



International Journal of Computer Applications in Technology

ISSN online: 1741-5047 - ISSN print: 0952-8091
<https://www.inderscience.com/ijcat>

Deep one-class classification induced authentication for security protection of wearable IoT application

Meng Tian, Guimei Liu, Lijing Xie

DOI: [10.1504/IJCAT.2025.10071395](https://doi.org/10.1504/IJCAT.2025.10071395)

Article History:

Received:	29 October 2023
Last revised:	06 April 2024
Accepted:	14 June 2024
Published online:	27 August 2025

Deep one-class classification induced authentication for security protection of wearable IoT application

Meng Tian

School of Information,
Changde College,
Changde, Hunan, China
Email: tianmeng@hnvcc.edu.cn

Guimei Liu*

Information Technology Branch,
Changsha Preschool Education College,
Changsha, Hunan, China
Email: guimei.liu123@outlook.com
*Corresponding author

Lijing Xie

Hunan Vocational College of Commerce,
Changsha, Hunan, China
Email: xielijing@hnvcc.edu.cn

Abstract: The Internet of Things (IoT) has become one of the most popular directions in the field of network and communication. However, with the rapid development of IoT, the number of terminal devices shows a geometric order of magnitude growth. The sensor network composed of sensing terminal devices can obtain information in all aspects, but at the same time, malicious attackers can also obtain the information. In order to solve this issue, this paper designs a lightweight authentication for security protection in wearable IoT environment through edge-cloud architecture. The proposed lightweight authentication system adopts PPG signal as biometric feature, which can be easily obtained and hard to forge. The authentication is implemented by using deep one-class classification model which is trained by using a PPG signal library. In order to avoid the limitation of resources at edge nodes, the deep one-class classification models are deployed at the cloud server. The experiments show that the proposed authentication system can achieve a promising result.

Keywords: authentication; IoT security protection; PPG signal; deep one-class classification.

Reference to this paper should be made as follows: Tian, M., Liu, G. and Xie, L. (2025) 'Deep one-class classification induced authentication for security protection of wearable IoT application', *Int. J. Computer Applications in Technology*, Vol. 76, Nos. 1/2, pp.65–75.

Biographical notes: Meng Tian is associate professor, and received the bachelor's degree from Hunan Agricultural University, China. Now, she works in the School of Information, Changde College, China. Her research interests include computer technology and network security.

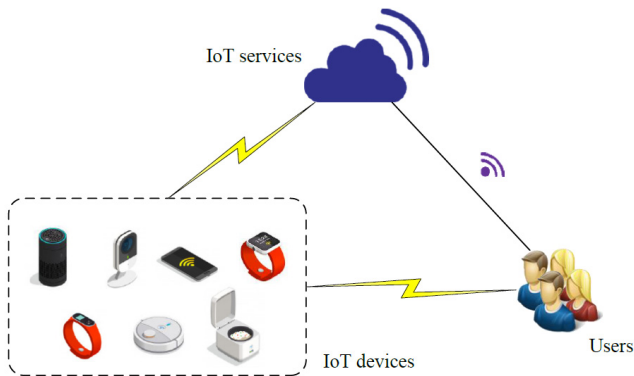
Guimei Liu is associate professor, and received the Master degree from Hunan University, China. Now, she works in Changsha Preschool Education College. Her research interests include application software development and network security.

Lijing Xie received the Master degree from Central South University, China. Now, he works in Practical Training and Information Management Center, Hunan Vocational College Of Commerce of Education. His research interests include cloud computing, network engineering and security.

1 Introduction

Internet of Things (IoT) (Laghari et al., 2021) refers to the intelligent service system that processes and responds to information from both physical and virtual worlds by sensing devices and connecting things, people, systems and information resources according to protocols. Here, ‘Things’ refers to a physical entity which may be anything. In general, IoT system consists of users, IoT devices and IoT services, which is shown in Figure 1.

