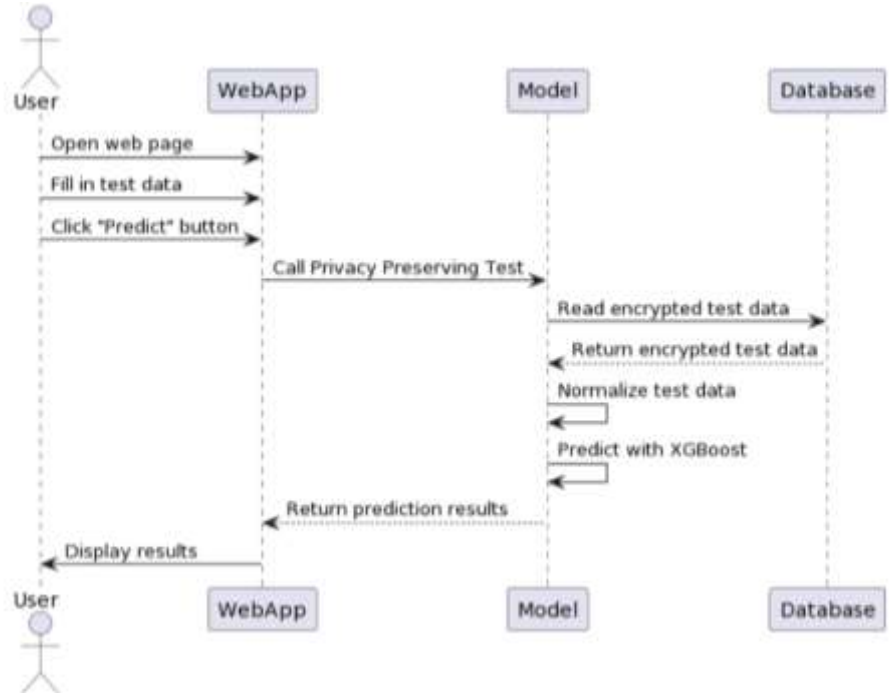
A use case diagram in the Unified Modeling Language (UML) is a type of behavioural diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.



Sequence Diagram

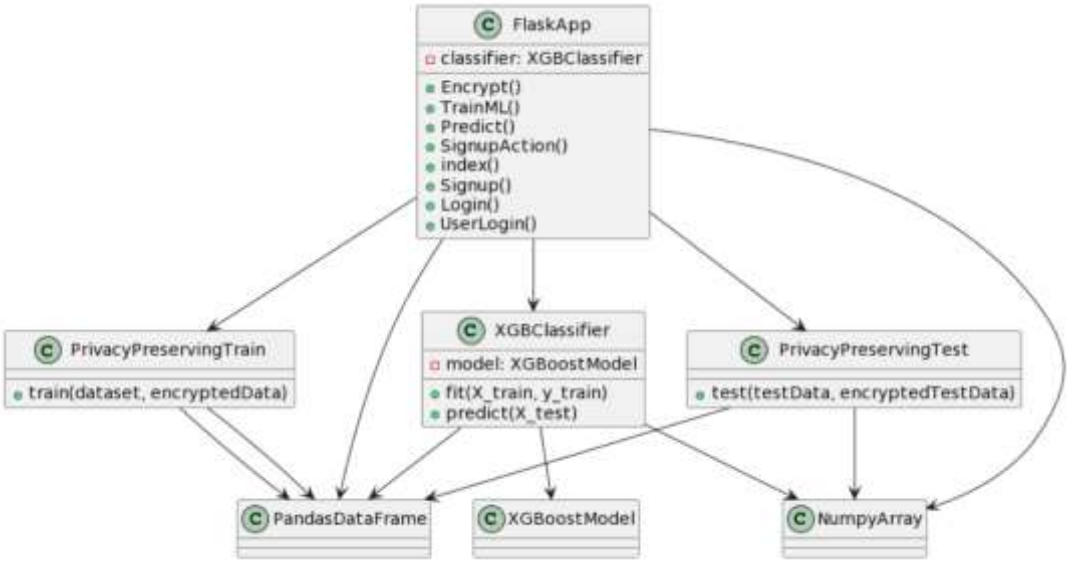
Represent the objects participating in the interaction horizontally and time vertically. A Use Case is a kind of behavioral classifier that represents a declaration of an offered behavior. Each use case specifies some behavior, possibly including variants that the subject can perform in collaboration with one or more actors. Use cases define the offered behavior of the subject without reference to its internal structure. These behaviors, involving interactions between the actor and the subject, may result in changes to the state of the subject and communications with its environment. A use case can include possible variations of its basic behavior, including exceptional behavior and error handling.

