International Journal of Reconfigurable and Embedded Systems (IJRES)
Vol. 15, No. 1, March 2026, pp. 119~129
ISSN: 2089-4864, DOI: 10.11591/ijres.v15.i1.pp119-129

Inquisitive biometric feature analysis and implementation for recognition tasks using camouflaged segmentation with AI and IoT

Mahesh Shankarrao Patil[1], Harsha J. Sarode[2], Abhijit Banubakode[3], Prakash Tukaram Patil[4], Nutan Patil[2], Vijayakumar Varadarajan[5], Deshinta Arrova Dewi[6]
[1]School of Bioengineering Sciences and Research, MIT ADT University, Pune, India
[2]Department of Electronics and Telecommunication Engineering, Nutan Maharashtra Institute of Engineering and Technology, Pune, India
[3]Department of Computer Science and Engineering, Pimpri Chinchwad University, Pune, India
[4]Department of Electronics and Telecommunication Engineering, Jayawantrao Sawant College of Engineering, Pune, India
[5]Swiss School of Business and Management, Geneva, Swizerland
[6]Faculty of Data Science and Information Technology, INTI International University, Nilai, Malaysia

Article Info

Article history:

Received Jan 7, 2025
Revised Jun 10, 2025
Accepted Jan 26, 2026

Keywords:

Biometric recognition
Camouflaged segmentation
Low-power internet of things devices
Machine-learning
Process innovation

ABSTRACT

A vital role in reconfigurable and embedded systems which are deployed in smart environements and healthcare monitoring applications is played by human activity recognition (HAR). However, the potential leakage of sensitive user attributes raises serious privacy issues due to collection of data from the end devices and it needs to be transmitted to more powerful platforms for inference. Addressing this key challenge is principally crucial for resource-constrained embedded systems where efficiency of energy is a chief design requirement. The aim of this paper is present an energy-aware, privacy-preserving HAR framework appropriate for low-power embedded platforms. A machine learning–based camouflaged signal segmentation technique is proposed to transform the data collected from the sensor by eliminating sensitive information while preserving activity-relevant features. For characterization of trade off between the energy consumption and accuracy of recognition, parameters are extensively tuned by careful optimization in this proposed model. Experimental evaluations demonstrate that the method significantly reduces the inference of sensitive attributes such as gender, age, height, and weight, with minimal impact on HAR accuracy. Furthermore, the system supports configurable trade-offs between energy usage and classification performance, making it suitable for implementation on low-power embedded devices.

Corresponding Author:

Mahesh Shankarrao Patil
School of Bioengineering Sciences and Research, MIT ADT University
Pune, India
Email: mpink.patil@gmail.com

1. INTRODUCTION

The increase in associated wearable devices has experienced noteworthy strides in last few years because of substantial technical developments in design of system-on-chip (SoC). The wearable devices market size has touched the 71.91 billion USD in the year 2023, this is according to the marte report of wearable technology [1], [2]. A wide range of products such as hearing aids, textiles, patches, rings, lenses, helmets, shoes, chest straps, smartbands, and smartwatches are encompassed by wearable devices. Out of these, vast majority of current market is covered by the smartbands and smartwatches [3]. From the perspective of the hardware, multiple core processors of 64 bit are found in traditional smartwatches to 32-bit or 16-bit energy efficient microcontrollers exists in rings, shoes, smartbands and other similar devices.

Gathering of huge amounts of information lead by acceptance of wearable internet of things (IoT) devices which enables advanced applications in different areas [4].

Significant attention among these given applications has gained by human activity recognition (HAR) because of its capability in elderly care [5], healthcare monitoring and smart homes systems [6]. With the start of voice assistants, ‘‘the era of ubiquitous listening’’ [7] in 2014 defined by MIT, that suffer from risks of privacy arising from 2 causes, i) sharing of raw audio signal from the service providers of cloud that may elevate inference attacks potential and ii) sensitive paralinguistic information contained by those signals [8]. Indeed, paralinguistic information can be used by models of deep acoustic for inferring sensitive and personal data like health status, ethnicity, mood, age, gender and speaker identity. For using ‘‘the era of ubiquitous listening’’ in parallelism in HAR domain, it can be said that we are coming in ‘‘the era of ubiquitous motion tracking’’. Serious concerns regarding individual privacy are raised because of tremendous amount of personal information is captured by these devices which integrate multiple sensors like magnetometers, gyroscopes and accelerometers. For example, the data captured by these devices are continuously transmitted to a remote server for identification of user activities like running, jogging, and walking. However, different factors such as weight, gender and age of an individual play role when they perform the activities differently. For instance, a person may walk slower if his body weight is high compared to a person having lower body weight. Determination of personal information like height, gender, age and weight can be allowed to be interpreted by the sensor signal without user’s explicit permission or conscious participation which becomes a possible risk in spite of being generally perceived as non-threatening [9]–[11].

Sensor’s data transmission directly without measures of protection of privacy is not accepted to safeguard privacy. However, activity recognition accuracy maintenance is crucial so as not to make application unusable. Privacy preservation techniques are surveyed by Antwi-Boasiako *et al*. [12] in recent times in distributed deep learning. Several stages give rise to issues of privacy in such scenarios like model training, feature extraction and dataset creation. Issues of privacy at the training stages are focused on this study although some privacy concerns are highlighted which might appear at the inference stage. Secure multi-party computations (SMPC), differential privacy (DP), and homomorphic encryption (HE) are mentioned by authors as methods of privacy preservation. However, it is important to highlight that Camouflaged segmentation and generative adversarial networks (GANs) are few examples of privacy preservation strategies employed. Perturbation and transformation methods may be grouped with all these methods. For privacy advancement in various domains of application such as face de-identification [13] and speech recognition [8] are looked by accepting camouflaged segmentation. Camouflaged segmentation are neural networks of neural which are planned to wrap (encode) the input into a telling representation, and in a subsequent phase decoding of input is done in a way that output is same as much as possible to the original input. In Bank *et al*. [14], most used camouflaged segmentation technique is surveyed by authors in this article, that highlights technique of regularization i.e., meaningfulness of compressed representation of input is ensured by camouflaged segmentation.

