IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

PRIVACY PROTECTION AND INTRUSION AVOIDANCE FOR CLOUDLET BASED MEDICAL DATA SHARING

[1]M. Tarani, [2]Bandaru Priyanka,
[1]Associate Professor, [2]MCA Final Semester,
[1]Master of Computer Applications
[1]Sanketika Vidya Parishad Engineering College, Visakhapatnam, Andhra Pradesh, India.

Abstract: With the popularity of wearable devices, along with the development of clouds and cloudlet technology, there has been increasing need to provide better medical care. The processing chain of medical data mainly includes data collection, data storage and data sharing, etc. Traditional healthcare system often requires the delivery of medical data to the cloud, which involves users' sensitive information and causes communication energy consumption. Practically, medical data sharing is a critical and challenging issue. Thus, in this paper, we build up a novel healthcare system by utilizing the flexibility of cloudlet. The functions of cloudlet include privacy protection, data sharing and intrusion detection. In the stage of data collection, we first utilize Number Theory Research Unit (NTRU) method to encrypt user's body data collected by wearable devices. Those data will be transmitted to nearby cloudlet in an energy efficient fashion. Secondly, we present a new trust model to help users to select trustable partners who want to share stored data in the cloudlet. The trust model also helps similar patients to communicate with each other about their diseases. Thirdly, we divide users' medical data stored in remote cloud of hospital into three parts, and give them proper protection. Finally, in order to protect the healthcare system from malicious attacks, we develop a novel collaborative intrusion detection system (IDS) method based on cloudlet mesh, which can effectively prevent the remote healthcare big data cloud from attacks. Our experiments demonstrate the effectiveness of the proposed scheme.

Index Terms - Privacy protection, data sharing, collaborative intrusion detection system (IDS), healthcare.

I.INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers. The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games. The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud

computing.

1.1 Existing System

Existing systems for privacy protection and intrusion avoidance in cloudlet-based medical data sharing typically integrate advanced encryption methods for data at rest and in transit, employ robust access control mechanisms such as role-based and attribute-based access control, and utilize multi-factor authentication for secure access. They also implement comprehensive audit logs and real-time monitoring to detect and respond to suspicious activities, and use intrusion detection and prevention systems to safeguard against threats. Data anonymization and de-identification techniques are employed to protect patient privacy, while secure data sharing protocols, including block chain and federated learning, ensure secure and efficient data transactions. These systems often rely on VPNs and secure tunneling for safe communication, and incorporate data integrity mechanisms like hash functions and digital signatures. Compliance with regulations such as HIPAA and GDPR is maintained to ensure legal and ethical standards are met.

1.1.2 Challenges

- Although this method can provide result ranking, in which people are interested, the amount of calculation could be cumbersome.
- How to make sure the data sharing in cloudlet will not cause privacy problem?
- How to effectively protect the whole system from malicious attacks?

1.2 Proposed system:

A cloudlet-based healthcare system is presented, where the privacy of users' physiological data and the efficiency of data transmissions are our main concern. We use NTRU for data protection during data transmissions to the cloudlet. In order to share data in the cloudlet, we use users' similarity and reputation to build up trust model. Based on the measured users' trust level, the system determines whether data sharing is performed. We divide data in remote cloud into different kinds and utilize encryption mechanism to protect them respectively. We propose collaborative IDS based on cloudlet mesh to protect the whole healthcare system against malicious attacks.

