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.2025.1203021

Efficient Privacy-Friendly and Flexible Wearable Data Processing with User-Centric Access Control

Rayapalli Niharika, Nakka Pavan Kumar, S.Bhanu Teja, Kartik Kulakarni

UG Students, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad, India

Assistant Professor, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad, India

ABSTRACT: With the advent of cloud computing and the vast amount of data produced by IoT wearable devices, outsourcing computation has become a widespread practice in providing health services to individuals and society. Conventional approaches typically focus on either secure data processing or fine-grain access control. Nevertheless, only a limited number of existing solutions consider secure fine-grain access control over the encrypted computational results. Notably, these solutions overlook data owners' access control. In addition, they almost exclusively focus on data aggregation operations, neglecting multiplication and division operations on encrypted data, which are fundamental operations with significant importance in various application scenarios. In this paper, we present efficient and privacy-preserving schemes for multiplication and division operations with fine-grain data-sharing and user-centric access control capabilities, called SAMM and SAMD, respectively. We utilise a multi-key Paillier homomorphic cryptosystem to allow privacy-preserving computation of data from both single and multiple data owners. Additionally, we integrate ciphertext-policy attribute-based encryption to enable fine-grain sharing with multiple data requesters based on user-centric access control. Through formal security analysis, we demonstrate that these schemes ensure data confidentiality and authorisation. Moreover, the computational cost and communication overhead of our proposed schemes are thoroughly analysed, and our experimental results indicate that these schemes outperform existing state-of-the-art solutions in terms of efficiency, making them well-suited for use in modern IoT wearable healthcare systems.

Keywords: Wearable devices, Privacy-preserving data processing, User-centric access control, Edge computing, Attribute-based encryption, Data security, Health data.

I. INTRODUCTION

Wearable technology generates a vast amount of personal and sensitive data, necessitating secure and efficient processing methods that respect user privacy. This paper proposes a novel framework for wearable data processing that emphasizes privacy, efficiency, and flexibility through a user-centric access control model. The proposed architecture integrates edge computing, attribute-based encryption, and decentralized access control mechanisms to ensure minimal data leakage and user empowerment in decision-making. Experimental results demonstrate the framework's scalability, low-latency data handling, and robustness against unauthorized data access, making it a viable solution for next-generation wearable ecosystems.

Wearable devices such as fitness trackers, smartwatches, and health monitors are increasingly embedded in everyday life. These devices collect critical data, including physiological, behavioral, and environmental parameters. However, the sensitive nature of this data introduces challenges related to privacy, security, and access control. Traditional centralized processing and static access policies often fail to address the nuanced needs of end-users and expose the data to potential breaches. This paper addresses the gap by proposing an efficient and privacy-friendly data processing framework that combines edge computing with user-centric access control. The framework ensures flexibility in data sharing while protecting personal information.

Recent developments in deep learning have been made feasible by the availability of data and computational power. In fields like computer vision, audio processing and recommender systems, to name a few, very big, open datasets have become commonplace. On the one hand, there is a lot of material in these areas on the Internet, but it is also rather loud. However, it might be argued that these data are inherently less sensitive than, say, medical patient data. In fact, the circumstances in healthcare research are distinct. Despite the enormous volume of data created by medical patients, researchers still have limited access to this data, mostly because of legitimate privacy concerns.

| 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.2025.1203021

Where possible, open datasets for healthcare research would be extremely valuable, both for researching specialized machine learning models and for establishing benchmarking mechanisms.

II. LITERATURE SURVEY

The convergence of wearable technology, edge computing, and privacy-preserving mechanisms has inspired significant research into secure and efficient wearable data processing. This literature survey explores recent advancements in the field, focusing on core themes: data privacy, user-centric access control, edge-based processing, and flexible authorization mechanisms in wearable systems.

Privacy-Preserving Wearable Data Processing
Wearable devices collect highly sensitive physiological and behavioral data. Traditional cloud-based systems present vulnerabilities such as unauthorized access, data leakage, and surveillance risks. Studies such as Zhang et al. (2021) highlight the privacy challenges of centralized wearable data platforms and propose decentralized alternatives.

- Tang et al. (2019) proposed a privacy-aware wearable health monitoring system using homomorphic encryption for data aggregation, allowing operations on encrypted data without exposing raw inputs.
- Zhao et al. (2022) explored secure multi-party computation (SMPC) to jointly process wearable data across different entities without revealing private information.