To take benefits of both the methodologies, GANs [15], other methods are used in combination of Camouflaged segmentation. Camouflaged segmentation application for enhancement of privacy in indicators from sensors is not a novel contribution; but in the previous studies focus was given on suggesting mechanism of transformation of data to anonymizing information of sensor [16]–[18], whereas these mechanisms are employed by others for anonymizing a single sensitive variable, such as gender [19]. The design of a multiple attributes obfuscator not considered by those works nor do they address deployment of such systems on real, low-power, resource-constrained devices; hence, overseeing obfuscation time factors of energy consumption. An energy-efficient strategy for privacy preservation devoted to devices constrained of low power is proposed in this article and which is based on machine-learning. High accuracy is maintained in activity recognition while covering user’s sensitive information Camouflaged segmentation are trained. The conventional working of biometric with AI and IoT is summarised in Figure 1. The flowchart represents the conventional working of a biometric face recognition–based access control system. The process begins when a person stands in front of the camera and a facial image is captured. The acquired image is then compared with the stored facial templates available in the database. A decision module evaluates whether the captured face matches an existing record. If a match is confirmed, access is granted by unlocking the door and the process terminates. If no match is found, access is denied and the system ends the authentication attempt.

For prevention of undesirable implications of various attributes of privacy such as age, weight, height, and gender from inertial sensors signal acquisition; examination of proposed methodology and architecture of model is investigated via parameter tuning is provided; possibility of transferring this architecture on systems of constraints is demonstrated on real low power platform for camouflaged segmentation obfuscation; efficacy and effectiveness of our method along with various dimensions such as

consumption of energy, capabilities of privacy preservation and HAR model's accuracy is characterised using wide experiment sets.

The organization of this paper is mentioned here: summarize current state-of-the-art research related to our study in section 2; in section 3, we introduce the learning architecture and system design choices proposed as a solution; in section 4, we illustrate the experimental setup adopted for performance assessment; in section 5, we describe and discuss the experimental results; in section 6, we conclude by summarizing the key findings of our investigation.

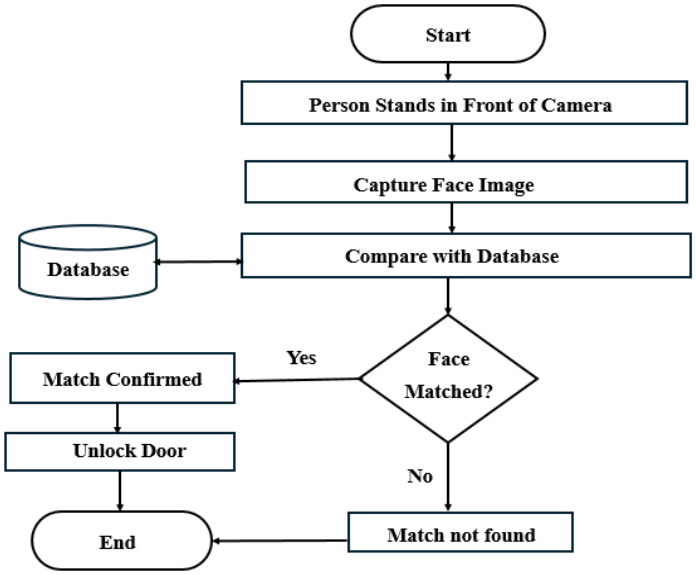

Figure 1. Conventional working of biometric with AI and IoT

2. LITERATURE REVIEW

The leakage of sensitive and personal information is avoided in privacy preservation. The data of sensor captured from wearable IoT devices having low-power is utilized by the HAR systems to constantly understand what a person is doing. Hence, severe concern is posed by the privacy of individuals. The privacy preservation in recognition of vision-based activity related work is not considered in this paper. Preservation of privacy in recognition of inertial sensor-based activity is the focus of this paper. The research community have investigated many privacy preserving strategies. A scheme which is based on two stage randomization techniques for improvement of preservation of privacy in collaborative deep learning is proposed by Lyu *et al*. [20]. A two-stage approach is implemented by them, in the first part, a non-linear function to disturb information is applied and in subsequent part a random projection matrix of row-orthogonal is used to compress the data to keep the Euclidean distance amongst braces of information points stochastically. Hopeful outcomes offering an optimal trade-off between accuracy and privacy recognition is shown by this approach.

Methods of transformation and perturbation noise both combine a framework proposed by Zhang *et al*. [21]. Sensors raw information is transformed into a newer presentation with a random noise "style", which is sensitive data and raw data's "content" that is information of activity. 2D convolutional neural networks are used by them for training sensors raw information for gathering information of target and then transformation networks are trained for avoiding leakage of information while keeping target data. Retaining information of target and protecting user sensitive data keeping accuracy drop of recognition low in this framework simultaneously. Data of user is differentially private and such HAR framework is proposed by Garain *et al*. [22]. For accomplishing this, mechanism of linear shifting was used when noise is added to original data for performing uniform noise distribution. Noise insertions of different levels are used for measurement of recognition and privacy by them. However, multilayer perceptron is used as classifier rather than deep learning and use sensitive information as user identification only. They show that significant drop in accuracy of user identifies is observed when data of accelerometer data is corrupted with noise and high accuracy is maintained by HAR.

Minimizing recognition of age and gender identification keeping activity recognition maximum is nondominated sorting genetic algorithm III are leveraged by Climent-Pérez and Florez-Revuelta [23].

Finding the best features is the main objective of evolutionary algorithm for achieving HAR as accurate as possible while hiding age and gender. Despite a significant reduction in accuracy is experienced by age and gender recognition, because of multidimensionality of problem non negligible drop on recognition of activity is observed. The solution can be optimum for some dimensions but sub optimum for other dimensions.

