IJARETY

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

Volume 12, Issue 3, May-June 2025

Impact Factor: 8.152

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: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203085

Toward Privacy-Aware and Scalable Wearable Data Handling via User-Controlled Access

A. Lakshmipathi Rao[1], CH.Jagadishwar[2], A. Hasini Reddy[3], D. Tulasi[4]

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India[1]

Student, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India[2, 3, 4]

ABSTRACT: With the rise of IoT wearable devices in healthcare, enormous amounts of data are being generated—making cloud-based computation a necessity. However, many existing solutions fail to combine strong data privacy with precise, user-controlled access, especially when it comes to performing secure operations like multiplication and division on encrypted data. In this paper, we introduce two practical and privacy-preserving schemes, SAMM and SAMD, designed to securely handle multiplication and division over encrypted data. These schemes integrate the multi-key Paillier cryptosystem with ciphertext-policy attribute-based encryption (CP-ABE) to offer fine-grained access control and flexible data sharing. Our approach supports secure computation across data from single or multiple owners, protecting both privacy and access rights—even on devices with limited resources. Through experimental evaluations and security analysis, we show that SAMM and SAMD deliver better performancand lower communication overhead than current methods.

I. INTRODUCTION

IoT wearable devices play a crucial role in collecting valuable health data for both personalized treatment and broader public health insights. However, sending this sensitive data to the cloud raises serious privacy and access control issues—especially under strict regulations like GDPR and HIPAA. Current cryptographic solutions fall short when it comes to securely processing this data and offering fine-grained access in all common sharing scenarios (such as between individual data owners, data owners and researchers, or across multiple data owners and researchers), particularly on devices with limited computing power. To solve these challenges, we introduce SAMM and SAMD—two efficient schemes that support secure multiplication and division on encrypted data using multi-key partially homomorphic encryption (PHE) and ciphertext-policy attribute-based encryption (CP-ABE). These schemes enable flexible, user-driven access control and detailed data sharing policies. Additionally, they incorporate popularity-based encrypted deduplication to improve storage efficiency without compromising data privacy.

II. LITERATURE SURVEY

Title: Privacy-preserving and outsourced multi-party k-means clustering based on multi-key fully homomorphic encryption. **Year:** 2024
Author: P. Zhang, T. Huang, X. Sun, W. Zhao, H. Liu, S. Lai, et al.
Description: Clustering algorithms are powerful tools for analyzing medical data. For example, k-means clustering can help identify the factors that contribute to the development of a disease. However, running these algorithms efficiently often requires outsourcing computation to cloud servers, which raises concerns about data privacy. Encryption is a typical solution, but cloud servers struggle to compute directly on encrypted data, especially when it comes from multiple parties.

To address this, we use multi-key fully homomorphic encryption (FHE), which allows computations on encrypted data even when different users have different encryption keys. In this paper, we build on Chen's multi-key FHE scheme and propose secure methods for computing squared Euclidean distances, comparisons, minimums, and averages—all fundamental operations in k-means clustering.

We design two secure versions of the multi-party k-means algorithm: a basic scheme and an advanced scheme. The basic scheme handles ciphertexts under different keys during multiplication by transforming them appropriately. The advanced scheme improves on this by making the transformation more efficient, significantly boosting the performance of homomorphic multiplication.Most of the heavy computation is securely offloaded to cloud servers. We also provide

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203085

formal proofs to show that our protocols are both secure and practical. Simulation results confirm that our advanced method improves the efficiency of Chen's original multi-key FHE scheme, particularly in the context of k-means clustering.

Title: An efficient ciphertext-policy weighted attribute-based encryption for the Internet of Health Things **Year:** 2023
Author: H. Li, K. Yu, B. Liu, C. Feng, Z. Qin and G. Srivastava
Description: The Internet of Health Things (IoHT) refers to a network of uniquely identifiable medical devices that are connected to the Internet and can communicate with each other. As a key part of smart health monitoring and improvement systems, IoHT offers many benefits—but it also brings significant cybersecurity challenges. One promising solution for protecting sensitive medical data is ciphertext-policy weighted attribute-based encryption (CP-WABE), which provides fine-grained access control. However, existing CP-WABE schemes often suffer from limitations such as inflexibility, high computational demands, and inefficient attribute comparison.