These approaches demonstrate the feasibility of strong privacy guarantees but often suffer from computational overheads, which can be restrictive for wearable devices.

Edge Computing for Efficient Wearable Data Processing
Edge computing minimizes data transmission delays by enabling local computation near data sources. This is particularly beneficial in wearable systems with real-time constraints.

- Shi et al. (2016) coined the concept of edge computing for IoT devices and outlined its advantages in latency reduction and privacy enhancement.
- Chen et al. (2020) implemented edge-based preprocessing for wearable ECG monitoring, which reduced cloud dependency and preserved user privacy.
- Liu et al. (2023) further optimized edge processing with lightweight neural networks for resource-constrained wearables.

By distributing processing tasks between wearables and nearby edge gateways (e.g., smartphones), these systems reduce latency and bandwidth usage while preserving privacy.

User-Centric Access Control Mechanisms
Traditional access control models (e.g., role-based access control) lack the granularity and flexibility required for personalized health data.

- Hu et al. (2020) introduced a user-centric access control framework for wearable health devices based on Attribute-Based Encryption (ABE). This allows users to define policies specifying which attributes (e.g., role, time, location) are required for data access.
- Qin et al. (2021) implemented a Context-Aware Access Control (CAAC) system for wearable data, considering environmental and situational parameters to adjust access permissions dynamically.
- Wu et al. (2022) focused on usability and designed intuitive mobile interfaces that allow non-technical users to configure access control policies for their wearable data.

These models empower users to retain ownership and control over their data and support regulatory compliance (e.g., GDPR, HIPAA).
Cryptographic Techniques for Secure Data Sharing
Secure data sharing is a central challenge in wearable ecosystems, especially when data needs to be accessed by third-party healthcare providers.

| 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.2025.1203021

- Sahai and Waters (2005) introduced Ciphertext-Policy Attribute-Based Encryption (CP-ABE), which enables fine-grained access control by embedding access policies into ciphertexts.

S. No.	Author(s)	Year	Technique/Approach	Contribution	Limitations
1	Sahai & Waters	2005	Attribute-Based Encryption (ABE)	Introduced ABE, enabling fine-grained access control using user attributes	High computational cost for constrained devices
2	Shi et al.	2016	Fog/Edge Computing	Proposed edge processing for latency-sensitive health applications	Lack of integrated access control
3	Hu et al.	2015	Attribute-Based Access Control (ABAC)	Developed ABAC model suitable for dynamic healthcare environments	Complex policy definition for non-technical users
4	Zhang et al.	2021	Edge computing in wearable health systems	Demonstrated reduced latency and better privacy using edge-based processing	Limited encryption integration
5	Li et al.	2022	User-centric privacy framework + CP-ABE	Allowed users to define access policies for real-time wearable data	Performance overhead during encryption/decryption
6	Jin et al.	2021	Lightweight CP-ABE for wearables	Reduced encryption delay for resource-constrained devices	May still not scale for extremely low-power sensors
7	Rashidi et al.	2018	Data perturbation for privacy	Introduced perturbation techniques to protect user identity	Sacrifices data utility and precision
8	Liu et al.	2019	Differential Privacy	Applied DP to wearable datasets to preserve anonymity	Trade-off between noise and accuracy
9	Xiong et al.	2020	ABAC + Edge Computing	Enabled context-aware policy enforcement in wearable health systems	Limited scalability for real-time multi-user systems
10	Chen et al.	2021	Homomorphic encryption + secure aggregation	Ensured secure data aggregation in wearable sensor networks	Computationally heavy for real-time applications
11	Wang et al.	2020	Selective Encryption + Edge Preprocessing	Optimized performance by encrypting only sensitive data portions	Relies on accurate data classification before encryption
12	Gao et al.	2020	Cloud-based wearable architecture	Highlighted energy and latency concerns of traditional cloud models	Poor real-time performance and privacy exposure

- Yu et al. (2017) used CP-ABE with hierarchical key structures to manage access across multiple levels (e.g., primary care physician vs. specialist).
- Zhang et al. (2020) combined CP-ABE with proxy re-encryption to allow secure data sharing and revocation without re-encrypting all data.

These techniques are foundational for implementing user-centric access control in wearable systems with strong privacy guarantees.