Two frameworks depend upon various adversarial training frameworks for private attribute obfuscation inference is proposed by Menasria *et al*. [24]. In part first, personal GAN1 which depend upon architecture of dual discriminator. Private GAN1 transforms, camouflages crucial parameters which are associated to personal features while retaining the non important features which are associated to non sensitive parameters. PGAN2, in the subsequent part, generation of new information with a least correlation to the sensitive features of distribution by leveraging the random distribution instead of transformation. Two estimator's architecture and one discriminator is the basis of PGAN2. Two strategies were tested by authors by anonymizing one of more crucial data at a time such as height, weight, age and gender. In concealing the sensitive information and features. PGAN2 is further operative than PGAN1 is the conclusion given in Menasria *et al*. [24]. A camouflaged segmentation, to camouflage private data in analysis of time-series data, develops a privacy-preserving platform mentined in Malekzadeh *et al*. [25]. This approach is based on the introduction of a deep Camouflaged segmentation architecture on which a real-time algorithm could excerpt valuable features from data of time-series; replacing sensitive information with non sensitive information is learned by this algorithm where required data is kept in information. Replacement camouflaged segmentation is the name of this method. Training of RAE system for learning to transform features of discrimination which are equivalent to sensitive interpretations into features identified in non-sensitive interpretations. A GAN was used by the authors for proving the efficacy of their method, which shows that RAE's output produced is vague compared to real non-sensitive data. The accuracy of recognition is retained simultaneously by RAE is proved by them.

Consequently, extension of their previous study is extended by the Malekzadeh *et al*. [26] by suggesting the guardian estimator neutralizer (GEN) framework, inteneded to present individual sensor data's transformed version. A learning framework like guardian component, which is based upon the camouflaged segmentation is outlined in their previous effort as stated, the predictor is a convolutional neural network of multi tasks in control of calculating algorithms accuracy for inferences of sensitive and not sensitive transformed data. The camouflaged segmentation is helped by the neutralizer which is an optimizer. Here the user's gender is considered as sensitive information by the authors. A good compromise between accuracy and utility is provided by GEN is proved by them. Delgado-Santos *et al*. [27] proposed a similar approach to style and content designing GaitPrivacyON. Two modules are present in the GaitPrivacyON. Two convolutional camouflaged segmentations are included in the first modules which provide weights and have a similar architecture. To extract meaningful info from converted data, these camouflaged segmentations are trained. Gait verification system is the second module; it consists of recurrent networks of neural united with convolutional neural network which supports system retain its helpfulness in foremost job of confirmation of gait. As the gait biometry confirmation work slightly reduced, good results are obtained. Contrary to this, protection of private information, here, gender, and activity is improved.

The problems which are seen from previous studies are conventional systems of biometric recognition face issues in surroundings where biometric features are occluded partially or masked by complex backgrounds [28], Traditional techniques of image segmentation frequently fail to distinguish accurately where recognition accuracy is reduced for similar biometric features, uncontrolled and outdoor surroundings are where adaptability is lacked by biometric systems in real time and dynamic conditions [29], for enhancing and extracting biometric features in noisy or camouflaged environments AI driven intelligent segmentation use is lacking and scalability and effectiveness of traditional recognition applications in surveillance and security is limited by absence of system integrating advanced segmentation, IoT, and AI [30]. The inspiration of our work is from Malekzadeh *et al*. [26], the idea of adopting the camouflaged segmentation is leveraged by us, which keeps the original input aspects that are relevant and useful to the recognition of the activity while concealing sensitive information which may incur privacy leakages. Though, the comparison between existing literature and their work, all the sensitive information is hidden by us, such as age, height, weight, and gender concurrently and hence generating a multiple attributes obfuscator. Furthermore, characterization of energy privacy preserving technique is carried out by the us, which was neglected in the existing literature best of our knowledge [31]. This preserving privacy technique, which, to the best of our information, was ignored in present works.

3. MATERIALS AND METHODS

The proposed method which is privacy-preserving HAR is described in this section. Transmission of data remotely produced by devices of mobile user to service providers of cloud based for inferring

corresponding activities through models of machine learnings, providing user with feedbacks and storing data [32] which happens in a typical application. A ‘‘honest but curious’’ threat model was assumed adversary model where provider of service has authentic admittance to user’s inertial signals, possibly could attempt to infer extra sensitive data from streams of sensor such as physical attributes, age or gender which compromise privacy of user [33].

Aim of the proposed approach is keeping the ability of correct recognition of activities for satisfactory levels while guarding from probable unapproved inference of sensitive features is coming from the machine learning models of attacker which are service providers. Benefits of the ability of camouflaged segmentation are especially are taken for learning input data’s representation via a non-linear prediction on a latent space and its succeeding rebuilding [34]. A system founded on deep learning camouflaged segmentation, was proposed for achieving this goal, which was trained for input data processing into a version which keeps the information necessary for nonsensitive elements classification. Simultaneously, difficulty in inference of sensitive information is made by them. A definite loss function was used consisting of 2 terms for training camouflaged segmentation where one was endorsing penalization of various types of sensitive information’s precise prediction and other in control of incentivizing accurate inference of authentic features. Benefits of the ability of camouflaged segmentation are especially taken for learning input data’s representation via a non-linear prediction on a latent space and its succeeding rebuilding. A wide range topic with various issues is represented by protection of privacy in mobile and wearable systems [35] of computing which might be considered carefully at time of design especially relating to balance between utility and privacy. Concept of resilience is discussed by Lin *et al*. [36] by providing assurances in adaptability and robustness terms. For complementing privacy protection this concept was leveraged. Security and privacy risks are related to various types of attacks in our suggested privacy-preserving HAR system. For example, for accessing inertial signals directly Camouflaged segmentation could be bypassed which makes suggested strategies unproductive. Illegitimate access to weighs and structure of Camouflaged segmentation represents another vulnerability that can be exploited by reverse engineering system of obfuscation and its functionality is compromised. The operating system of device enforce resistance to attacks of theses types. Mechanisms of authentication are leveraged by various approaches for supporting resilience depending upon generation of symmetric key systems which is presented in [37] that was discovered to be helpful in attacks of eavesdropping.