ISSN: 0975-3583, 0976-2833 VOL14, ISSUE 10, 2023



Class Diagram

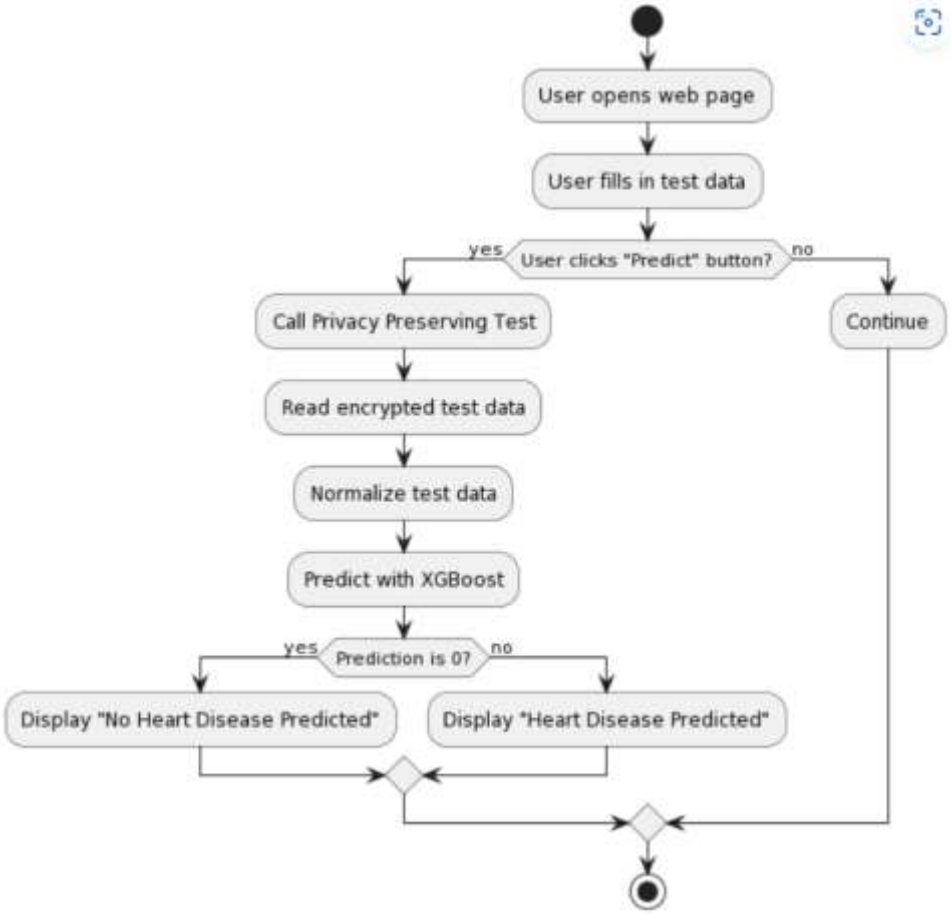
The class diagram is used to refine the use case diagram and define a detailed design of the system. The class diagram classifies the actors defined in the use case diagram into a set of interrelated classes. The relationship or association between the classes can be either an "is-a" or "has-a" relationship. Each class in the class diagram may be capable of providing certain functionalities. These functionalities provided by the class are termed "methods" of the class. Apart from this, each class may have certain "attributes" that uniquely identify the class.