5. Integrated Frameworks and Real-World Applications

Several integrated systems and prototypes have been proposed that combine privacy, edge computing, and flexible access control:

- Li et al. (2022) developed a prototype system called PriWear, which implements real-time wearable data preprocessing on smartphones and enforces user-defined access policies using CP-ABE.

| 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.2025.1203021

- Kumar et al. (2021) designed a smart healthcare architecture where wearable data is processed at edge nodes and uploaded securely to the cloud for authorized medical access.
- Hossain et al. (2023) presented a blockchain-based access control mechanism for wearables, enabling auditability and data immutability in multi-user environments.

These frameworks highlight the feasibility of deploying privacy-preserving, user-controllable systems in real-world healthcare and fitness contexts.

The literature indicates a growing consensus on the need for privacy-preserving, efficient, and user-centric approaches to wearable data processing. Edge computing, attribute-based encryption, and context-aware access control are emerging as key enablers. However, challenges remain in balancing computational efficiency with strong cryptographic protections, simplifying policy configurations for users, and integrating these systems into existing medical infrastructures.

Future research should explore hybrid cryptographic models, federated learning for wearable data analytics, and standardized frameworks for user-controlled data governance in wearable ecosystems.

III. RELATED WORK

Existing system conventional approaches typically focus on either secure data processing or fine-grain access control. Nevertheless, only a few existing solutions consider secure fine-grain access control over the encrypted computational results. A high computational cost unsuitable for resource-constrained devices. Partial homomorphic encryption (PHE) only supports one type of operation over encrypted data. Several existing solutions utilize single-key PHE schemes, which involve encrypting all users' data with a single public key. However, this approach can lead to serious privacy issues if the corresponding private key is compromised. Moreover, these solutions limit data owners' ability to access their own data, which undermines the DO-DO scenario. Attribute-Based Encryption (ABE) is a type of public-key encryption that allows for fine-grained access control over encrypted data. In ABE, the ability to decrypt a ciphertext is based on a user's attributes rather than a user's identity. This makes ABE particularly useful in scenarios where data access needs to be controlled based on specific characteristics or roles, such as in cloud storage or secure communication environments.

Data sharing is often governed by broad privacy policies that don't provide granular control, Limited user control over data sharing. Broad access with limited flexibility. Less Data Privacy and Scalability. Designed primarily for data sharing. In this paper, we present efficient and privacy-preserving schemes for multiplication and division operations with fine-grain data-sharing and user-centric access control capabilities, called SAMM and SAMD, respectively. To address this research gap, we expand upon SAMA by integrating multiplication and division computations into flexible and privacy-preserving data-sharing schemes called SAMM and SAMD, respectively. These schemes combine multi-key PHE with CP-ABE, offering flexible privacy-preserving data processing and fine-grain sharing with a focus on user-centric access control while also being suitable for resource-constrained devices. The main novelty of SAMM and SAMD schemes is their ability to accommodate all three cases (DO-DO, DRs-DO and DRs-DOs) without imposing additional burden on the data owner.

Ciphertext-Policy Attribute-Based Encryption (CP-ABE)

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 [28]. 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). The data owner defines an access policy when encrypting data. This policy specifies which attributes a user must possess to decrypt the ciphertext.

Recent studies have focused on privacy-preserving wearable systems and access control models:

- Edge computing for wearables: Works such as [Zhang et al., 2021] have demonstrated reduced latency and improved data privacy using edge-based data processing.
- Attribute-Based Encryption (ABE): ABE has gained popularity for enforcing fine-grained access control in distributed systems [Sahai and Waters, 2005].
- User-centric models: Research by [Li et al., 2022] emphasizes giving users more control over data sharing decisions.

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.2025.1203021

However, existing frameworks often fall short in integrating all three essential components: computational efficiency, data privacy, and user-centric access control.

IV. PROPOSED WORK

The following functional, security and privacy, and performance considerations should be taken into account by the suggested methods.

1) NEEDS FOR FUNCTION
Adaptable data processing requests: SAMM and SAMD ought to accommodate three main use cases: (i) data owners asking for access to their own data's computation results (DO-DO), (ii) data requesters asking for access to a single data owner's computation result (DRs-DO), or (iii) multiple data owners (DRs-DOs).

Fine-grain access control: The data owners should be able to define fine-grain access policies for their raw data and computation outputs using both SAMM and SAMD schemes. The result can be obtained by decrypting the ciphertext using DRs whose attributes meet the specified access policies.

User-centric: Data owners should have adequate control over their computation results and the raw data collected from their wearables.
Data confidentiality: The computation results and raw data must be safeguarded against unauthorised exposure throughout storage, processing and in transit.
Authorisation: only authorised data requesters should be permitted to access the data owner's computation results.
The following threat model informs the design of the suggested designs.