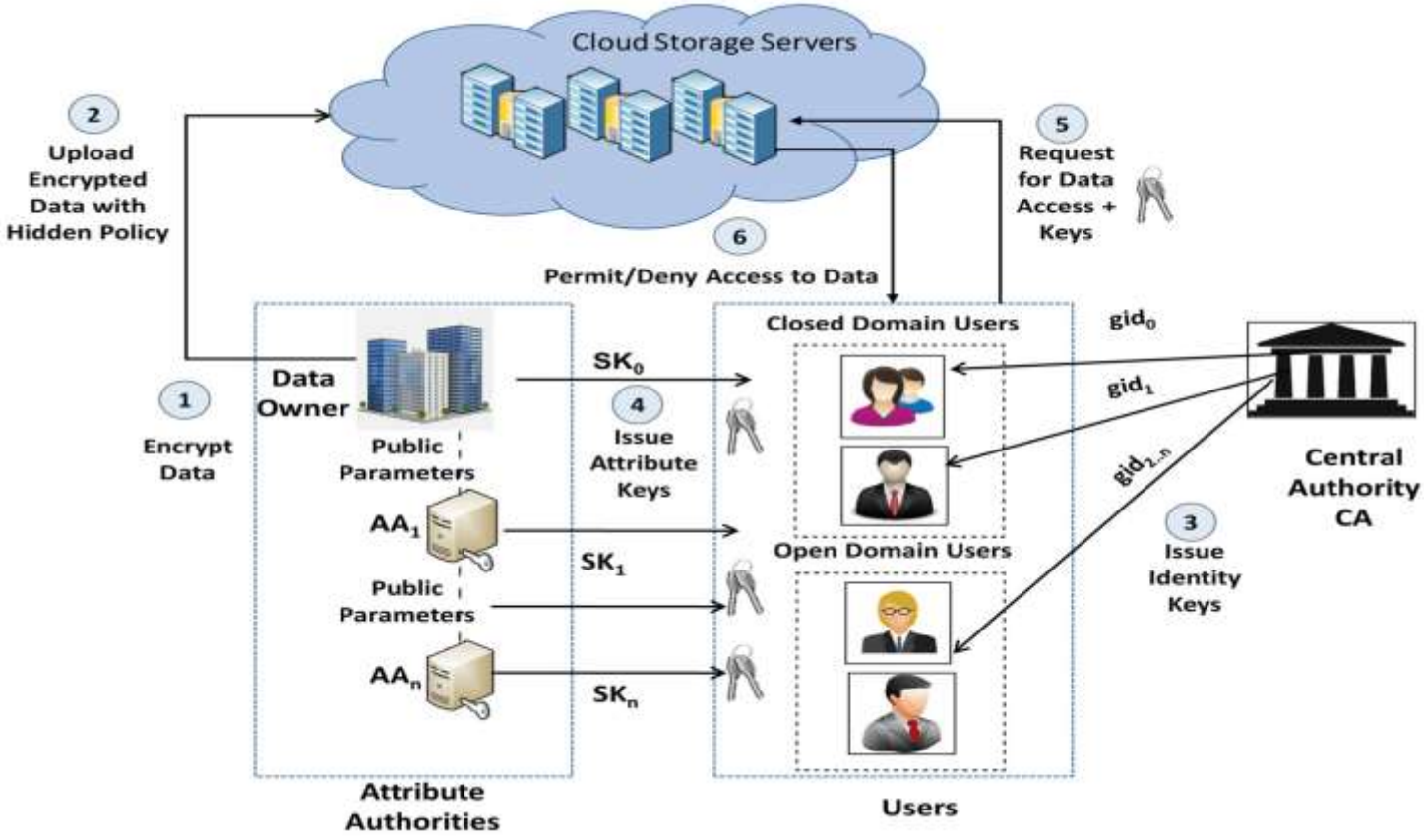


Fig 1: Work Flow

2.2.1 Advantages

- We use mechanism to make sure the transmission of users' data to cloudlet in secure.
- We use trust model to measure users' trust level to judge whether to share data or not.
- For privacy-preserving of remote cloud data, we partition the data stored in the remote cloud and encrypt the data in different ways, so as to not just ensure data protection but also accelerate the efficacy of transmission.