Anticipation of privacy risks and potential attacks in principle could happen [38]. But that is beyond the articles scope and can be considered as future work. Inertial sensor data’s sensitive attributes safeguarding is focus of work. For compressing input into telling representation neural networks of camouflaged segmentation are designed and in second part decoding of input is done for similarity between output and original input. Most commonly used camouflaged segmentation, surveyed by Bank *et al*. [14], highlights, especially techniques of regularization i.e. the representation of compression of input is expressive is ensured in camouflaged segmentation. Method presented by Malekzadeh *et al*. [26], is followed for designing system where a conversion of an assumed segment of window of multidimensional time series into an output of the same dimensionality is performed by camouflaged segmentation. The activity recognition module takes input from time series segments transformed version [39]. For carrying out inference of private features and if it is given as an input then no any attributes should be revealed hence by reducing accuracy of legitimate activity recognition by preserving privacy. Hence, for compressing models of machine learning, models are needed for specific solutions and fit them with compute and resources of memory of specified embedded systems [40].

For doing so, following design things are proposed: i) for inference of non sensitive information using deep learning model using Tensor flow framework [41] and ii) a deep leaning model set which is proficient of creating inference of private data like as height, age, gender, and weight as mentioned in Figure 2. Data can be kept locally for avoiding privacy leaks and execution of any inference movement on panel of device of user’s directly is one of the possible ways. Many modern models of machine learning wants computational requirements which contrast with this approach. Certainly, hardware resources accessible on restricted devices, particularly those depend on microprocessor units [42], low-cost, low-power, frequently hindering implementation of inference works depending upon networks of neural.

The diagram illustrates the proposed workflow of a biometric access control system integrated with AI and IoT technologies. The process begins with capturing the facial image of the user, followed by feature extraction to obtain discriminative biometric representations. These features are processed by a matcher module, where identification is performed through comparison with stored templates in the database and verification is supported using a user identity token. Based on the matching outcomes, the decision logic determines whether a valid match exists. If confirmed, access is granted by unlocking the door; otherwise, access is denied and the system returns to the monitoring state for subsequent authentication attempts.

From a security and privacy perspective, the system enforces multi-stage authentication to reduce unauthorized access, while sensitive biometric information is handled in the form of extracted features rather

than raw images. Limiting database interactions to matching operations and separating identification and verification stages minimizes data exposure and supports privacy-aware authentication in IoT-enabled environments.

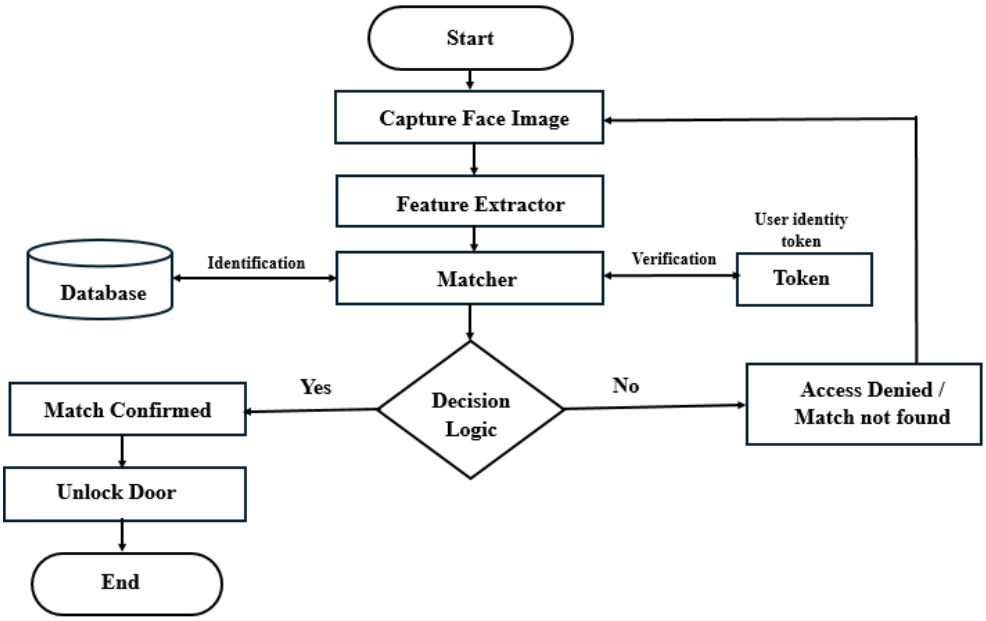

Figure 2. Proposed method working diagram

3.1. Internet of things

DevKit of Espressif ESP32-wroom-32 [43] was taken as wearable low power connected devices representative, which was connected to 6-axis motion tracking device named MPU6050, which integrates three-axial accelerometer and three-axial gyroscope is an IoT device. A real time application is developed on top of a hardware device for gathering data of sensor and transforming it as described previously using camouflaged segmentation [44]. Devices' consumption of energy is observed in mean time for characterizing efficacy of Camouflaged segmentation. Espressif IoT development framework (ESP-IDF) platform was used for writing application which was written in C++ with installation of libraries of tensor flow lite micro. Individual control of two separate CPU cores of ESP32 is given which are running at 80 to 240 MHz adjustable frequency. This will help for transforming and sensing application as two separate tasks executed on two different CPU cores. A data producer, which is one thread that captures continuous data from sensors while another thread works as data consumer by performing models of ML for removing data-sensitive information [45]. 400 KB of RAM and 4 MB of flash ROM is used by the version of ESP32. Tesnor Flow lite model can directly store in flash memory due to its representation by a static set of instructions and weights alogwith components of firmware that result in a model of installable size somewhat reduced than 4 MB.