To tackle these problems, we propose a new method for expressing access policies using 0-1 coding technology. Building on this approach, we develop a flexible and efficient CP-WABE scheme specifically designed for IoHT environments. Our scheme not only supports weighted attributes but also allows for complex comparisons between them.

III. EXISTING SYSTEM

Most existing systems tend to prioritize either secure data processing or fine-grained access control, but rarely both together—especially when it comes to securing access over encrypted computational results. This creates a significant gap in protecting sensitive information effectively. Additionally, many current methods are too computationally heavy, making them impractical for devices with limited processing power. While partial homomorphic encryption (PHE) offers a way to compute on encrypted data, it only supports one type of operation, which limits its flexibility. A number of solutions also rely on a single public key for encrypting all users' data. This single-key approach poses serious privacy risks—if the private key is compromised, the entire dataset becomes vulnerable. On top of that, it restricts data owners from accessing their own information, which contradicts the user-centric nature of systems where data owners are expected to retain control (also known as the DO-DO scenario).

EXISTING SYSTEM DISADVANTAGES

- Limited user control over data sharing.
- Broad access with limited flexibility.
- Less Data Privacy and Scalability.
- Designed primarily for data sharing.

IV. PROPOSED SYSTEM

In this paper, we introduce two efficient and privacy-preserving schemes—SAMM and SAMD—that support multiplication and division operations, respectively, while enabling fine-grained data sharing and user-centric access control. These schemes build on the foundation of SAMA by addressing a key research gap: the lack of flexible computation over encrypted data. By integrating multiplication and division capabilities, SAMM and SAMD enhance the flexibility of secure data processing. They leverage a combination of multi-key partial homomorphic encryption (PHE) and ciphertext-policy attribute-based encryption (CP-ABE), enabling privacy-preserving computations and fine-grained access control tailored for user-centric scenarios. Importantly, these solutions are lightweight enough to operate effectively on resource-constrained devices. A key innovation of SAMM and SAMD is their ability to seamlessly support all three practical access scenarios—Data Owner to Data Owner (DO-DO), Data Requesters to Data Owner (DRs-DO), and Data Requesters to Data Owners (DRs-DOs)—without placing any extra burden on the data owner.

PROPOSED SYSTEM ADVANTAGES

- Data Privacy and Scalability more.
- Full user control with customizable, user-centric access policies.
- Fine-grained, attribute-based access control used for collaborative data processing.
- Multiple data owners and data owners' access control.

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

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203085

V. SYSTEM ARCHITECTURE

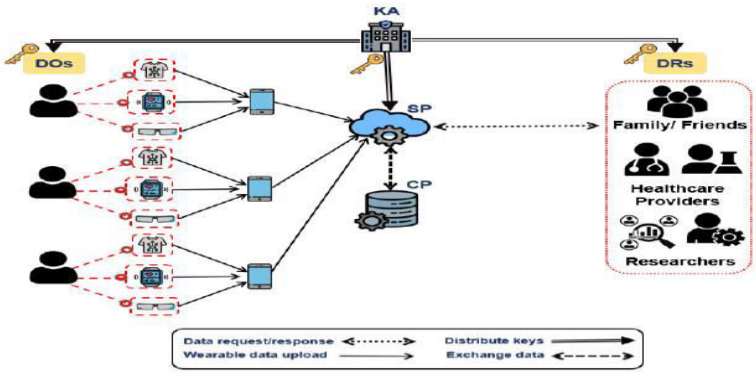


Fig1: System Architecture

The system model consists of the entities shown in Fig. 2, following the same system model. Wearables measure and collect personal data (e.g., vital signs) of DOs and transmit it to a synchronised smartphone (gateway). Data owners (DOs) are individuals who want the data collected by their wearables to be processed and the results shared with data requesters (DRs) for their own personal and/or societal benefits. A service provider (SP) stores and processes DOs' wearable data as well as manages data access requests from DRs. A computational party (CP) processes users' data (in coordination with SP) and provides access control. Data Requesters (DRs) require access to data owners' raw data or the processed results. They can be Dos themselves, family members, a friend, health providers, researchers and insurance staff. A key authority (KA) manages the generation and distribution of cryptographic key pairs.