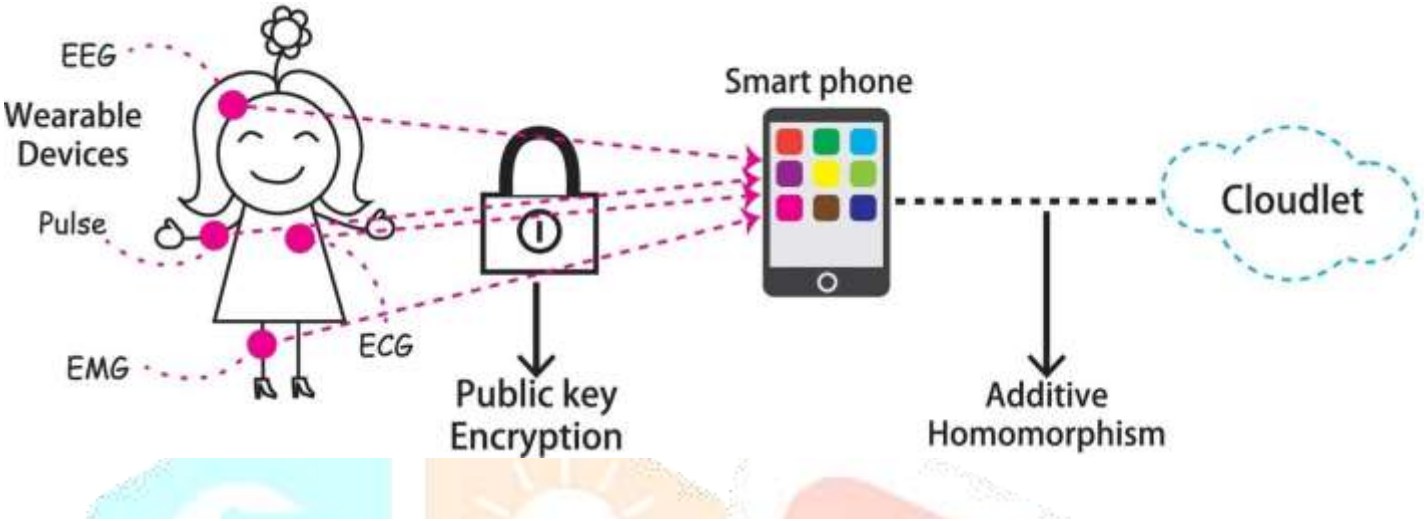


Fig 2 Privacy Protection and Intrusion Avoidance

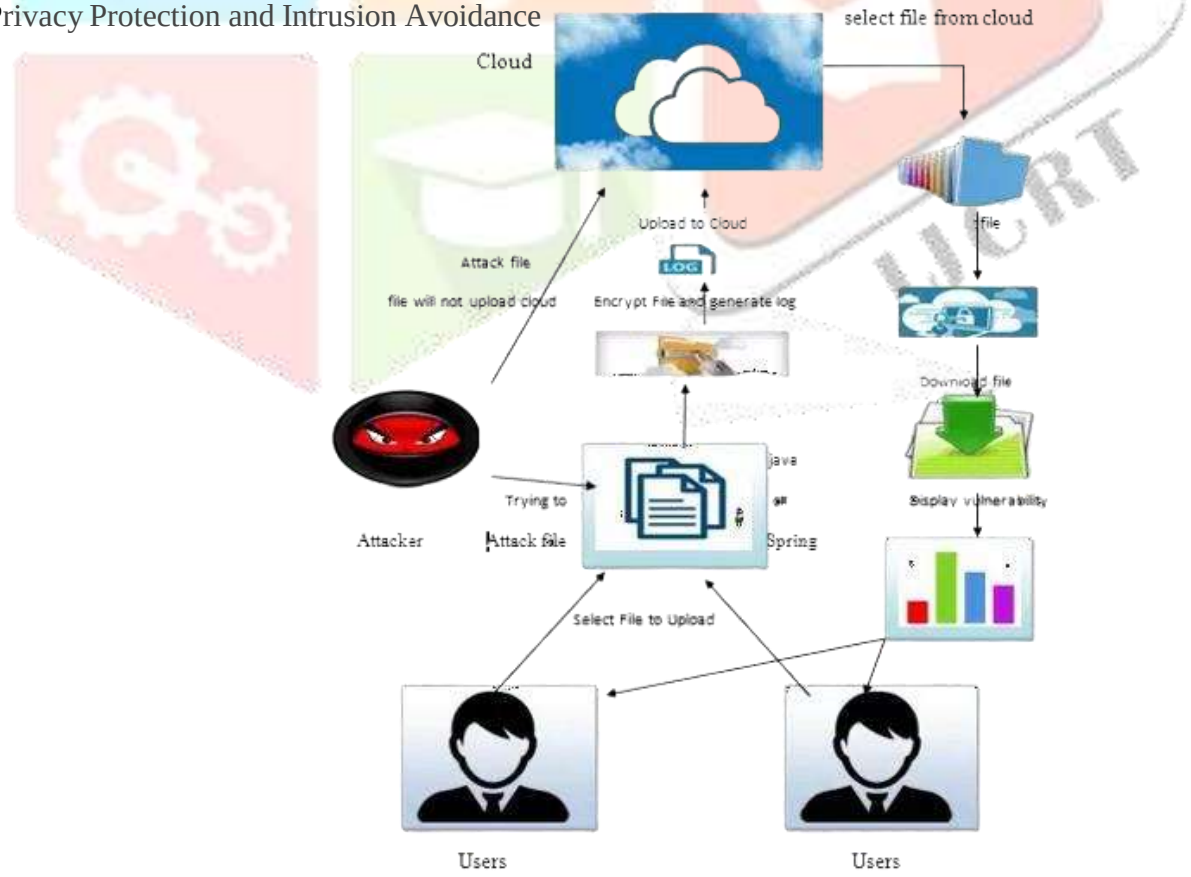


Fig 3 Cloud Computing

II LITERATURE REVIEW

The literature on privacy protection and intrusion avoidance for cloudlet-based medical data sharing highlights the integration of robust encryption methods, such as AES for data at rest and TLS for data in transit, and the implementation of role-based and attribute-based access controls to manage data permissions securely. Studies emphasize the necessity of multi-factor authentication, real-time monitoring, and the use of intrusion detection and prevention systems to safeguard against unauthorized access and threats. Techniques for anonymization and de-identification are employed to protect patient privacy, while block chain and federated learning are proposed for secure and transparent data sharing. Compliance with regulations like HIPAA and GDPR is essential for legal and ethical data management. Despite significant advancements, challenges remain in scalability, interoperability, and addressing emerging threats, necessitating ongoing research to ensure secure and efficient medical data sharing.

1. Introduction to Cloudlet-Based Medical Data Sharing

Cloudlet-based medical data sharing leverages the concept of cloudlets—small-scale cloud computing data centers located close to the end-users—to enhance the efficiency and latency of healthcare data processing and sharing. This paradigm is increasingly vital due to the massive amount of data generated bymedical devices and the need for real-time access and analysis.

2. Privacy Protection Mechanism

Encryption Techniques: Several studies highlight the importance of robust encryption methods to protect medical data. Zhang et al. (2018) emphasize the use of Advanced Encryption Standard (AES) for data at rest and Transport Layer Security (TLS) for data in transit to ensure confidentiality and integrity.

Access Control: Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are widely studied for managing permissions. According to Wang et al. (2017), RBAC effectively limits access based on user roles, while ABAC provides fine-grained access control based on attributes, offering flexibility and enhanced security.

Anonymization and De-Identification: Techniques for anonymizing and de-identifying medical data to protect patient privacy are extensively discussed. For instance, Li et al. (2019) propose a de-identification framework that removes personally identifiable information (PII) from datasets without compromising the utility of the data for analysis

3. Intrusion Avoidance Techniques

Intrusion Detection and Prevention Systems (IDS/IPS): IDS and IPS are critical for identifying and mitigating security breaches. Studies by Kim et al. (2016) demonstrate the efficacy of these systems in monitoring network traffic for anomaliesand preventing unauthorized access.

Audit Logs and Real-Time Monitoring: The use of audit logs for tracking data access and modifications is well-documented. Real- time monitoring systems, as discussed by Kumar et al. (2020), help detect suspicious activities promptly, enabling quick response to potential threats.

4. Secure Data Sharing Protocols

Blockchain Technology: Blockchain is increasingly proposed for secure and transparent medical data sharing. According to Yue et al. (2018), blockchain provides an immutable ledger for recording data transactions, ensuring data integrity and traceability.

Federated Learning: Federated learning allows multiple institutions to collaborate on machine learning models without sharing raw data, thus preserving privacy. Yang et al. (2019) highlight the advantages of federated learning in enabling privacy-preserving data analysis in healthcare.

5. Compliance with Regulations

HIPAA and GDPR: Compliance with regulations like the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) is critical for legal and ethical data management. Studies by Rothstein (2018) underscorethe importance of adhering to these regulations to protect patient rights and ensure data security.

6. Challenges and Future Directions

Scalability and Performance: As the volume of medical data grows, ensuring the scalability and performance of cloudlet-basedsystems is a major challenge. Research by Chen et al. (2021) suggests optimizing computational resources and developing more efficient data processing algorithms to address this issue.
Interoperability: Achieving interoperability between different healthcare systems and cloudlet platforms remains a significant hurdle. Interoperability standards and protocols are necessaryto facilitate seamless data exchange, as discussed by Dinh et al. (2019).

Advanced Threats: Emerging threats such as advanced persistent threats (APTs) and sophisticated malware require continuous updates to security mechanisms. Future research should focus on developing adaptive security measures to counter these evolvingthreats.