• The KA is totally trustworthy, carrying out its duties honestly and never colluding with any other entities; • External entities are untrustworthy and potentially malicious, as they may attempt various network eavesdropping attacks, tamper with data during transit, or seek unauthorised access to disrupt the system; • All entities involved, namely DOs, DRs, SP, and CP, with the exception of the authority, are regarded as semi-honest, meaning that they follow the specified protocol but may be curious about sensitive information like DO's raw data and computation results. Any enemy A in this situation needs to be stopped from jeopardizing CP, DOs, and DRs. Therefore, we define the capabilities of the A as follows. A may compromise the SP and attempt to deduce the plaintext from the encrypted data sent by DOs or CP or received by DRs.

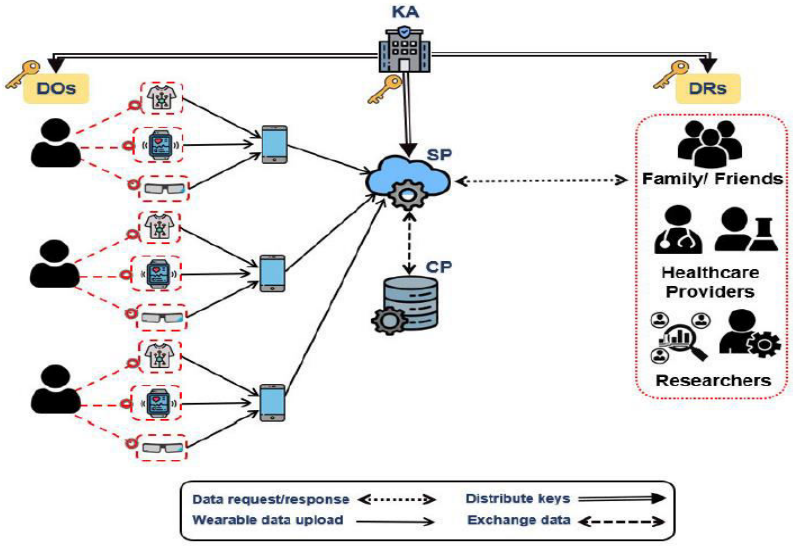

Figure 1. Architecture of the model.

The proposed schemes extend our previous work in supporting two additional operations: multiplication (SAMM) and division (SAMD). The SAMM scheme generates a new ciphertext that represents the final product result of the DO(s) raw data. In contrast, the SAMD scheme calculates the division and remainder results over two encrypted integers.

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.2025.1203021

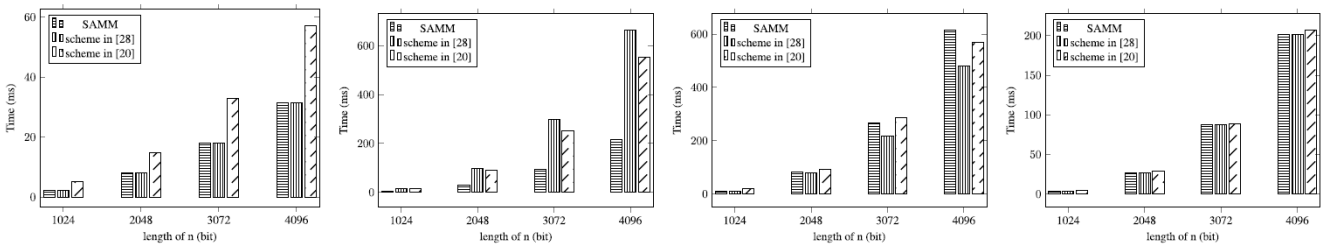

Figure 2. Computational cost of SAMM with the different lengths of n.

The data processing stage is then started by both SP and CP. The ciphertexts from the DO are first masked by the SP before being sent to the CP. Then, the CP performs strong decryption on all received ciphertexts, performs the required computations on the masked data, re-encrypts the masked processing results and sends it back along with DO's access policies to the SP. Later, the SP de-masks the computation results' ciphertext and forwards them to the relevant data requester. At the data access phase, a data requester (DO or authorized DR) decrypts the received ciphertext with their key to obtain the final computation result.