VI .METHODOLOGIES

MODULES NAME

Modules Name:

- User Interface Design
- Data Owner (DOs)
- Data Requesters (DRs)
- Computational Party (CP)
- Key Authority (KA)
- Cloud Service Providers (CSPs)

MODULES EXPLANATION

1) User Interface Design:

The system is designed with a user-friendly interface where users begin by logging in with their username and password. New users are required to register first. Once logged in, users can easily search and view the data they're authorized to access, with the system keeping track of their activity using their username as a unique ID.

2) Data Owner (Dos):

Data Owners are individuals who generate wearable data, such as health metrics. They encrypt this data using their own public key and upload it to the cloud-based Service Provider (SP). Once uploaded, the data is securely stored and made available for computation and sharing through the system, without compromising privacy.

3) Data Requesters (DRs):

Data Requesters are individuals or entities who need access to either raw or processed data. These can include the DOs themselves, family members, doctors, researchers, or insurance staff. DRs request access to the results of computations performed on the DOs' data and are granted access only if they meet the required access policies.

4) Computational Party (CP):

The Computational Party is responsible for processing the encrypted data, often in coordination with the Service Provider. This party could be a secure cloud service or an internal department, and its main responsibilities include performing computations and enforcing access control policies to ensure only authorized users can access results.

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

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203085

5) Key Authority (KA):
The Key Authority is a trusted entity that handles the generation and distribution of cryptographic keys. It ensures that DRs receive the appropriate keys for decryption, but only if their attributes match the access control policies set by the Data Owner. This ensures that only eligible users can view sensitive information.

6) Cloud Service Providers (CSPs):
Cloud Service Providers host the Service Provider (SP), which is responsible for securely storing and processing data uploaded by DOs. The SP manages all access requests, whether it's a DO retrieving their own results or a DR requesting processed data from one or more DOs, ensuring privacy and control are maintained throughout the process.

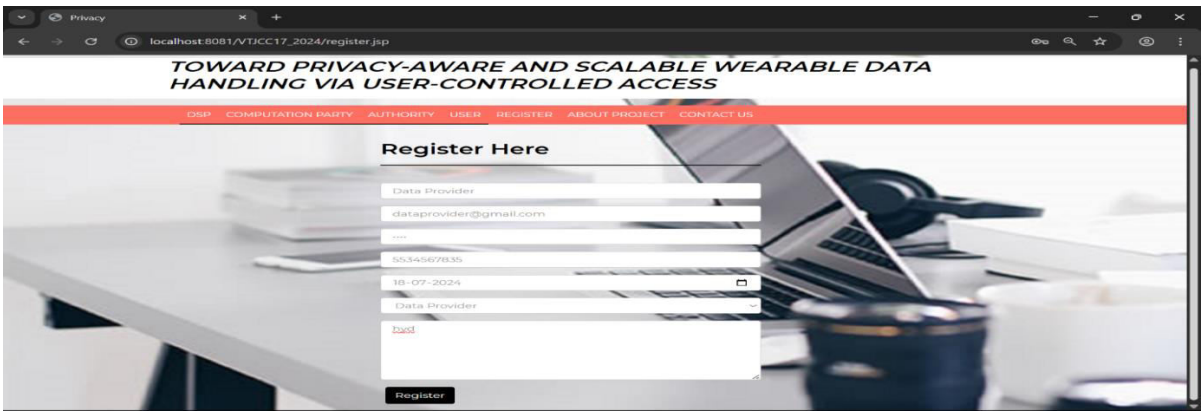
VII. ALGORITHM USED

EXISTING ALGORITHM USED:
Attribute-Based Encryption (ABE):
Attribute-Based Encryption (ABE) is an advanced form of public-key encryption that provides fine-grained access control to encrypted data. Instead of tying access to specific user identities, ABE uses attributes—like roles, departments, or clearance levels—to determine who can decrypt the data. For example, only users with the attribute "Doctor" or "Researcher" might be allowed to access certain health records. This approach is especially useful in environments like cloud storage or secure communication, where flexible and scalable access control is essential.