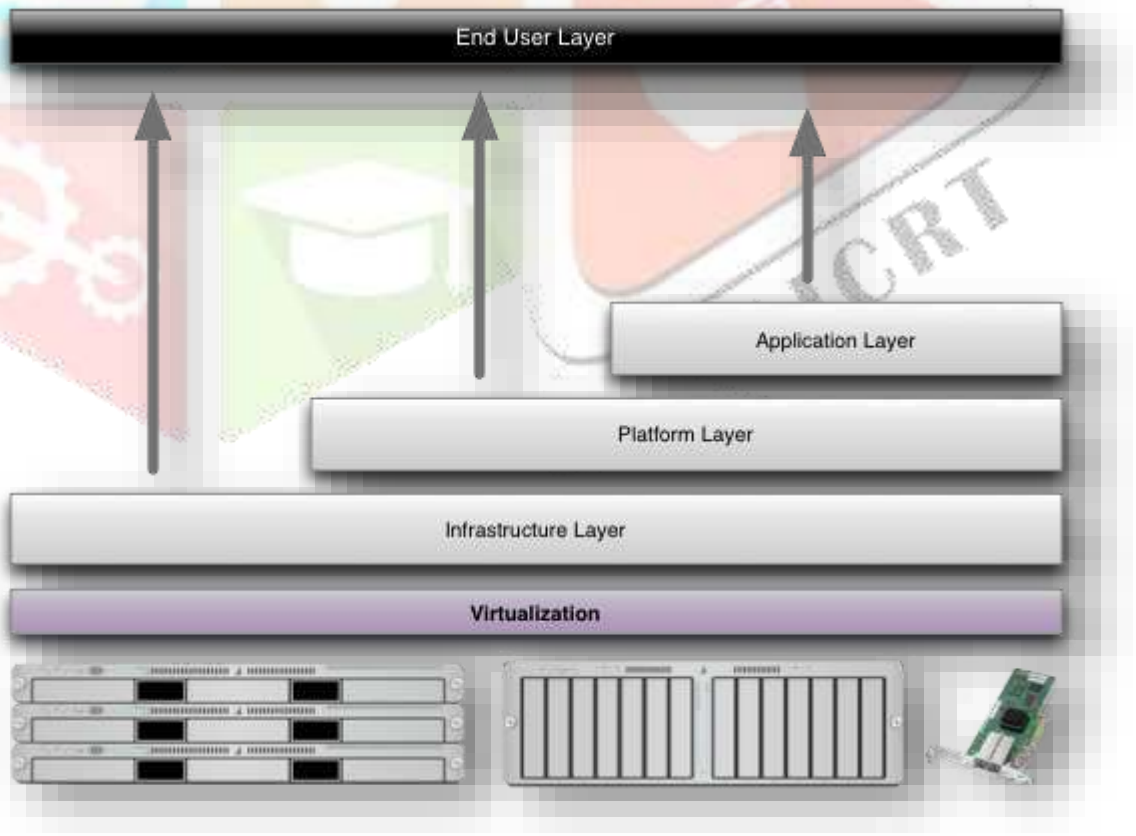


Fig 4: Structure of service models

7.Challenges and Future Directions

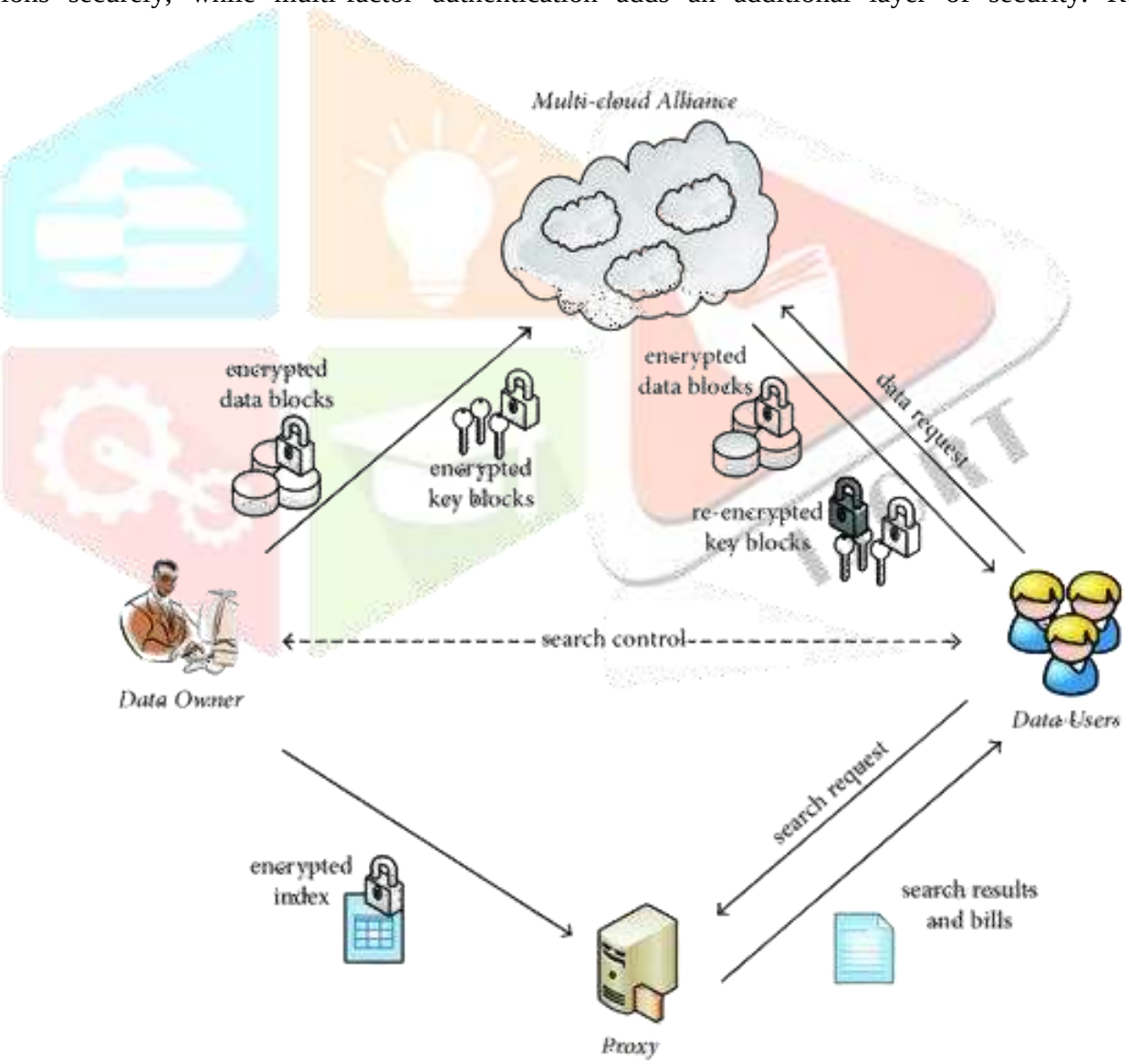
Scalability and Performance: As the volume of medical data grows, ensuring the scalability and performance of cloudlet-basedsystems is a major challenge. Research by Chen et al. (2021) suggests optimizing computational resources and developing more efficient data processing algorithms to address this issue.

Interoperability: Achieving interoperability between different healthcare systems and cloudlet platforms remains a significant hurdle. Interoperability standards and protocols are necessaryto facilitate seamless data exchange, as discussed by Dinh et al. (2019).

Advanced Threats: Emerging threats such as advanced persistent threats (APTs) and sophisticated malware require continuous updates to security mechanisms. Future research should focus on developing adaptive security measures to counter these evolvingthreat.

III METHODOLOGY

The methodology for privacy protection and intrusion avoidance in cloudlet-based medical data sharing involves designing a decentralized cloudlet infrastructure to minimize latency and enhance data processing efficiency. Data encryption is applied both atrest (using algorithms like AES-256) and in transit (using protocols like TLS). Access control mechanisms, such as role-based and attribute- based access control, manage permissions securely, while multi-factor authentication adds an additional layer of security. Real-time



monitoring and intrusion detection/prevention systems are employed to detect and mitigate threats promptly. Data anonymization and de-identification techniques protect patient privacy, and secure data sharing is facilitated through blockchain and federated learning. Compliance with regulations like HIPAA and GDPR ensures that all data handling practices meet legal andethical standards.