Activity diagram

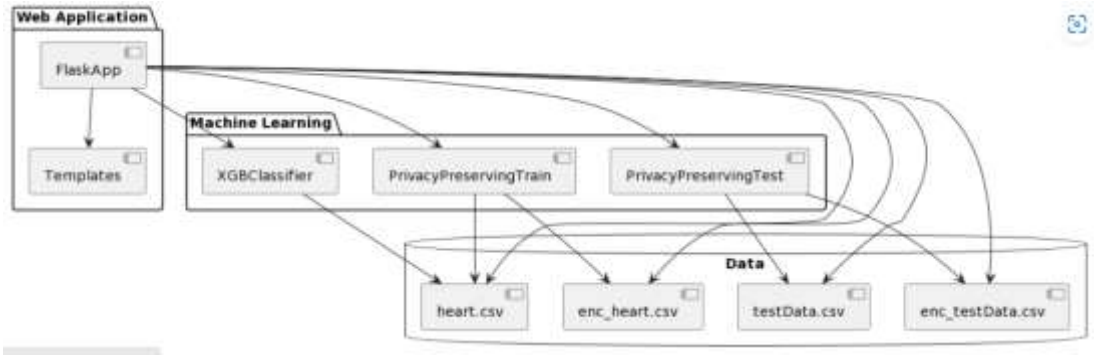
Activity diagram is another important diagram in UML to describe the dynamic aspects of the system.

ISSN: 0975-3583, 0976-2833 VOL14, ISSUE 10, 2023



Component diagram

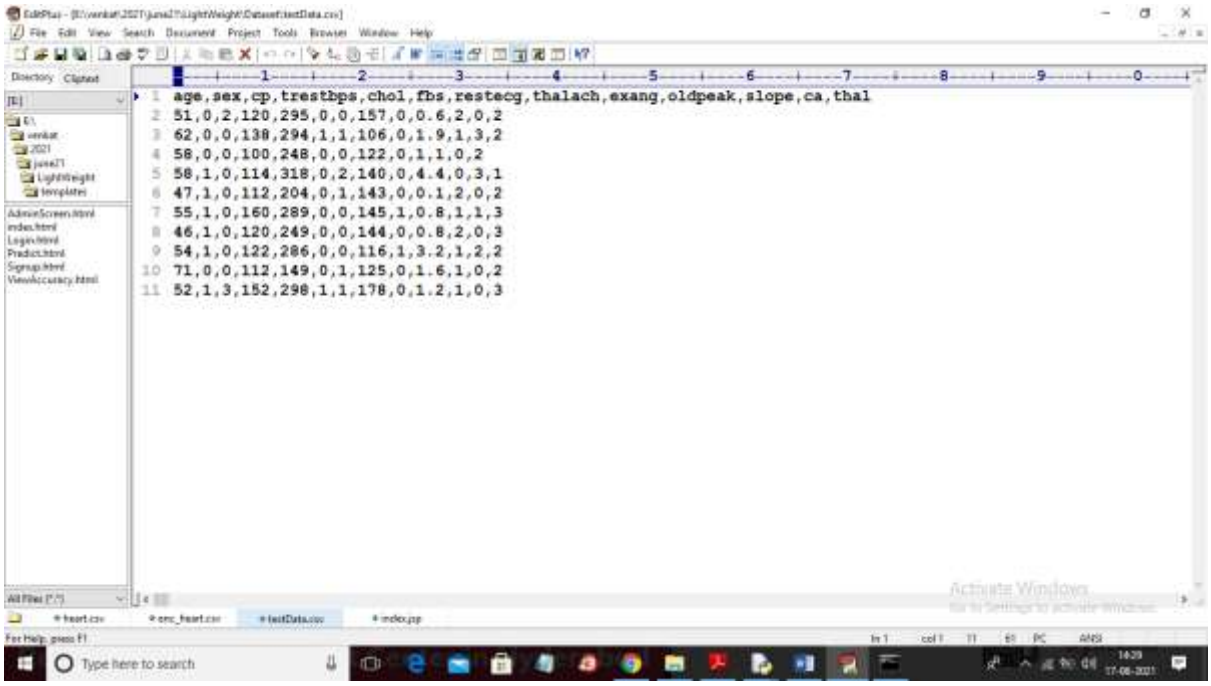
Component diagram describes the organization and wiring of the physical components in a system.