3.2. Datasets

Two openly accessible datasets MotionSense [46] and MobiAct [47] are used for conduction of the experiments. The information is gathered from an iPhone 6s in the applicant’s front pocket in and is included in MotionSense. It also comprises information from virtual sensors like as attitude (pitch, roll, and yaw) and gravity which are taken from software elaboration, along with gyroscope and triaxial accelerometer as native sensors, commonly available in the current smartphones. The focus of the work is on the performance of the IoT devices having very low performance which was not possible to compute using virtual sensor, the data coming from only native sensors is considered for the experiments. The datasets consist of total of 24 participants which consists 14 males and 10 females consisting of average age 29 and minimum and maximum age of 18 and 35 respectively, whereas the average weight is 72 kg and minimum weight is 40 kg and maximum weight is 100 kg while the average height is 174 cm and maximum height is 190 cm and minimum height is 161 cm. The participants performed six different activities in the fifteen trials in the same conditions and the environments like as standing, sitting, jogging, walking, upstairs, and downstairs. For

models testing and training, each trial segment is divided into the segments of sliding window of 50 points which corresponds to 1 second with 75%. Choosing the percentage of overlap and time window size is non trivial task as the time window length impacts the model's classification performance. For example, in HAR works, literature uses different window lengths ranging from 1 to 30 s [39]. 75% of overlap and 1-second time window was used in this study which was proposed by Zhang *et al*. [21] for comparing with their work directly. Data collected from the orientation, gyroscope and accelerometer sensors of a Samsung Galaxy S3 smartphone consisted by MobiAct dataset. 57 individuals are used for collecting the data while they were performing different actions. Particularly, these dataset objectives to reproduce day to day actions by having applicants transfer the smartphone in a loose pocket with arbitrary alignment. The sensor of the geomagnetic field and accelerometer are sensors from where information is derived by the alignment sensor, and it depends upon the software. Software sensors are not considered because of little computation abilities of our target devices in case of MotionSense. Data was gathered from 30 females and 14 males totaling 44 subjects which is our dataset that is subset for the comparison of method by us with method described in Zhang *et al*. [21]. These subjects engaged in different activities like jogging, walking, upstairs, and downstairs. The average age of participants is 25 years, ranging from 20 years to 47 years, average weight of 77 kg ranging form minimum of 50 kg to maximum 120 kg, and average height of 176 cm, whereas minimum of 158 cm and maximum of 193 cm. Each trial is divided into sections by a gliding length of window of 50 points with overlap of 75% in case of MotionSense dataset.

4. RESULT AND DISCUSSION

This section describes, efficiency of privacy preserving in HAR and efficiency of energy of the projected method is characterized by experiments performed and presented here. Table 1 consists of results of recognition obtained by the model. The modern HAR regression and classification is represented here. The initial set of data is separated into 'test' and 'train' in which 25% is utilised as test data and 75% is used as a training set and testing and training of the proposed model using the original datasets is done. Table 2 consists of result of performance on MobiAct dataset by multiple feature obfuscators. The five diverse seeds of an arbitrary producer with 5 times are performed with training-testing procedure to have five different datasets, which are divided to evaluate the robustness of the approach. The measurement of detection outcomes of malicious models after and before the conversion, for evaluating capability of obfuscating sensitive information, which is applied through the camouflaged segmentation. The projected method is considered as ineffective in defending the sensitive information of user if the drop in the recognition capability is very negligible. On the contrary, the appropriateness of the projected technique is certified by the high drop.

Table 1. Results of model's characterization

Model	Measure	Motion sense	Size (MB)
Activity	Accuracy	0.992±0.003	10.8
Gender	Accuracy	0.996±0.002	204.5
Age (years)	MAE	0.375±0.046	8.6
Height (cm)	MAE	1.622±0.185	96.2
Weight (kg)	MAE	1.224±0.132	116.1

Table 2. Multiple attributes obfuscator performance on MobiAct dataset

Model	Measure	Motion sense	Size (MB)
Activity	Accuracy	0.926±0.002	0.163
Gender	Accuracy	0.952±0.100	0.702
Age (years)	MAE	1.364±0.121	3.061
Height (cm)	MAE	4.081±0.155	4.624
Weight (kg)	MAE	4.636±0.250	2.521

5. CONCLUSION

Human activity specific pattern recognition has gaining attention in various applications starting from smart homes to healthcare due to growing diffusion of mobile and wearable devices armed with various sensor types like as magnetometers, gyroscopes and accelerometers. The inference about various activities at high levels of accuracy are allowed when models of deep learning are intended to implemented on existing sensor. The tasks of classifications are often presented to cloud or edge computing devices because of the computational and energy burdens required by the modern neural network architectures which expose users for leaking sensitive data or information. For protecting the privacy of the user concerning the inference of

the private data from streams of the sensor like as gender, age, height and weight using camouflaged segmentation of deep learning approach is presented in this study. To transform the signal neural networks of this type are trained in such a way that the data could increase the privacy breaches which are filtered out. Simultaneously, activity recognitions revealing portion is kept. To allow the porting on the low power IoT platforms segmentation architectures of camouflaged has been fine tuned and to characterize the performance completely its consumption of energy also has been measured. The ability of the projected systems for obfuscating signal for the inference of sensitive attributes while keeping high accuracy levels in HAR tasks is validated by the comprehensive set of experimental results. Indeed, complete neutralization of the privacy related inference in the experimental set up is achieved with a modest (5% maximum) decrease in accuracy. At the same time, the feasibility of this approach in particular wearable applications is showed through implantation on a low power IoT or embedded device keeping the best trade off between accuracy loss and maximum consumption of energy of 165.240 mJ during the execution of the obfuscation task with an obfuscation latency of around 30 ms.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Mahesh Shankarrao Patil	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Harsha J. Sarode		✓				✓		✓	✓	✓	✓	✓		
Abhijit Banubakode	✓		✓	✓			✓			✓		✓	✓	
Prakash Tukaram Patil	✓					✓	✓		✓	✓				
Nutan Patil				✓		✓			✓	✓	✓			
Vijayakumar Varadarajan		✓			✓		✓			✓		✓		
Deshinta Arrova Dewi	✓					✓	✓			✓		✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] K. Gopinath and L. P. Sai, "A study on the positioning of the brand variants by smartwatch manufacturers: a technometrics approach," *Technology Analysis and Strategic Management*, vol. 35, no. 6, pp. 689–703, 2023, doi: 10.1080/09537325.2021.1980210.