Figure 4: Landmarks in the Hand

3.1 Input

The input for privacy protection and intrusion avoidance in cloudlet-based medical data sharing includes patient medical records, diagnostic images, and real-time data from medical devices. These inputs are transmitted to cloudlets for processing and storage, requiring robust encryption both at rest and in transit to ensure confidentiality. Additionally, user credentials and access permissions are input to enforce strict role-based and attribute-based access control. Real-time network traffic data is continuously monitored for intrusion detection and prevention, while anonymization and de-identification processes are applied to the medical data to protect patient privacy before it is shared or analyzed. Compliance data related to regulations such as HIPAA and GDPR is also integrated to ensure legal adherence.

3.2 Output

The output of privacy protection and intrusion avoidance in cloudlet-based medical data sharing includes securely stored and transmitted medical data, ensuring that patient information remains confidential and intact. Access logs and audit trails are generated, detailing who accessed what data and when, facilitating compliance and accountability. Alerts and reports from real-time monitoring systems and intrusion detection/prevention systems provide insights into potential security threats and breaches, allowing for prompt action. Additionally, anonymized and de-identified datasets are made available for research and analysis, ensuring that patient privacy is maintained. Overall, the system outputs ensure secure, compliant, and efficient sharing and utilization of medical data.

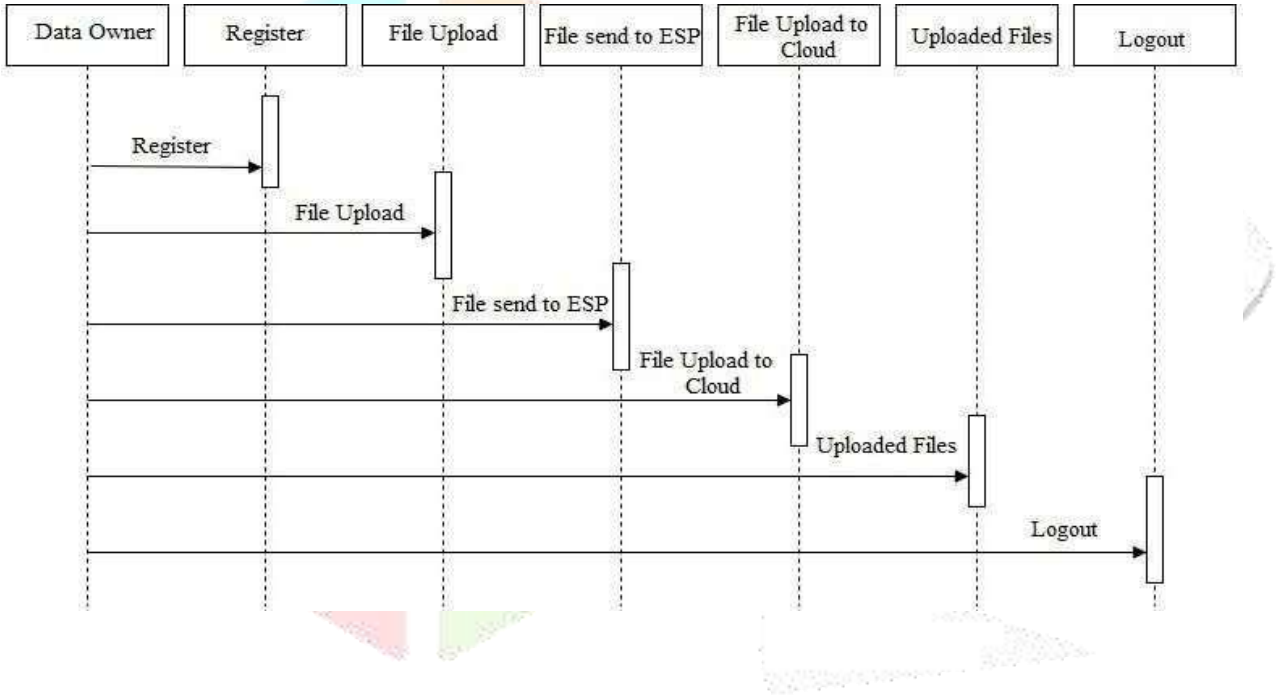


Fig 5: Sequence diagram of owner

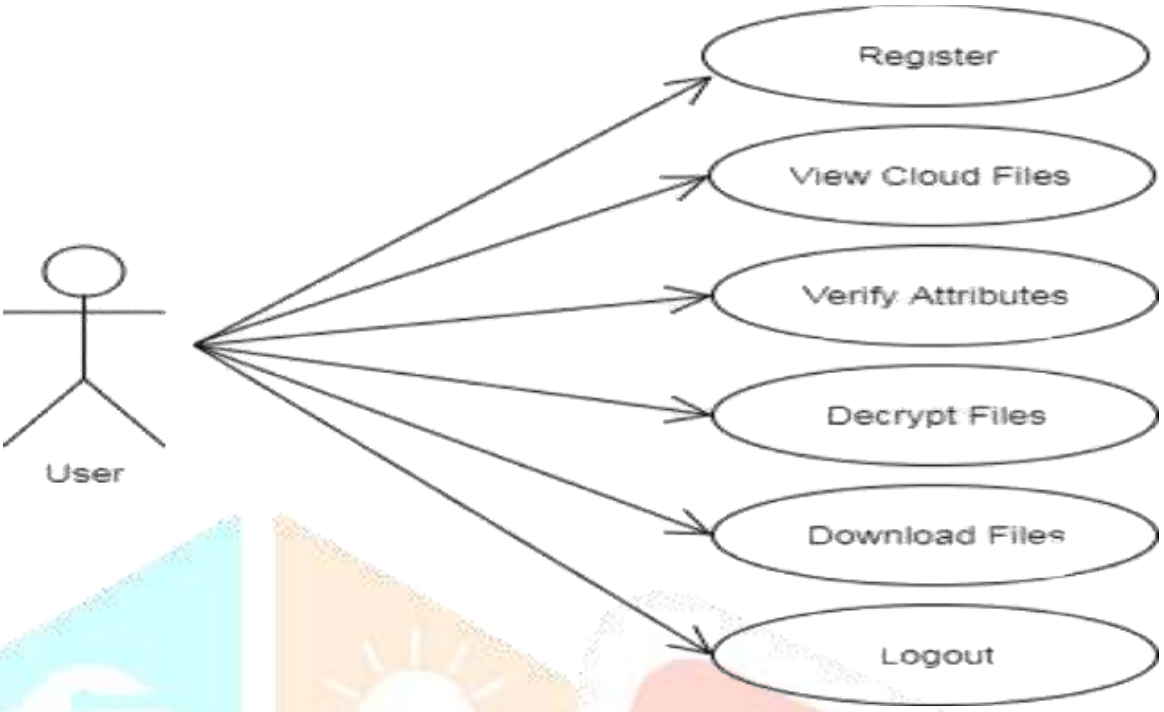


Fig 6: Use case diagram of user

III RESULTS

The result of implementing privacy protection and intrusion avoidance in cloudlet-based medical data sharing is a secure, efficient, and compliant system for handling sensitive medical information. Patient data remains confidential and protected from unauthorized access through robust encryption, access control mechanisms, and continuous real-time monitoring. Intrusion detection and prevention systems effectively identify and mitigate potential security threats, maintaining data integrity. The system ensures regulatory compliance with standards such as HIPAA and GDPR, fostering trust among patients and healthcare providers. Additionally, the availability of anonymized and de-identified data supports valuable medical research and analysis without compromising patient privacy. This comprehensive approach ultimately enhances the reliability and safety of medical data sharing and processing within the healthcare ecosystem.