PROPOSED ALGORITHM USED:
CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION

- The CP-ABE is a form of public-key encryption wherein the ciphertext is linked to an access policy. User keys are constructed based on attributes, facilitating fine-grain access control. This encryption scheme comprises four fundamental algorithms: a setup algorithm (Setup), an encryption algorithm (EncABE), a key generation algorithm (KGenABE), and a decryption algorithm (DecABE).
- **Setup(s,U)→pk,mk :** Given a security parameter s and a universe of attributes U, the setup algorithm outputs the public parameters pk and a main (primary) secret key mk .
- **EncABE(pk,M,A)→C :** Given public parameters pk, a message M, and an access structure A over the universe of attributes, the encryption algorithm outputs a ciphertext C which implicitly contains A.
- **KGenABE(mk,s)→sk :** Given a main (primary) secret key mk and a set of attributes s which describe the key, the key generation algorithm outputs a private key sk .
- **DecABE(pk,C,sk)→M :** Given public parameters pk, a ciphertext C, which includes an access policy A, and a private key sk, using a decryption algorithm, a user can decrypt the ciphertext and get a message M only if the attributes associated with the private key satisfy.

VIII.EXPERIMENTAL RESULTS

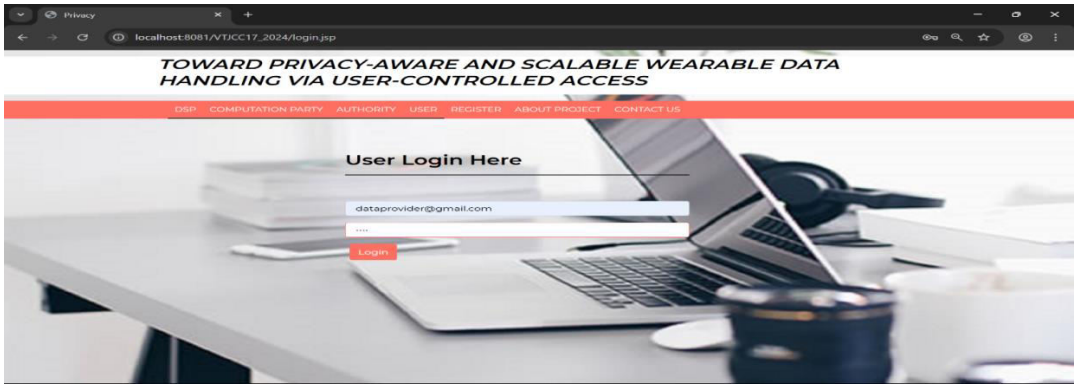


User registration page for enrolling a new data provider into the system.

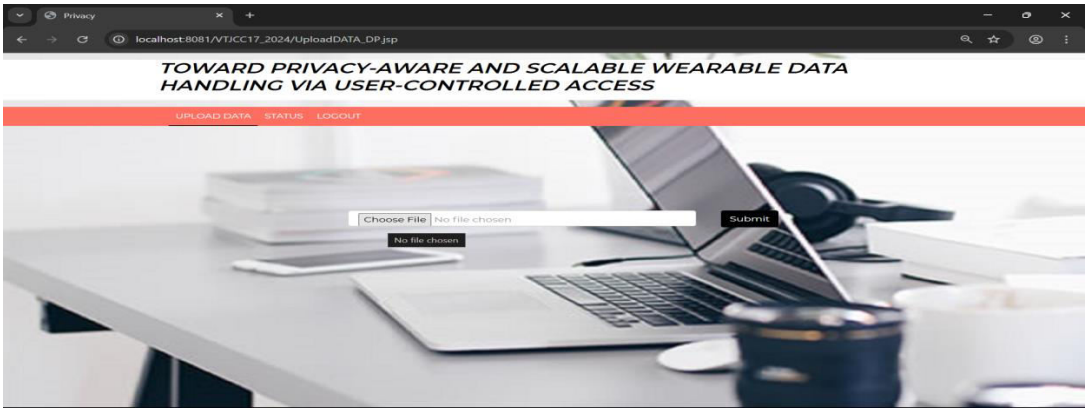
| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203085



Now the new data provider can log in as a use



After logging in as a user, the data provider should upload a .txt file

The files accepted by the DSP can be seen by the CP, and encryption is added here to protect the files from attackers.