[2] Grand View Research, "Wearable technology market size, share and trends analysis report by product," grandviewresearch.com. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/wearable-technology-market, (Accessed: Jan. 29, 2024).

[3] T. Poongodi, R. Krishnamurthi, R. Indrakumari, P. Suresh, and B. Balusamy, "Wearable devices and IoT," *Intelligent Systems Reference Library*, vol. 165, pp. 245–273, 2020, doi: 10.1007/978-3-030-23983-1_10.

[4] K. Chen, D. Zhang, L. Yao, B. Guo, Z. Yu, and Y. Liu, "Deep learning for sensor-based human activity recognition: Overview, challenges, and opportunities," *ACM Computing Surveys*, vol. 54, no. 4, pp. 1–40, 2022, doi: 10.1145/3447744.

[5] Z. Qian *et al.*, "Development of a Real-Time Wearable Fall Detection System in the Context of Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 21, pp. 21999–22007, 2022, doi: 10.1109/JIOT.2022.3181701.
[6] A. Hussain, S. U. Khan, N. Khan, M. Shabaz, and S. W. Baik, "AI-driven behavior biometrics framework for robust human activity recognition in surveillance systems," *Engineering Applications of Artificial Intelligence*, vol. 127, p. 107218, 2024, doi: 10.1016/j.engappai.2023.107218.
[7] S. Alzahrani, J. Alderaan, D. Alatawi, and B. Alotaibi, "Continuous Mobile User Authentication Using a Hybrid CNN-Bi-LSTM Approach," *Computers, Materials and Continua*, vol. 75, no. 1, pp. 651–667, 2023, doi: 10.32604/cmc.2023.035173.
[8] R. Aloufi, H. Haddadi, and D. Boyle, "Paralinguistic Privacy Protection at the Edge," *ACM Transactions on Privacy and Security*, vol. 26, no. 2, pp. 1–27, 2023, doi: 10.1145/3570161.
[9] P. Bagga, A. Mitra, A. K. Das, P. Vijayakumar, Y. H. Park, and M. Karuppiah, "Secure biometric-based access control scheme for future IoT-enabled cloud-assisted video surveillance system," *Computer Communications*, vol. 195, pp. 27–39, 2022, doi: 10.1016/j.comcom.2022.08.003.
[10] L. Causa, J. E. Tapia, A. Valenzuela, D. Benalcazar, E. L. Droguett, and C. Busch, "Analysis of behavioural curves to classify iris images under the influence of alcohol, drugs, and sleepiness conditions," *Expert Systems with Applications*, vol. 242, p. 122808, 2024, doi: 10.1016/j.eswa.2023.122808.
[11] L. Zhang, W. Cui, B. Li, Z. Chen, M. Wu, and T. S. Gee, "Privacy-Preserving Cross-Environment Human Activity Recognition," *IEEE Transactions on Cybernetics*, vol. 53, no. 3, pp. 1765–1775, 2023, doi: 10.1109/TCYB.2021.3126831.
[12] E. Antwi-Boasiako, S. Zhou, Y. Liao, Q. Liu, Y. Wang, and K. Owusu-Agyemang, "Privacy preservation in Distributed Deep Learning: A survey on Distributed Deep Learning, privacy preservation techniques used and interesting research directions," *Journal of Information Security and Applications*, vol. 61, p. 102949, 2021, doi: 10.1016/j.jisa.2021.102949.
[13] J. Liu, Z. Zhao, P. Li, G. Min, and H. Li, "Enhanced Embedded AutoEncoders: An Attribute-Preserving Face De-Identification Framework," *IEEE Internet of Things Journal*, vol. 10, no. 11, pp. 9438–9452, 2023, doi: 10.1109/JIOT.2023.3235725.
[14] D. Bank, N. Koenigstein, and R. Giryes, "Autoencoders," *arXiv preprint*, 2020, doi: 10.48550/arXiv.2003.05991.
[15] G. Schram, R. Wang, and K. Liang, "Using Autoencoders on Differentially Private Federated Learning GANs," *arXiv preprint*, 2022, doi: 10.48550/arXiv.2206.12270.
[16] P. Deng, C. Ge, H. Wei, Y. Sun, and X. Qiao, "Multimodal contrastive learning for face anti-spoofing," *Engineering Applications of Artificial Intelligence*, vol. 129, p. 107600, 2024, doi: 10.1016/j.engappai.2023.107600.
[17] A. A. S. Mohammad *et al.*, "Strategies for applying interpretable and explainable AI in real world IoT applications," *Discover Internet of Things*, vol. 5, p. 71, 2025, doi: 10.1007/s43926-025-00155-z.
[18] K. Shaheed, P. Szczuko, M. Kumar, I. Qureshi, Q. Abbas, and I. Ullah, "Deep learning techniques for biometric security: A systematic review of presentation attack detection systems," *Engineering Applications of Artificial Intelligence*, vol. 129, p. 107569, 2024, doi: 10.1016/j.engappai.2023.107569.
[19] A. Boutet, C. Frindel, S. Gambs, T. Jourdan, and R. C. Ngueveu, "DySan: Dynamically Sanitizing Motion Sensor Data against Sensitive Inferences through Adversarial Networks," in *ASIA CCS 2021 - Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, 2021, pp. 672–686, doi: 10.1145/3433210.3453095.
[20] L. Lyu, X. He, Y. W. Law, and M. Palaniswami, "Privacy-preserving collaborative deep learning with application to human activity recognition," in *International Conference on Information and Knowledge Management, Proceedings*, 2017, pp. 1219–1228, doi: 10.1145/3132847.3132990.
[21] D. Zhang, L. Yao, K. Chen, Z. Yang, X. Gao, and Y. Liu, "Preventing Sensitive Information Leakage from Mobile Sensor Signals via Integrative Transformation," *IEEE Transactions on Mobile Computing*, vol. 21, no. 12, pp. 4517–4528, 2022, doi: 10.1109/TMC.2021.3078086.
[22] A. Garain, R. Dawn, S. Singh, and C. Chowdhury, "Differentially private human activity recognition for smartphone users," *Multimedia Tools and Applications*, vol. 81, no. 28, pp. 40827–40848, 2022, doi: 10.1007/s11042-022-13185-4.
[23] P. Climent-Pérez and F. Florez-Revuelta, "Privacy-Preserving Human Action Recognition with a Many-Objective Evolutionary Algorithm," *Sensors*, vol. 22, no. 3, p. 764, 2022, doi: 10.3390/s22030764.
[24] S. Menasria, M. Lu, and A. Dahou, "PGAN framework for synthesizing sensor data privately," *Journal of Information Security and Applications*, vol. 67, p. 103204, 2022, doi: 10.1016/j.jisa.2022.103204.
[25] M. Malekzadeh, R. G. Clegg, and H. Haddadi, "Replacement autoencoder: a privacy-preserving algorithm for sensory data analysis," *arXiv preprint*, 2017, doi: 10.1109/IoTDI.2018.00025.
[26] M. Malekzadeh, A. Cavallaro, R. G. Clegg, and H. Haddadi, "Protecting sensory data against sensitive inferences," in *Proceedings of the Workshop on Privacy by Design in Distributed Systems, P2DS 2018, co-located with European Conference on Computer Systems, EuroSys 2018*, 2018, doi: 10.1145/3195258.3195260.
[27] P. Delgado-Santos, R. Tolosana, R. Guest, R. Vera-Rodriguez, F. Deravi, and A. Morales, "GaitPrivacyON: Privacy-preserving mobile gait biometrics using unsupervised learning," *Pattern Recognition Letters*, vol. 161, pp. 30–37, 2022, doi: 10.1016/j.patrec.2022.07.015.
[28] S. Abbasi, M. Famouri, M. J. Shafiee, and A. Wong, "Outliernets: Highly compact deep autoencoder network architectures for on-device acoustic anomaly detection," *Sensors*, vol. 21, no. 14, p. 4805, 2021, doi: 10.3390/s21144805.
[29] H. Ren, D. Anicic, and T. A. Runkler, "TinyOL: TinyML with Online-Learning on Microcontrollers," in *Proceedings of the International Joint Conference on Neural Networks*, 2021, doi: 10.1109/IJCNN52387.2021.9533927.
[30] A. Alsalemi, Y. Himeur, F. Bensaali, and A. Amira, "An innovative edge-based Internet of Energy solution for promoting energy saving in buildings," *Sustainable Cities and Society*, vol. 78, p. 103571, 2022, doi: 10.1016/j.scs.2021.103571.
[31] D. V. Bratu, R. Ş. T. Ilinoiu, A. Cristea, M. A. Zolya, and S. A. Moraru, "Anomaly Detection Using Edge Computing AI on Low Powered Devices," in *IFIP Advances in Information and Communication Technology*, 2022, pp. 96–107, doi: 10.1007/978-3-031-08333-4_8.
[32] A. Sathiamoorthy, S. Mithusan, R. Rathnayaka, S. Kajenthiran, M. M. Hansika, and D. Pandithage, "StreamSafe: Improving QoS and Security in IoT Networks," *International Research Journal of Innovations in Engineering and Technology*, vol. 7, no. 11, p. 170, 2023.
[33] S. S. Hammad, D. Iskandaryan, and S. Trilles, "An unsupervised TinyML approach applied to the detection of urban noise anomalies under the smart cities environment," *Internet of Things (Netherlands)*, vol. 23, p. 100848, 2023, doi: 10.1016/j.iot.2023.100848.
[34] H. V. Dudukcu and M. Taskiran, "ECG data anomalies detection with stacked autoencoder on low power and low memory microcontrollers," in *Current Research in Engineering*, S. Bardak and U. Ayata, Eds., Ankara: Gece Kitaplığı, 2023, ch. 14, pp. 275–289.
[35] E. Oliver, R. Yue, and A. Dutta, "A Secure Vitals Monitoring Point-of-Care Device," in *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS*, 2023, pp. 1–4, doi:

10.1109/EMBC40787.2023.10340768.
[36] W. Lin, M. Xu, J. He, and W. Zhang, "Privacy, security and resilience in mobile healthcare applications," *Enterprise Information Systems*, vol. 17, no. 3, p. 1939896, 2023, doi: 10.1080/17517575.2021.1939896.
[37] Q. Lin, "Developing wearable applications with innovative sensing modalities for human activity recognition and key generation," Ph.D. dissertation, University of New South Wales, Sydney, Australia, 2020.
[38] M. A. Jan *et al.*, "Lightweight Mutual Authentication and Privacy-Preservation Scheme for Intelligent Wearable Devices in Industrial-CPS," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5829–5839, 2021, doi: 10.1109/TII.2020.3043802.
[39] E. Lattanzi, M. Donati, and V. Freschi, "Exploring Artificial Neural Networks Efficiency in Tiny Wearable Devices for Human Activity Recognition," *Sensors*, vol. 22, no. 7, p. 2637, 2022, doi: 10.3390/s22072637.
[40] C. Contoli and E. Lattanzi, "A Study on the Application of TensorFlow Compression Techniques to Human Activity Recognition," *IEEE Access*, vol. 11, pp. 48046–48058, 2023, doi: 10.1109/ACCESS.2023.3276438.
[41] TensorFlow, "TensorFlow Official Website." [Online]. Available: http://www.tensorflow.org/?hl=en (Accessed: Jun. 22, 2023).
[42] Espressif, "ESP32C3-WROOM-02 Datasheet." [Online]. Available: https://www.espressif.com/en/support/documents/technical-documents, (Accessed: Jun. 22, 2023).
[43] S. Girmay, F. Samsom, and A. M. Khattak, "AI based Login System using Facial Recognition," in *2021 5th Cyber Security in Networking Conference, CSNet 2021*, 2021, pp. 107–109, doi: 10.1109/CSNet52717.2021.9614281.
[44] M. Y. S. Krishna, A. Arya, S. Ansari, S. Awasya, J. Sushakar, and N. Uikey, "Real Time Door Unlocking System using Facial Biometrics based on IoT and Python," in *2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science, SCEECS 2023*, 2023, pp. 1–5, doi: 10.1109/SCEECS57921.2023.10063142.
[45] M. Malekzadeh, R. G. Clegg, A. Cavallaro, and H. Haddadi, "Mobile sensor data anonymization," in *IoTDI 2019 - Proceedings of the 2019 Internet of Things Design and Implementation*, 2019, pp. 49–58, doi: 10.1145/3302505.3310068.
[46] H. Meddeb, Z. Abdellaoui, and F. Houaidi, "Development of surveillance robot based on face recognition using Raspberry-PI and IoT," *Microprocessors and Microsystems*, vol. 96, p. 104728, 2023, doi: 10.1016/j.micpro.2022.104728.
[47] W. H. Tan, F. Wahab, F. Mat, C. K. Chan, and R. J. Teoh, "Sound absorption coefficient measurement and analysis for multisection perforation microperforated panel," *Journal of Mechanical Science and Technology*, vol. 38, no. 6, pp. 2797–2803, 2024, doi: 10.1007/s12206-024-2210-6.