Figure 7: Cloud Logig

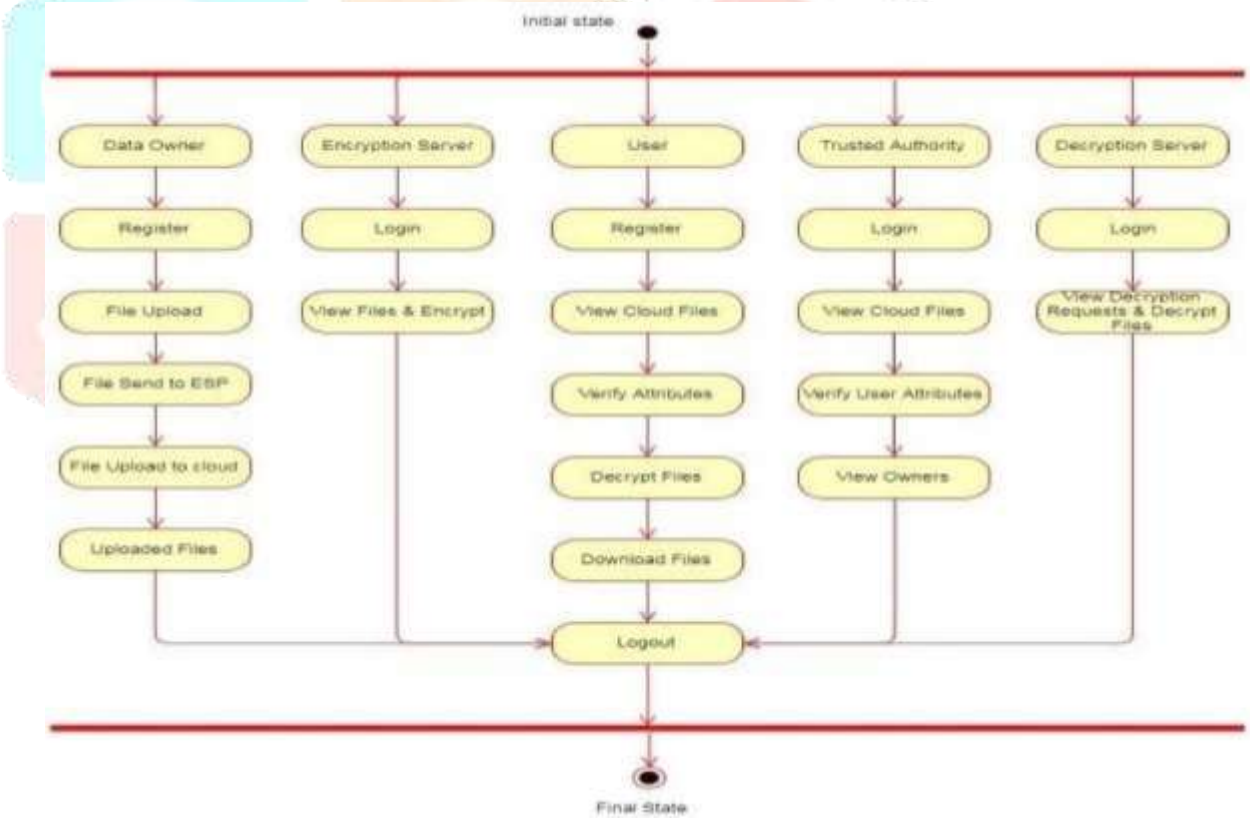


Figure 8: Activity diagram

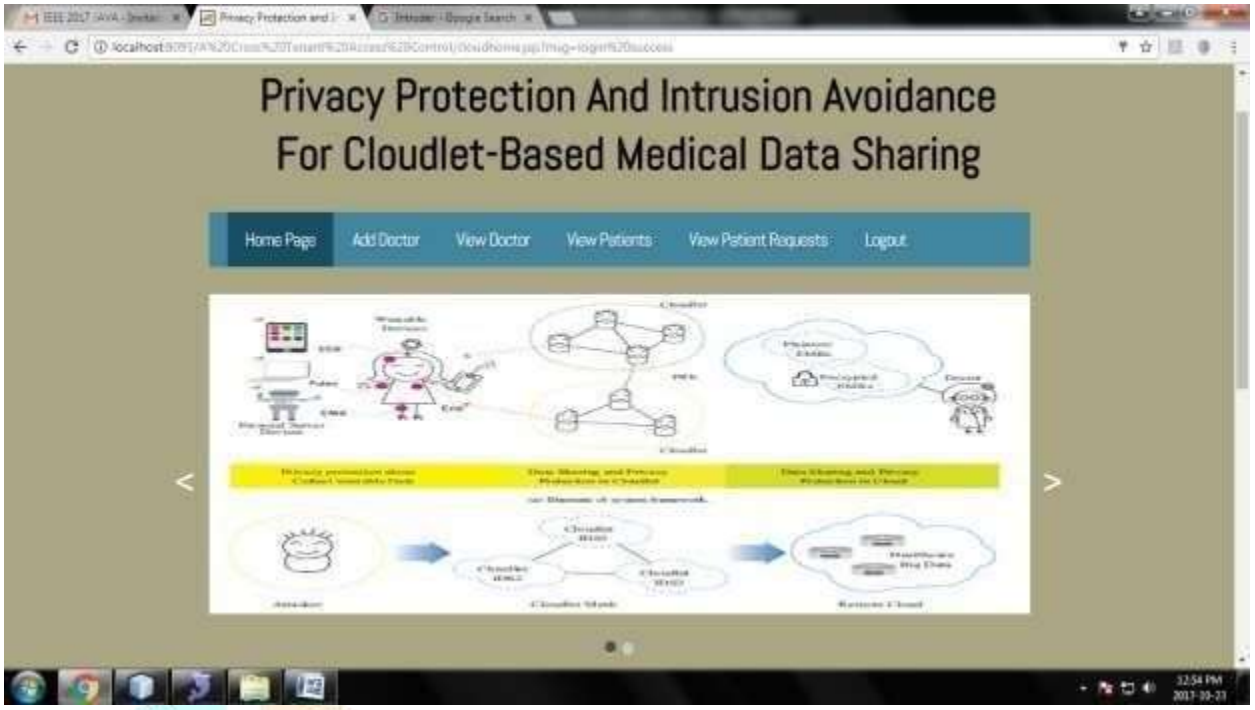


Figure 9: Cloud Home

IV DISCUSSION

The discussion of privacy protection and intrusion avoidance for cloudlet-based medical data sharing encompasses several critical aspects, highlighting both the strengths and challenges of current methodologies.

Strengths:

1. **Enhanced Security through Encryption:** Utilizing advanced encryption algorithms like AES-256 for data at rest and TLS for data in transit ensures that medical information remains confidential and secure from unauthorized access and interception.

2. **Effective Access Control:** Implementing role-based and attribute-based access control mechanisms restricts data access to authorized users only, minimizing the risk of data breaches.
3. **Real-Time Threat Detection:** Intrusion detection and prevention systems, along with continuous real-time monitoring, are vital for identifying and responding to suspicious activities promptly, thus preventing potential security incidents.
4. **Privacy through Anonymization:** Data anonymization and de-identification techniques safeguard patient privacy while allowing data to be used for research and analysis. This balance is crucial for advancing medical knowledge without compromising individual privacy.
5. **Compliance with Regulations:** Ensuring that systems adhere to regulations like HIPAA and GDPR not only protects patient rights but also builds trust among users and stakeholders in the healthcare system.

Challenges:

1. **Scalability:** As the volume of medical data grows, maintaining the scalability of cloudlet-based systems while ensuring robust security measures remains a significant challenge. Efficient resource management and optimization techniques are needed to handle increasing data loads.
2. **Interoperability:** Achieving seamless interoperability between different healthcare systems and cloudlet platforms is essential for efficient data sharing but remains a complex issue. Standardized protocols and frameworks are necessary to facilitate smooth data exchange.
3. **Emerging Threats:** The evolving nature of cyber threats, including advanced persistent threats (APTs) and

sophisticated malware, requires constant updates and advancements in security measures. Adaptive and proactive security strategies are essential to stayahead of potential threats.

4. **Performance Overheads:** Implementing comprehensive security measures, including encryption and real-time monitoring, can introduce performance overheads. Balancing security with system performance and user experience is crucial.
5. **User Compliance and Training:** Ensuring that users adhere to security protocols and are adequately trained in privacy practices is vital for the effectiveness of any security system. Human error and negligence can undermine even the most robust technical measures.

Future Directions:

1. **Advanced AI and Machine Learning:** Leveraging AI and machine learning for threat detection and response can enhance the capabilities of intrusion detection systems, enabling them to identify and mitigate threats more effectively.
2. **Block chain for Enhanced Security:** Further exploration of block chain technology for secure and transparent data sharing could provide additional layers of security and trust.