4. Results and discussion

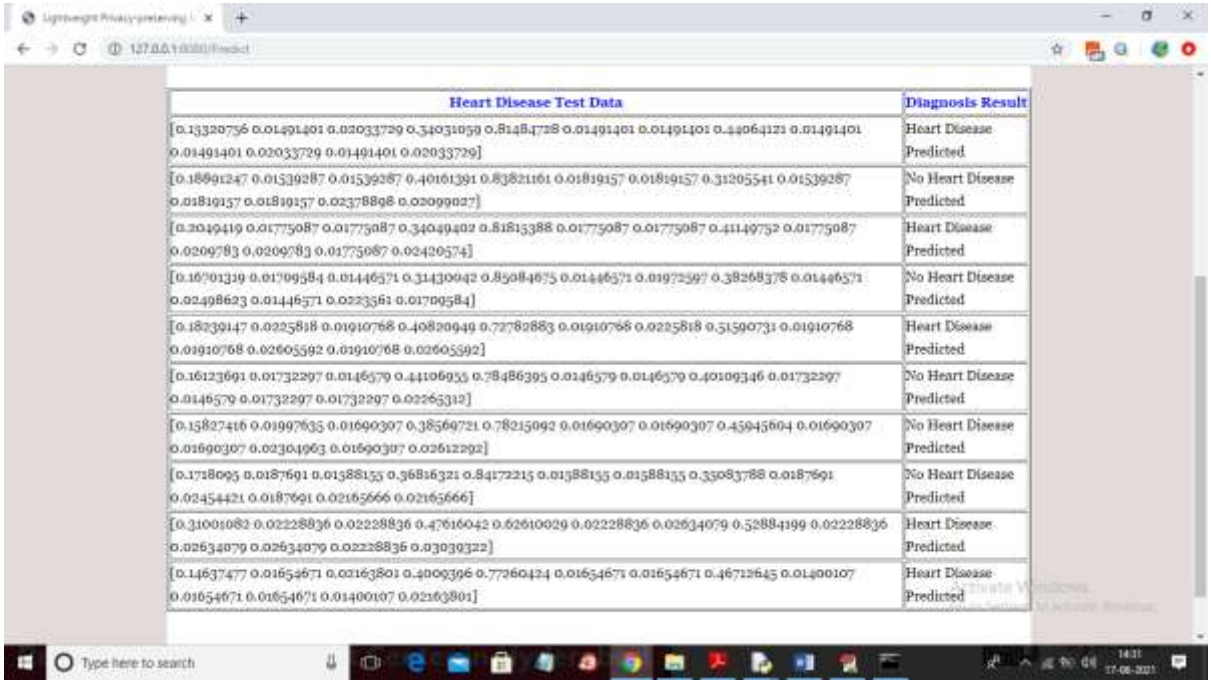
In above screen read red colour comments to know about XGBOOST training on encrypted data and now go back to previous application and click on 'Predict Using Encrypted Data' link to predict disease from new test data and below is the test data screen

ISSN: 0975-3583, 0976-2833 VOL14, ISSUE 10, 2023



```
age,sex,cp,trestbps,chol,fbs,restecg,thalach,exang,oldpeak,slope,ca,thal
51,0,2,120,295,0,0,157,0,0.6,2,0,2
62,0,0,138,294,1,1,106,0,1.9,1,3,2
58,0,0,100,248,0,0,122,0,1,1,0,2
58,1,0,114,318,0,2,140,0,4.4,0,3,1
47,1,0,112,204,0,1,143,0,0.1,2,0,2
55,1,0,160,289,0,0,145,1,0.8,1,1,3
46,1,0,120,249,0,0,144,0,0.8,2,0,3
54,1,0,122,286,0,0,116,1,3.2,1,2,2
71,0,0,112,149,0,1,125,0,1.6,1,0,2
52,1,3,152,298,1,1,178,0,1.2,1,0,3
```

Above is the test data which XGBOOST will encrypt and perform prediction of disease and if you want u can add new records to above test data and this testData.csv file is available inside 'Dataset' folder