Figure 1 The structure of IoT system. The IoT system consists of three parts: users, IoT terminal devices and IoT service



In Figure 1, the IoT system consists of three parts: users, IoT terminal devices and IoT service. The IoT devices are the terminal devices, including smart watch, smart phone, smart speaker, robot vacuum, etc. IoT services are deployed in cloud server. In recent years, with the transformation and innovation breakthroughs of information and communication technology, the rapid innovation and development of technologies such as big data and artificial intelligence promote the growth of IoT which has become the new trend in the technology industry (Hansen and Bøgh, 2021). The merit of IoT system is that it can inter-connect highly heterogeneous devices and systems which may have various shapes, sizes and functions. The rapid development of IoT industry leads to the exponential growth trend in the number of IoT devices, which are widely used in public health, smart grids, intelligent transportation, garbage management, smart homes, smart cities, smart agriculture, energy management and other fields. The physical entities in IoT system have the ability to communicate and interact with each other, and the ability to exchange data and perform certain specific task objectives to completely change human lifestyles to be safer, more convenient and more comfortable. More and more researchers are participating in designing and inventing innovative solutions and applications in the IoT environment (Li et al., 2024a).

In the smart city (Rejeb et al., 2022), the rapid development of IoT promotes the emerging applications, such as smart home, personal intelligent wearable devices and smart healthcare. Through automatic perception, data collection and intelligent control, the IoT technology promotes the creation of smart cities, achieving precise

management and optimisation services in transportation management, traffic control, and video surveillance, improving urban efficiency and benefitting people's lives. Currently, many cities in China are promoting the planning of ‘smart cities’, mainly applied in fields such as public safety, transportation, healthcare, communities, environmental protection, underground pipeline network monitoring, water supply, education, etc. These applications achieves comprehensive integration using automatic perception, data collection and intelligent control.

IoT technology supports the digital transformation of traditional industries (Ferreira and Lind, 2023). It empowers traditional industries and promotes the digital transformation, such as transportation, healthcare, logistics, industry, agriculture, manufacturing and security. For example, IoT technology has enabled the detection of goods and tracking of transportation vehicles, achieving comprehensive perception and analysis of various links such as logistics transportation, warehousing and distribution, and improving the transportation efficiency and intelligence level of the logistics industry; Industrial Internet of Things (IIoT) technology enables enterprises to connect sensors to machines, perceive information from everything and based on big data analysis technology, achieve intelligent decision-making and judgment, improve production efficiency and capacity.

With the rapid development of the Internet of Things industry, the application of new technologies has also brought some security risks to people's lives (Hassan et al., 2019). If the Internet of Things is attacked, it may lead to network paralysis. The devices based on national security, personal health and life and property security may suffer serious threats and losses. Compared to traditional internet, the security issues of the Internet of Things are more complex. Generally speaking, the network architecture of the Internet of Things mainly includes the terminal access layer, network transmission layer and application service layer. Its security issues can be divided into the risks of terminals, communication networks and application services. The risks of terminal security mainly manifest in the physical security, network communication and structural security, data leakage, security vulnerabilities, etc. The risks of communication networks mainly manifest in aspects such as wireless data transmission link security, unauthorised access and network access. Application services have the characteristics of storing a large amount of data on their servers and diverse application logic, which makes the vulnerabilities in the basic environment and components of the system easily exploited by hackers to launch attacks.

According to the function, the architecture of the Internet of Things system is divided as three parts: perception layer, network layer and application layer. In recent years, the research about Internet of Things security incidents shows that security threats not only appear in various layers of the Internet of Things, but also extend to aspects such as perception terminals, perception layer gateways, perception layer access and data transmission. The security attacks

against the Internet of Things are from the bottom to the top (Xiao et al., 2018; Li et al., 2024b). It may meet the interception and tampering of sensor information at the bottom, and the occupation of vulnerabilities in the middle network and service layers. Like other technologies, the Internet of Things also has some issues in terms of security and privacy. Owing to the fact that IoT networks are a combination of devices, communication technologies and various protocols, there are also security issues related to availability, data integrity, data confidentiality and identity verification, which directly lead to low operational efficiency, poor robustness and low throughput of IoT operations. Meanwhile, the Internet of Things faces some security and technical challenges due to the inherent limitations of devices, such as simple CPU structure, low storage capacity and weak computing power. In order to establish a sustainable and robust Internet of Things network, it is necessary to address security and privacy issues while fully considering the following limitations.

First, in IoT environments, interconnected devices, such as IoT sensors, are often equipped with low-speed processors and limited memory storage. These devices cannot perform expensive computing operations that require high computing power and high memory storage. It is a challenging task to design a solution that can minimise resource consumption and maximise security protection, simultaneously. When designing user identity authentication schemes for such environments, lightweight encryption operations can be used. The high-power computing and storage of devices are moved to cloud servers to save resources on the IoT devices.