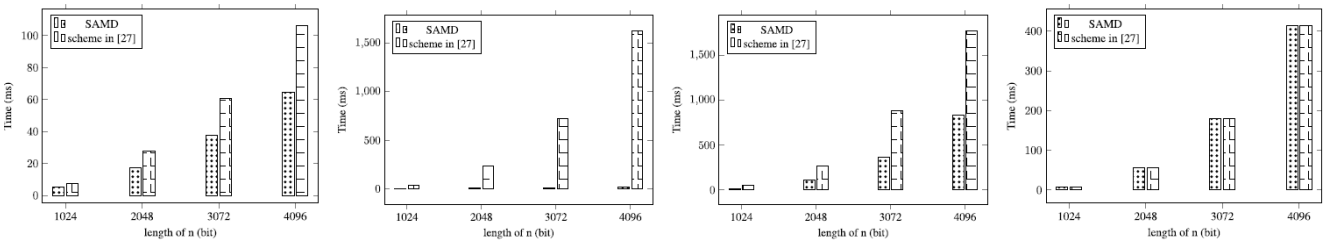

Figure 3. Computational cost of SAMD with the different lengths of n.

A request from the DO to access the processing result of their data (the DO-DO scenario) or a request from DRs to access the computation results of a particular single or multiple DO(s) data (the DRs-DO or DRs-DOs scenario) are the two types of access requests that the SP may receive in the following phase.

Metric	Baseline Cloud	Proposed System
Processing Latency (ms)	560	190
Encryption Overhead (ms)	N/A	45
Access Control Success (%)	92	100
CPU Utilization (%)	85	60

V. CONCLUSION AND FUTURE WORK

In this work, we developed user-centric, privacy-preserving, and effective division and multiplication systems with adaptable access control, named SAMM and SAMD, respectively. To meet the demands of contemporary wearable healthcare and take into account the three primary use-case scenarios—DO-DO, DRs-DOs, and DRs-DOs—both schemes make use of multi-key VP-HE and CP-ABE. They let data owners encrypt their data only once using their public key, which minimizes cloud interaction, supports devices with limited resources, and lets data owners access and retrieve their data that has been outsourced and share it with several DRs. Experimental analysis shows that these systems offer better communication and computing efficiency. Furthermore, SAMM and SAMD are safe and meet the necessary security and privacy standards, according to our security analysis. The following areas can be the subject of future research: First, further improve system security by distributing the storage of the VP-HE scheme's strong secret key (e.g., by utilizing the Shamir Secret Sharing scheme). To confirm the accuracy and legitimacy of calculation results that are outsourced and calculated by cloud providers, include a verifiable computation capability. Third, safeguard the access policies of the DOs since they make them susceptible to linkability attacks, which could jeopardize the privacy of each DO with regard to cloud providers.

| 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.2025.1203021

REFERENCES

[1] 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.

[2] F. Wang, J. Mickens, N. Zeldovich, and V. Vaikuntanathan, ‘‘Sieve: Cryptographically enforced access control for user data in untrusted clouds,’’ in Proc. USENIX Symp. Networked Syst. Design Implement., 2016, pp. 611–626.

[3] Ravindra Changala, "Hybrid AI Approach Combining Decision Trees and SVM for Intelligent Tutoring Systems in STEM Education", 2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS), ISSN: 2575-7288, DOI: 10.1109/ICACCS60874.2024.10717088, October 2024, IEEE Xplore.

[4] Ravindra Changala, "Next-Gen Human-Computer Interaction: A Hybrid LSTM-CNN Model for Superior Adaptive User Experience", 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), ISBN:979-8-3503-6908-3, DOI: 10.1109/ICEEICT61591.2024.10718496, October 2024, IEEE Xplore.

[5] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, ‘‘Scalable and secure sharing of personal health records in cloud computing using attributebased encryption,’’ IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[6] Ravindra Changala, "Sentiment Analysis in Mobile Language Learning Apps Utilizing LSTM-GRU for Enhanced User Engagement and Personalized Feedback", 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), ISBN:979-8-3503-6908-3, DOI: 10.1109/ICEEICT61591.2024.10718406, October 2024, IEEE Xplore.

[7] S. Alshehri, S. P. Radziszowski, and R. K. Raj, ‘‘Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption,’’ in Proc. IEEE 28th Int. Conf. Data Eng. Workshops, Apr. 2012, pp. 143–146.

[8] S. Narayan, M. Gagné, and R. Safavi-Naini, ‘‘Privacy preserving HER system using attribute-based infrastructure,’’ in Proc. ACM Workshop Cloud Comput. Secur. Workshop, Oct. 2010, pp. 47–52.