BIOGRAPHIES OF AUTHORS

Mahesh Shankarrao Patil received his B.E. degree in Electronics and Telecommunications and M.E. in Electronics from Savitribai Phule Pune University, Pune, India and Ph.D. at SJJT University, Rajasthan, India. He serves as a reviewer for many international journals. He is full-time assistant professor at School of Bioengineering Sciences and Research, MIT ADT University, Pune, India. His research lines are signal processing, image and video processing, embedded systems, IoT, robotics, and bio sensors. He can be contacted at email: mpink.patil@gmail.com.

Harsha J. Sarode received her B.E. degree in Electronics and Telecommunications from Amravati University and M.E. in Electronics from Savitribai Phule Pune University, Pune, India and Ph.D. at SJJT University, Rajasthan, India. She serves as reviewer for many international journals. She is full-time assistant professor at Department of Electronics and Telecommunication Engineering, Nutan Maharashtra Institute of Engineering and Technology, Pune, India. Her research lines are signal processing, image and video processing, machine learning, and deep learning. She can be contacted at email: sarodeharsha28@gmail.com.

Abhijit Banubakode received Ph.D. degree in Computer Studies from Symbiosis International University (SIU), Pune and M.E. degree in Computer Engineering from Savitribai Phule Pune University in 2005. He is a member of board of studies, academic council of various universities. He is a member of national and international professional bodies like International Association of Computer Science and Information Technology (IACSIT), IEEE, ISTE, and CSI. He is a Ph.D. guide to distinguished Indian Universities and presented 100+ research papers at international journals and conferences. Authored a world class international textbook of "Springer", "Bentham Science Publishers" and IGI Global Publication along with Patents and Copyright to his credit. He is currently working as Director of Computer Science and Engineering at Pimpri Chinchwad University, Pune. He has over 26 years of experience in academic and leadership roles. He can be contacted at email: abhijit.banubakode@pcu.edu.in.

Prakash Tukaram Patil received his Bachelor's degree in Electronics and Telecommunication Engineering and Master's degree in Electronics Engineering from Savitribai Phule Pune University, Pune, India. He has over 13 years of industry experience in the field of electronics, with specialization in PCB design, embedded systems, and internet of things (IoT) applications. He is currently working as an assistant professor in the Department of Electronics and Telecommunication Engineering. His research interests include embedded systems, IoT, PCB design, and industrial electronics. He can be contacted at email: prakash11862314@gmail.com.

Nutan Patil received her B.E. degree in Electronics and Telecommunications from North Maharashtra University Jalgaon Maharashtra India and M.Tech. from Bharti Vidyapeeth University Pune Maharashtra India. Pursuing Ph.D. in Electronics and Communication from JJT University Rajasthan, India. She is full time assistant professor at Nutan Maharashtra Institute of Engineering and Technology, Talegaon, Pune, Maharashtra, India. Her research lines are AI M, embedded system, and IoT. She can be contacted at email: nspatil9604@gmail.com.

Vijayakumar Varadarajan received Ph.D. degree from Anna University, India. He has completed his Diploma with first class honors. He obtained his B.E. in Computer Science and Engineering and MBA in Human Resource Development with first class distinction. He also earned his M.E. in Computer Science and Engineering, receiving the First Rank Award. He is currently an EAI Fellow and serves as a Visiting Professor at Universitas Diponegoro (UNDIP), Indonesia. He has over 18 years of combined industrial and academic experience. He has also worked as a Team Lead in leading industries such as Satyam, Mahindra Satyam, and Tech Mahindra for several years. He is a reviewer in IEEE Transactions, Inderscience, and Springer Journals. He has initiated a number of international research collaborations with universities in Europe, Australia, Africa, Malaysia, Singapore, and North and South America. He is also the Lead Guest Editor for a few journals in Inderscience, Springer, Elsevier, IOS, UM, and IGI Global. He can be contacted at email: vijayakumar.varadarajan@uts.edu.au.

Deshinta Arrova Dewi is a distinguished academic, researcher, and innovator specializing in artificial intelligence (AI) and big data analytics. She earned his doctorate from Universiti Kebangsaan Malaysia (UKM), focusing on applying AI to enhance efficiency and innovation across education, economics, and healthcare sectors. She has an impressive portfolio of award-winning AI solutions, including predictive machine learning algorithms and adaptive learning models that have transformed technology-based education. As an educator, she inspires students through interactive, practice-oriented teaching and frequently serves as a keynote speaker at international AI conferences, sharing insights on leveraging AI to address digital-era challenges. A prolific researcher, she has published extensively in top journals and leads cross-disciplinary projects aimed at sustainable, AI-driven community empowerment. Her contributions and leadership make her a prominent figure in artificial intelligence and digital technology. She can be contacted at email: deshinta.ad@newinti.edu.my.