Second, in certain given environments, most IoT devices are designed to be small in size and have limited inherent resources, such as batteries and storage. These devices automatically turn on power saving mode to save energy, when they are free. Owing to the limitations of battery resource storage, the main challenge is to develop lightweight security mechanisms for highly limited devices. In addition, all transmitted data needs to be encrypted to achieve privacy and confidentiality. Therefore, it is necessary to develop protocols based on lightweight cryptosystems.

Third, in order to overcome the security vulnerabilities of some existing schemes, it is necessary to maintain the latest security schemes. The existing scheme protocols need to be updated periodically. Therefore, it is a challenging task to design a solution that supports dynamic installation or updates without compromising security.

One of the most important functions provided by the Internet of Things is to support resource constrained devices. In fact, a large portion of devices in the Internet of Things have low energy consumption and computing power, which results in existing algorithms and solutions that require complex calculations and high energy consumption being unable to be applied to IoT devices. Therefore, the unique nature of IoT devices means that traditional data security and identity authentication schemes are infeasible. In order to handle this issue, this paper proposes an authentication protection scheme for wearable IoT application, which

adopt edge-cloud computing structure. The authentication protection adopts photoplethysmography (PPG) signals as biometric features to identify persons. Owing to the limitations of storage and computing capability, the edge nodes merely collect user's PPG signals and extract the associated features to reduce the computation burden. Then, a deep One-Class Classification (OCC) model is deployed at the cloud server, which is used to identify whether the user is himself or herself. The edge node sends the PPG features to cloud server, while the deep OCC model returns the identified result to edge node according to the PPG features. Since the most computation of authentication protection is in the cloud server, it is a lightweight scheme. Thus, the proposed authentication protection scheme is suitable for wearable IoT application. Compared with the shallow one-class classifiers, such as one-class support vector machine (Zhu et al., 2014, 2016) and support vector data description (Tax and Duin, 2004), Deep SVDD can disclose the essential features in the IoT data. The main contributions are summarised as follows:

- 1) An edge-cloud structure authentication scheme is proposed for wearable IoT application.
- 2) The PPG signals are adopted for authentication to overcome the weaknesses of traditional biometric features.
- 3) The Deep SVDD is introduced into authentication to handle the imbalance problem.

The rest of this paper is organised as follows: the related works about authentication protection using biometric features are reviewed in Section 2; the authentication and security protection for wearable IoT system is proposed in Section 3; the experiments and simulations are provided in Section 4; the conclusions and discussions are summarised in Section 5.

2 Related works

The inherent physiological characteristics or behavioural patterns are unique for individuals, which can uniquely represent their identity. Compared with other authentication and identification methods, physiological characteristics are difficultly replicated or counterfeited. It has become a new trend to utilise biometric features in identity recognition. A biometric-based identity recognition system has high security, simple operation and low cost. As an inherent physiological signal of the human body, PPG signal contains a large amount of pathological and physiological information of the human cardiovascular system. There are significant differences in PPG signals between different individuals, which have good confidentiality and uniqueness. Identity recognition based on PPG signals is receiving increasing attention.

Kavsaoglu et al. (2014) extracted 40 time-domain features from a single period of PPG signal and its first and second order differential signals. The Euclidean distance is used to

calculate the contributions of each feature. This method combines the first and second order features of PPG signals, and provides a more accurate description of PPG signals. However, due to the weak and complex transformation of PPG signals, the extracted features are easily affected by various noises. The computational complexity of feature extraction is expensive. Gu et al. (2003) extracted features, including the number of peaks, the slope of the rising branch, the slope of the falling peak to the trough and the time interval and utilised Euclidean distance between feature vectors as the basis for identity classification. Subsequently, they also proposed a method based on fuzzy logic to verify the feasibility of using PPG signals for identity recognition (Gu and Zhang, 2003). Lee and Kim (2015) extracted PPG signal features, including area, waveform angle, inflection point data, etc., which are input into feedforward neural network. Kavsaoğlu et al. (2014) proposed a feature sorting algorithm to rank raw signal features, first- and second-derivative features according to their contributions to biometric recognition. Jaafar et al. (2015) used the single cycle waveform of PPG signal for identity recognition. They first performed a second derivative of the PPG signal to obtain an acceleration pulse wave, then used a Bass low-pass filter to remove high-frequency noise from the acceleration pulse wave, segmented and normalised the denoised acceleration pulse wave. These methods all directly locate the PPG signal or its first and second derivative reference points to extract time-domain features, which have high requirements for feature localisation performance and are easily affected by external factors.