Heart Disease Test Data	Diagnosis Result
[0.13320756 0.01491401 0.02033729 0.34031059 0.81847728 0.01491401 0.01491401 0.44064121 0.01491401 0.01491401 0.02033729 0.01491401 0.02033729]	Heart Disease Predicted
[0.18891247 0.01539287 0.01539287 0.40161391 0.83821161 0.01819157 0.01819157 0.31205541 0.01539287 0.01819157 0.01819157 0.02378898 0.02099027]	No Heart Disease Predicted
[0.2049419 0.01775087 0.01775087 0.34049402 0.81813388 0.01775087 0.01775087 0.41149752 0.01775087 0.0209783 0.0209783 0.01775087 0.02420574]	Heart Disease Predicted
[0.16701319 0.01709584 0.01446571 0.31430942 0.85084675 0.01446571 0.01972597 0.38268378 0.01446571 0.02498623 0.01446571 0.0223561 0.01709584]	No Heart Disease Predicted
[0.18239147 0.0225818 0.01910768 0.40820949 0.72782883 0.01910768 0.0225818 0.51590731 0.01910768 0.01910768 0.02605592 0.01910768 0.02605592]	Heart Disease Predicted
[0.16123691 0.01732297 0.0146579 0.44106955 0.78486395 0.0146579 0.0146579 0.40109346 0.01732297 0.0146579 0.01732297 0.01732297 0.02265312]	No Heart Disease Predicted
[0.15827416 0.01997635 0.01690307 0.38569721 0.78215092 0.01690307 0.01690307 0.45945604 0.01690307 0.01690307 0.02304963 0.01690307 0.02612292]	No Heart Disease Predicted
[0.1718095 0.0187691 0.01588155 0.36816321 0.84172215 0.01588155 0.01588155 0.33083788 0.0187691 0.02454421 0.0187691 0.02165666 0.02165666]	No Heart Disease Predicted
[0.31001082 0.02228836 0.02228836 0.47616042 0.62610029 0.02228836 0.02634079 0.52884199 0.02228836 0.02634079 0.02634079 0.02228836 0.03039322]	Heart Disease Predicted
[0.14637477 0.01654671 0.02163801 0.4009396 0.77260424 0.01654671 0.01654671 0.46712645 0.01400107 0.01654671 0.01654671 0.01400107 0.02163801]	Heart Disease Predicted

In above screen in first column you can see then encrypted test data and in second column you can see prediction result as 'No Heart Disease Detected' or 'Heart Disease Detected.

5. Conclusion

The proposed research work presents a comprehensive solution to the challenges associated with mobile-based health symptom prediction and disease diagnosis, with a strong emphasis on patient data privacy and response time optimization. By introducing Edge Nodes into the healthcare ecosystem, the research effectively reduces response times, ensuring that patients receive timely diagnoses, particularly critical in cases like heart disease. The use of Light Weight Homomorphic Encryption safeguards patient data during machine learning model training and prediction, eliminating the risk of data exposure. The LPME framework, which combines this encryption technique with the XGBOOST classifier, offers a robust approach to disease prediction while

ISSN: 0975-3583, 0976-2833 VOL14, ISSUE 10, 2023

preserving patient privacy. Overall, this research paves the way for secure, efficient, and privacy-conscious healthcare applications that can revolutionize the delivery of medical services in the digital age.

References

[1]. Shah, A.A.; Piro, G.; Grieco, L.A.; Boggia, G. A qualitative cross-comparison of emerging technologies for software-defined systems. In Proceedings of the 2019 Sixth International Conference on Software Defined Systems (SDS), Rome, Italy, 10–13 June 2019; pp. 138–145.

[2]. Ali, A.; Mehboob, M. Comparative analysis of selected routing protocols for wlan based wireless sensor networks (wsns). In Proceedings of the 2nd International Multi-Disciplinary Conference, Gujrat, Pakistan, 19–20 December 2016; Volume 19, p. 20.

[3]. Shah, A.; Piro, G.; Grieco, L.A.; Boggia, G. A review of forwarding strategies in transport software-defined networks. In Proceedings of the 2020 22nd International Conference on Transparent Optical Networks (ICTON), Bari, Italy, 19–23 July 2020; pp. 1–4.

[4]. Bruce, R.R.; Cunard, J.P.; Director, M.D. From Telecommunications to Electronic Services: A Global Spectrum of Definitions, Boundary Lines, and Structures; Butterworth-Heinemann: Oxford, UK, 2014.