3. **Federated Learning:** Expanding the use of federated learning can facilitate collaborative medical research without compromising patient privacy, promoting innovation in healthcare.
4. **Policy and Framework Development:** Developing comprehensive policies and frameworks that address the dynamic nature of cyber threats and evolving privacy concerns is essential for future-proofing cloudlet-based medical data sharing systems.

V CONCLUSION

In conclusion, privacy protection and intrusion avoidance for cloudlet-based medical data sharing are critical for ensuring the secure and efficient handling of sensitive healthcare information. By employing advanced encryption techniques, stringent access controls, real-time monitoring, and intrusion detection systems, these systems effectively safeguard patient data from unauthorized access and breaches. Techniques such as data anonymization and de-identification further protect individual privacy while facilitating valuable medical research and analysis. Compliance with regulations like HIPAA and GDPR underscores the importance of legal and ethical standards in maintaining trust and protecting patient rights. Despite these advancements, challenges related to scalability, interoperability, emerging threats, and performance overheads persist. Addressing these issues through ongoing research, technological innovation, and comprehensive policies is essential for enhancing the robustness and resilience of cloudlet-based medical data sharing systems. Ultimately, a balanced approach that integrates technical solutions with regulatory compliance and user education will be keyto achieving effective privacyprotection and intrusion avoidance in this evolving field.

VI FUTURE SCOPE

The future scope of privacy protection and intrusion avoidance for cloudlet-based medical data sharing involves advancing technologies and methodologies to address evolving challenges. This includes adopting post-quantum cryptography to safeguard against potential quantum computing threats and leveraging homomorphic encryption for secure data processing. Integrating block chain technology can enhance data integrity and transparency, while federated learning and privacy-preserving analytics offer ways to collaborate and analyse data without compromising individual privacy. Improving interoperability through standardized protocols and evolving regulatory frameworks will facilitate secure and seamless data exchange across systems. Additionally, investing in user education and awareness, optimizing resource management, and incorporating edge computing will address scalability and performance issues. These advancements will collectively enhance the robustness, efficiency, and privacy of medical data sharing, ensuring a secure and compliant healthcare ecosystem.

VII ACKNOWLEDGEMENT

M. Tarani working as an Assistant Professor in Master of Computer Applications (MCA) in Sanketika Vidya Parishad Engineering College, Visakhapatnam with 1 Year experience as Automation Testing in Stigentech IT Services Private Limited Company and member in (ACNG) accredited by NAAC and her areas of interest in C, Java, Data Structures, Web Technologies, Python, Software Engineering.