Salanke et al. (2013) used Fourier series coefficients to reconstruct PPG signals to reduce the impact of motion artifacts, used semi discrete decomposition methods to extract features and matched them using Euclidean distance. Yadav et al. (2018) proposed a template matching identity authentication method that utilises continuous wavelet transform for feature extraction and direct linear discriminant analysis for feature dimensionality reduction. Spachos et al. (2011) located the maximum and minimum points of the original PPG signal after preprocessing, and used them as a benchmark to perform periodic segmentation of the signal. Nadzri et al. (2016) introduced a twin biometric recognition technology based on PPG signals. Firstly, the PPG signal was preprocessed, and then multiple periods of PPG waveforms were extracted. The subjects were classified using naive Bayesian and radial basis functions. Karimian et al. (2017) performed single cycle segmentation on PPG signals and then applied discrete wavelet transform to extract signal features. The advantage of using a certain transformation to extract

feature vectors from the single cycle waveform of PPG signals for identity recognition lies in strong anti-interference, high stability and strong specificity. However, the number of extracted features is relatively large, requiring additional dimensionality reduction of the data, increasing system complexity and affecting recognition speed.

Sarkar et al. (2016) proposed a dynamic model-based identity authentication method, which mapped each cardiac cycle to the limit cycle, decomposes the PPG signal into a sum of Gaussian functions, used the obtained Gaussian parameters as biometric templates, and finally utilised linear discriminant analysis and quadratic discriminant analysis as classifiers for identity recognition. Cao et al. (2020) utilised wristband wearable devices to collect PPG signals and a two-stage algorithm to reduce the impact of motion artifacts on the original signal. Zhao et al. (2020) designed motion artifact cancellation schemes for different exercise intensities based on PPG data collected by wrist strap devices, extracted benchmark features to generate templates and used gradient lifting trees to generate adaptive classifiers. These works do not consider the limitations of resources, which may fail in wearable IoT environment.

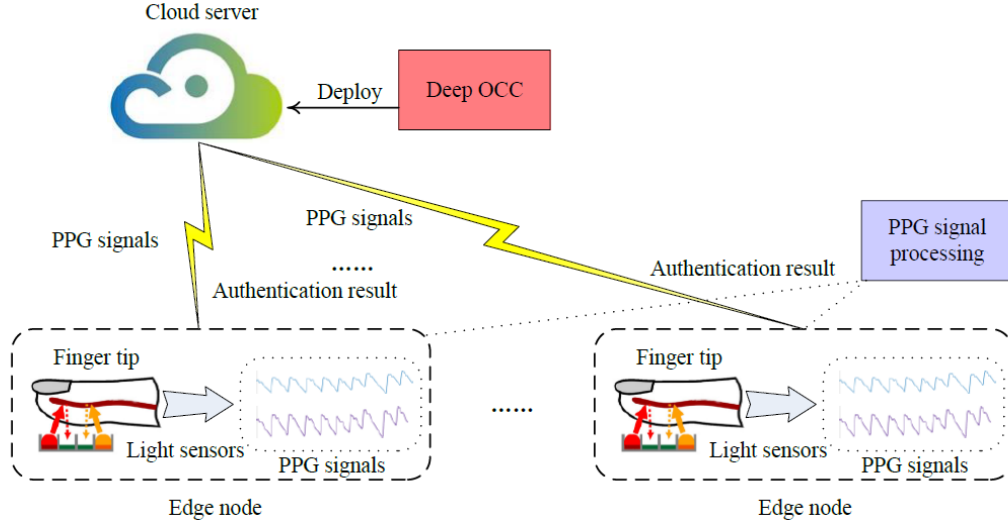
3 Authentication and security protection for wearable IoT system

3.1 The structure of authentication and identification for wearable IoT system

Compared with traditional authentication and identification, the devices in wearable IoT system have limited resources, such as memory storage and computing power. In order to overcome these limitations, the authentication and security protection adopts edge-cloud computing architecture which consists of edge nodes and cloud server. The edge nodes mainly focus on PPG signal collection and preprocessing which do not need high computation resource. The deep one-class classification is deployed in cloud server to reduce the computing burden of edge nodes. The details of authentication and identification for wearable IoT system are provided in Figure 2.