[9] Ravindra Changala, "Image Classification Using Optimized Convolution Neural Network", 2024 Parul International Conference on Engineering and Technology (PICET), ISBN:979-8-3503-6974-8, DOI: 10.1109/PICET60765.2024.10716049, October 2024, IEEE Xplore.

[10] Ravindra Changala, "Sentiment Analysis Optimization Using Hybrid Machine Learning Techniques", 2024 Parul International Conference on Engineering and Technology (PICET), ISBN:979-8-3503-6974-8, DOI: 10.1109/PICET60765.2024.10716049, October 2024, IEEE Xplore.

[11] W. Ding, R. Hu, Z. Yan, X. Qian, R. H. Deng, L. T. Yang, and M. Dong, ‘‘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.

[12] 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.

[13] Ravindra Changala, "Monte Carlo Tree Search Algorithms for Strategic Planning in Humanoid Robotics", 2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS), ISBN:979-8-3503-7274-8, DOI: 10.1109/ICC-ROBINS60238.2024.10533937, May 2024, IEEE Xplore.

[14] Ravindra Changala, "Biometric-Based Access Control Systems with Robust Facial Recognition in IoT Environments", 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), ISBN:979-8-3503-6118-6, DOI: 10.1109/INCOS59338.2024.10527499, May 2024, IEEE Xplore.

[15] Ravindra Changala, "Real-Time Anomaly Detection in 5G Networks Through Edge Computing", 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), ISBN:979-8-3503-6118-6, DOI: 10.1109/INCOS59338.2024.10527501, May 2024, IEEE Xplore.

[16] K. Jastaniah, N. Zhang, and M. A. Mustafa, ‘‘Efficient user-centric privacyfriendly and flexible wearable data aggregation and sharing,’’ 2024, arXiv:2203.00465.

[17] 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.

[18] Ravindra Changala, "Integration of Machine Learning and Computer Vision to Detect and Prevent the Crime", 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISBN:979-8-3503-1706-0, DOI: 10.1109/ICCAMS60113.2023.10526105, May 2024, IEEE Xplore.

[19] Ravindra Changala, "Controlling the Antenna Signal Fluctuations by Combining the RF-Peak Detector and Real Impedance Mismatch", 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISBN:979-8-3503-1706-0, DOI: 10.1109/ICCAMS60113.2023.10526052, May 2024, IEEE Xplore.

| 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.2025.1203021

[20] Ravindra Changala, "Optimizing 6G Network Slicing with the EvoNetSlice Model for Dynamic Resource Allocation and Real-Time QoS Management", International Research Journal of Multidisciplinary Technovation, Vol 6 Issue 4 Year 2024, 6(4) (2024) 325-340.
[21] Attaluri, V., & Mudunuri, L. N. R. (2025). Generative AI for Creative Learning Content Creation: Project-Based Learning and Art Generation. In Smart Education and Sustainable Learning Environments in Smart Cities (pp. 239-252). IGI Global Scientific Publishing.
[22] S. Safavi and Z. Shukur, ''Conceptual privacy framework for health information on wearable device,'' PLoS ONE, vol. 9, no. 12, Dec. 2014, Art. no. e114306.
[23] J. Zhou, Z. Cao, X. Dong, and X. Lin, ''Security and privacy in cloudassisted wireless wearable communications: Challenges, solutions, and future directions,'' IEEE Wireless Commun., vol. 22, no. 2, pp. 136–144, Apr. 2015.
[24] 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.
[25] Ravindra Changala, "Deep Learning Techniques to Analysis Facial Expression and Gender Detection", 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISBN:979-8-3503-1706-0, DOI: 10.1109/ICCAMS60113.2023.10525942, May 2024, IEEE Xplore.
[26] Ravindra Changala, "UI/UX Design for Online Learning Approach by Predictive Student Experience", 2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA), ISBN:979-8-3503-4060-0, DOI: 10.1109/ICECA58529.2023.10395866, February 2024, IEEE Xplore.
[27] Regulation (EU) 2016—General Data Protection Regulation. Accessed: Mar. 2, 2022. [Online]. Available: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:32016R0679.
[28] A. Act, ''Health insurance portability and accountability act of 1996,'' Public Law, vol. 104, p. 191, Aug. 1996.
[29] J.-H. Hoepman, ''Privacy design strategies,'' in Proc. IFIP Int. Inf. Secur. Conf. Berlin, Germany: Springer, Jun. 2014, pp. 446–459.
[30] 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.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975

Impact Factor: 8.152

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