IX. CONCLUSION

In this paper, we designed privacy-preserving and efficient multiplication and division schemes with flexible access control based on a user-centric approach called SAMM and SAMD, respectively. Both schemes utilise multi-key VP-HE and CP-ABE to accommodate modern wearable healthcare needs and address all three main use-case scenarios: DO-DO, DRs-DOs, and DRs-DOs. They allow data owners to encrypt their data only once with their public key, which reduces interaction with the cloud, accommodates resource-constrained devices, and enables data owners to

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203085

retrieve/access their outsourced data and share it with multiple DRs. Experimental evaluation demonstrates that these schemes provide superior efficiency in computation and communication. Moreover, our security analysis shows that SAMM and SAMD are secure and satisfy the specified security and privacy requirements.

X. FUTURE ENHANCEMENTS

As future work, one can focus on the following aspects: First, enhance further the overall security of the system by storing the strong secret key of the VP-HE scheme in a distributed manner (for example, by using the Shamir Secret Sharing scheme). Second, incorporate a verifiable computation feature to verify the validity and correctness of outsourced computation results computed by the cloud providers. Third, protect the DOs' access policies as they make DOs vulnerable to linkability attacks and hence may compromise individual DOs' privacy towards the cloud providers.

REFERENCES

1. K. Jastaniah, N. Zhang, and M. A. Mustafa, "Efficient user-centric privacy-friendly and flexible wearable data aggregation and sharing", arXiv: 2203.00465, 2024.
2. P. Zhang, T. Huang, X. Sun, W. Zhao, H. Liu, S. Lai, et al., "Privacy-preserving and outsourced multi-party k-means clustering based on multi-key fully homomorphic encryption", IEEE Trans. Dependable Secure Computing, vol. 20, no. 3, pp. 2348-2359, May/Jun. 2023.
3. H. Li, K. Yu, B. Liu, C. Feng, Z. Qin, and G. Srivastava, "An efficient ciphertext-policy weighted attribute-based encryption for the Internet of Health Things", IEEE J. Biomed. Health Informat, vol. 26, no. 5, pp. 1949-1960, May 2022.
4. Regulation (EU) 2016 General Data Protection Regulation, Mar. 2022, [online] Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.
5. A. Aloufi, P. Hu, Y. Song, and K. Lauter, "Computing blindfolded on data homomorphically encrypted under multiple keys: A survey", ACM Comput. Surv., vol. 54, no. 9, pp. 1-37, Dec. 2022.
6. B. Zhao, J. Yuan, X. Liu, Y. Wu, H. Hwa Pang, and R. H. Deng, "SOCI: A toolkit for secure outsourced computation on integers", IEEE Trans. Inf. Forensics Security, vol. 17, pp. 3637-3648, 2022.
7. T. Zhou, W. Liu, N. Li, X. Yang, Y. Han, and S. Zheng, "Secure scheme for locating disease-causing genes based on multi-key homomorphic encryption", Tsinghua Sci. Technol., vol. 27, no. 2, pp. 333-343, Apr. 2022.
8. J. Zhang, Z. L. Jiang, P. Li and S. M. Yiu, "Privacy-preserving multikey computing framework for encrypted data in the cloud", Inf. Sci., vol. 575, pp. 217-230, Oct. 2021.
9. J. Chen, Y. Feng, Y. Liu, W. Wu and G. Yang, "Non-interactive privacy-preserving naíve Bayes classifier using homomorphic encryption", Proc. Int. Conf. Secur. Privacy New Computing. Environments, pp. 192-203, Dec. 2021.
10. H. Pang and B. Wang, "Privacy-preserving association rule mining using homomorphic encryption in a multikey environment", IEEE Syst. J., vol. 15, no. 2, pp. 3131-3141, Jun. 2021.
11. A. Aloufi, P. Hu, H. W. H. Wong and S. S. M. Chow, "Blindfolded evaluation of random forests with multi-key homomorphic encryption", IEEE Trans. Dependable Secure Comput., vol. 18, no. 4, pp. 1821-1835, Jul. 2021.
12. Z. Hong, Z. Zhang, P. Duan, B. Zhang, B. Wang, W. Gao, et al., "Secure privacy-preserving association rule mining with single cloud server", IEEE Access, vol. 9, pp. 165090-165102, 2021.
13. D. Wenxiu, Z. Yan and R. H. Deng, "Privacy-preserving data processing with flexible access control", IEEE Trans. Dependable Secure Comput., vol. 17, no. 2, pp. 363-376, Mar./Apr. 2020.
14. V. G. Motti, Wearable Interaction, Springer, pp. 81-107, 2020.
15. W. Ding, R. Hu, Z. Yan, X. Qian, R. H. Deng, L. T. Yang, et al., "An extended framework of privacy-preserving computation with flexible access control", IEEE Trans. Netw. Service Manag., vol. 17, no. 2, pp. 918-930, Jun. 2020.
16. M. M. Islam, S. Mahmud, L. J. Muhammad, M. R. Islam, S. Nooruddin and S. I. Ayon, "Wearable technology to assist the patients infected with novel coronavirus (COVID-19)", Social Netw. Comput. Sci., vol. 1, no. 6, pp. 1-9, Nov. 2020.
17. G. Wang, R. Lu and Y. L. Guan, "Achieve privacy-preserving priority classification on patient health data in remote eHealthcare system", IEEE Access, vol. 7, pp. 33565-33576, 2019.
18. S. Sharma, K. Chen and A. Sheth, "Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems", IEEE Internet Comput., vol. 22, no. 2, pp. 42-51, Mar./Apr. 2018.
19. A. Ara, M. Al-Rodhaan, Y. Tian and A. Al-Dhelaan, "A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems", IEEE Access, vol. 5, pp. 12601-12617, 2017.
20. S. M. Mathew and S. Sabitha, "Arithmetic operations on encrypted data using fully homomorphic encryption", Proc. 14th IEEE India Council Int. Conf. (INDICON), pp. 1-6, Dec. 2017.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203085