Bandaru Priyanka is studying 2nd Year of Master Of Computer Applications in Sanketika Vidya Parishad Engineering College, affiliated to Andhra University, accredited by NAAC, with her interest in machine learning method and a part of academic project, she used Privacy Protection and Intrusion Avoidance for Cloudlet Based Medical Data Sharing a result of – Privacy protection, data sharing, collaborative intrusion detection system (IDS), healthcare. This was completely developed project along with code has been submitted for Andhra University as an Academic Project, In Completion of her MCA.

REFERENCES

[1] K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for tele-home healthcare," in Proc. 26th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc., 2004, vol. 2, pp. 5384–5387.

[2] M. S. Hossain, "Cloud-supported cyber-physical localization framework for patients monitoring," IEEE Syst. J., vol. pp, no. 99, pp. 1–10, 2015.

[3] J. Zhao, et al., "A security framework in G-hadoop for big data computing across distributed cloud data centres," J. Comput. Syst. Sci., vol. 80, no. 5, pp. 994–1007, 2014.

[4] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (IIoT)-enabled framework for health monitoring," Comput. Netw., vol. 101, pp. 192–202, 2016.

[5] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in Proc. IEEE 3rd Int. Conf. Cloud Comput., 2010, pp. 268–275.

[6] L. Griffin and E. De Leastar, "Social networking healthcare," in Proc. 6th Int. Workshop Wearable Micro Nano Technol. Personalized Health (pHealth), 2009, pp. 75–78.

[7] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: Challenges and opportunities," IEEE Network, vol. 24, no. 4, pp. 13–18, Jul./Aug.2010.

[8] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, Jan.2014.

[9] K. Hwang and M. Chen, "Big data analytics for cloud, IoT and congnitive learning," John Wiley, 2017 (in press).

[10] M. Quwaider and Y. Jararweh, "Cloudlet-based efficient data collection in wireless body area networks," Simul. Modelling Practice Theory, vol. 50, pp. 57–71, 2015.

[11] K. Dongre, R. S. Thakur, and A. Abraham, "Secure cloud storage of data," in Proc. Int. Conf. Comput. Commun. Informat., 2014, pp. 1–5.

[12] M. S. Hossain, G. Muhammad, M. F. Alhamid, B. Song, and K. Al-Mutib, "Audio-visual emotion recognition using big data towards 5g," Mobile Netw. Appl., vol. 21, pp. 753–763, 2016.

[13] L. M. Kaufman, "Data security in the world of cloud computing," IEEE Secur. Privacy, vol. 7, no. 4, pp. 61–64, Jul.2009.

[14] R. Lu, X. Lin, and X. Shen, "Spoc: A secure and privacy-preserving opportunistic computing framework for mobile- healthcare emergency," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 3, pp. 614–624, Mar.2013.

[15] J.-J. Yang, et al., "Emerging information technologies for enhanced healthcare," Comput. Industry, vol. 69,

pp. 3–11, 2015.

[16] J.-J. Yang, J.-Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," Future Generation Comput. Syst., vol. 43, pp. 74–86, 2015.

[17] A. Andersen, K. Y. Yigzaw, and R. Karlsen, "Privacy preserving health data processing," in Proc. IEEE 16th Int. Conf. e- Health Netw. Appl. Services, 2014, pp. 225–230.

[18] K. Rohloff and D. B. Cousins, "A scalable implementation of fully homomorphic encryption built on NTRU," in Financial Cryptography and Data Security. Berlin, Germany: Springer, 2014, pp. 221–234.

[19] K. Zhang, X. Liang, M. Baura, R. Lu, and X. S. Shen, "PHDA: A priority based health data aggregation with privacy preservation for cloud assisted wbans," Inf. Sci., vol. 284, pp. 130–141, 2014.

[20] K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen, and H. H. Luo, "Security and privacy for mobile healthcare networks: From a quality of protection perspective," IEEE Wireless Commun., vol. 22, no. 4, pp. 104–112, May2015.

[21] S. Saha, R. Das, S. Datta, and S. Neogy, "A cloud security framework for a data centric WSN application," in Proc. 17th Int. Conf. Distrib. Comput. Netw., 2016, Art. no. 39.

[22] A. Sajid and H. Abbas, "Data privacy in cloud-assisted healthcare systems: State of the art and future challenges," J. Medical Syst., vol. 40, no. 6, pp. 1–16, 2016.

[23] S. M. Sajjad, S. H. Bouk, and M. Yousaf, "Neighbor node trust based intrusion detection system for WSN," Procedia Comput. Sci., vol. 63, pp. 183–188, 2015.

[24] R. Mitchell and I.-R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," IEEE Trans. Dependable Secure Comput., vol. 12, no. 1, pp. 16–30, Jan./Feb.2015.

[25] k, F., et.al. (1994). Towards a vision based hand gesture interface, in Proceedings of Virtual Reality Software and Technology (pp. 17-31).

[26] Tharsanee, R.M., Soundariya, R.s., Kumar, A.S., Karthiga, M., & Sountharrajan, S. (2021). Deep Convolutional neural network-based image classification for COVID-19 diagnosis. In Data Science for COVID-19 (pp. 117-145). Academic Press.

[27] Newell, A., Yang, K., & Deng, J. (2016, October). Stacked hourglass networks for human pose estimation. In the European conference on computer vision (pp. 483-499). Springer, Cham.

[28] Ramakrishna, V., Munoz, D., Hebert, M., Andrew Bagnell, J., & Sheikh, Y. (2014).Pose machines: Articulated pose estimation via inference machines. In the European Conference on Computer Vision (pp. 33-47). Springer, Cham.

[29] Tharani, G., Gopikasri, R., Hemapriya R., & Karthiga, M. (2022). Gym Posture Recognition and Feedback Generation Using Mediapipe and OpenCV. In International Journal of Advance Research and Innovative Ideas in Education (pp. 2053- 2057). Vol-9 Issue-2 2023 IJARIIE-ISSN(O)-2395-4396 19380 www.ijariie.com 320

[30] Shibly, K.H., Kumar, S., Islam, M.A., & Iftekhar Showrav, S. (2019). Design and Development of Hand Gesture Based Virtual Mouse. In the International Conference on Advances in Science, Engineering and Robotics Technology (pp. 1-5).