[5]. Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; Santamaría, V. Blockchain and smart contracts for insurance: Is the technology mature enough? Future Internet 2018, 10, 20.

[6]. Jia, B.; Zhou, T.; Li, W.; Liu, Z.; Zhang, J. A Blockchain-Based Location Privacy Protection Incentive Mechanism in Crowd Sensing Networks. Sensors 2018, 18, 3894.

[7]. Biswas, K.; Muthukkumarasamy, V. Securing smart cities using blockchain technology. In Proceedings of the 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, NSW, Australia, 12–14 December 2016; pp. 1392–1393.

[8]. Fernández-Caramés, T.M.; Froiz-Míguez, I.; Blanco-Novoa, O.; Fraga-Lamas, P. Enabling the Internet of Mobile Crowdsourcing Health Things: A Mobile Fog Computing, Blockchain and IoT Based Continuous Glucose Monitoring System for Diabetes Mellitus Research and Care. Sensors 2019, 19, 3319.

[9]. Ali, A.; Naveed, M.; Mehboob, M.; Irshad, H.; Anwar, P. An interference aware multi-channel mac protocol for wasn. In Proceedings of the 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT), Karachi, Pakistan, 5–7 April 2017; pp. 1–9.

[10]. Beebeejaun, A. VAT on foreign digital services in Mauritius; a comparative study with South Africa. Int. J. Law Manag. 2020, 63, 239–250.

[11]. Aziz Shah, A.; Piro, G.; Grieco, L.A.; Boggia, G. A quantitative cross-comparison of container networking technologies for virtualized service infrastructures in local computing environments. Trans. Emerg. Telecommun. Technol. 2021, 32, e4234.

[12]. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Choo, K.-K.R. Blockchain-enabled authentication handover with efficient privacy protection in sdn-based 5g networks. IEEE Trans. Netw. Sci. Eng. 2019, 8, 1120–1123.

[13]. Kim, H.; Kim, S.-H.; Hwang, J.Y.; Seo, C. Efficient Privacy-Preserving Machine Learning for Blockchain Network. IEEE Access 2019, 7, 136481–136495.

[14]. Cirstea, A.; Enescu, F.M.; Bizon, N.; Stirbu, C.; Ionescu, V.M. Blockchain Technology Applied in Health The Study of Blockchain Application in the Health System (II). In Proceedings of the 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 28–30 June 2018; pp. 1–4.

[15]. Yazdinejad, A.; Srivastava, G.; Parizi, R.M.; Dehghantanha, A.; Choo, K.-K.R.; Aledhari, M. Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain. IEEE J. Biomed. Health Inform. 2020, 24, 2146–2156.

ISSN: 0975-3583, 0976-2833 VOL14, ISSUE 10, 2023

[16]. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Inform. J. 2018, 25, 1398–1411.

[17]. El-Rewini, Z.; Sadatsharan, K.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Cybersecurity challenges in vehicular communications. Veh. Commun. 2019, 23, 100214.

[18]. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for iot security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.

[19]. Hang, L.; Kim, D.-H. Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. Sensors 2019, 19, 2228.

[20]. Yu, B.; Kermanshahi, S.K.; Sakzad, A.; Nepal, S. Chameleon Hash Time-Lock Contract for Privacy Preserving Payment Channel Networks. In International Conference on Provable Security; Springer: Cham, Switzerland, 2019; pp. 303–318.

[21]. Hameed, K.; Ali, A.; Naqvi, M.H.; Jabbar, M.; Junaid, M.; Haider, A. Resource management in operating systems-a survey of scheduling algorithms. In Proceedings of the International Conference on Innovative Computing (ICIC), Lanzhou, China, 2–5 August 2016; pp. 2–5.

[22]. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. Sensors 2019, 19, 326.

[23]. Daraghmi, E.-Y.; Daraghmi, Y.-A.; Yuan, S.-M. MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management. IEEE Access 2019, 7, 164595–164613.

[24]. Jung, Y.; Peradilla, M.; Agulto, R. Packet Key-Based End-to-End Security Management on a Blockchain Control Plane. Sensors 2019, 19, 2310.

[25]. Esposito, C.; de Santis, A.; Tortora, G.; Chang, H.; Choo, K.-K.R. Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. 2018, 5, 31–37.