21. S. Boukoros, N. P. Karvelas and S. Katzenbeisser, "A lightweight protocol for privacy preserving division", Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), pp. 717-722, Jun. 2017.
22. W. Ding, Z. Yan and R. H. Deng, "Encrypted data processing with homomorphic re-encryption", Inf. Sci., vol. 409, pp. 35-55, Jan. 2017.
23. F. Wang, J. Mickens, N. Zeldovich and V. Vaikuntanathan, "Sieve: Cryptographically enforced access control for user data in untrusted clouds", Proc. USENIX Symp. Networked Syst. Design Implement, pp. 611-626, 2016.
24. J. Zhou, Z. Cao, X. Dong and X. Lin, "Security and privacy in cloud-assisted wireless wearable communications: Challenges, solutions and future directions", IEEE Wireless Commun., vol. 22, no. 2, pp. 136-144, Apr. 2015.
25. J. Liu, X. Huang and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption", Future Gener. Comput. Syst., vol. 52, pp. 67-76, Nov. 2015.
26. Y. Zhang, W. Dai, X. Jiang, H. Xiong and S. Wang, "Foresee: Fully outsourced secure genome study based on homomorphic encryption", BMC Medical Informatics and Decision Making, vol. 15, pp. 1-11, Dec. 2015.
27. M. A. Mustafa, N. Zhang, G. Kalogridis and Z. Fan, "DEP2SA: A decentralized efficient privacy-preserving and selective aggregation scheme in advanced metering infrastructure", IEEE Access, vol. 3, pp. 2828-2846, 2015.
28. X. Li, D. Chen, C. Li and L. Wang, "Secure data aggregation with fully homomorphic encryption in large-scale wireless sensor networks", Sensors, vol. 15, no. 7, pp. 15952-15973, Jul. 2015.
29. S. Safavi and Z. Shukur, "Conceptual privacy framework for health information on wearable device", PLoS ONE, vol. 9, no. 12, Dec. 2014.
30. J.-H. Hoepman, "Privacy design strategies", Proc. IFIP Int. Inf. Secur. Conf., pp. 446-459, Jun. 2014.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

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