In Figure 2, the dashed rounded rectangles are edge nodes in the wearable IoT system. The edge node has a finger tip to collect PPG signal and a smart part with limited computing ability to process collected PPG signals. The cloud server has strong power to support authentication and identification through a deep one-class classification model which is learnt offline.

Figure 2 The structure of authentication and identification for wearable IoT system. The authentication and identification system consists of two parts: edge nodes and cloud server. The edge nodes collect, while cloud server deploys deep SVDD models to recognise the identity of user through PPG signals from edge node



3.2 PPG signals processing and feature extraction

PPG signal refers to the pulse wave signal detected by the photoplethysmography method which consists of a transmitter and a receiver to detect the changes in human blood volume. Owing to the increase in arterial blood volume caused by ventricular contraction, the systolic peak is generated, which is the most obvious reference point in the PPG signal waveform. The systolic peak is related to the individual's cardiac bleeding volume and arterial wall elasticity. When the heart is in the diastolic phase, blood will flow back to cause a small increase in blood in the blood vessels. The descending isthmus indicates the end of the systolic period of the heart. A complete heartbeat cycle refers to the PPG signal between two adjacent valleys.

The PPG signal is related to many factors, including heart size, health status, age, gender, emotional state, exercise status, posture, etc. The frequency generally distributes between 0.5 Hz and 5 Hz. With the increasing of age, individual PPG signal changes over time, age, health status and other factors. The collection environment of physiological factors may also induce the changes of PPG signal. In order to handle these issues, PPG signals need to be pre-processed before identification.

The PPG signal is a typical quasi periodic and non-linear weak electrophysiological signal with amplitudes generally in the millivolt level, which are unstable due to the beating of the heart cycle and external environmental influences. During the measurement process, the complexity of the external environment causes many interferences to the shape of the waveform. Meanwhile, during measurement, the noises may also be caused by the subjects' respiratory tremors and weak displacement during contact, which affects the recognition results. The common noises in PPG signals include high frequency interference, low frequency interference and baseline drift.

The high frequency interference refers to random noises caused by instability of the measurement environment. Meanwhile, the physiological signal may corrupted by power

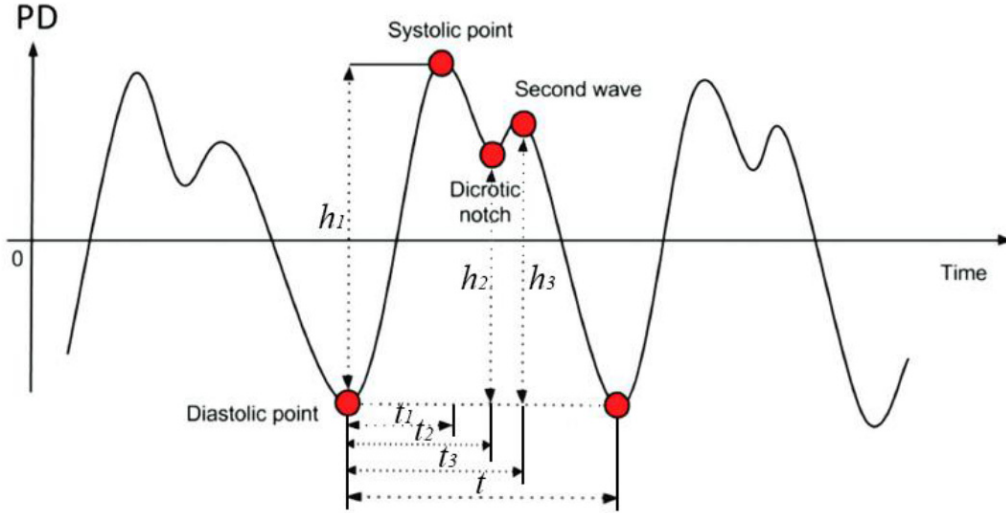
frequency interference which is caused by collection circuit design and power consumption of collection devices. The power frequency interference also belongs to high frequency interference. The low frequency interference includes motion artifact which is produced by spontaneous and unconscious muscle shaking, breathing during signal collection. Baseline drift refers to the slight fluctuation trend of the original signal on the waveform over time and is mainly caused by sensor movement, which induces aliasing with the signal during the signal acquisition process. If not eliminated, it will have an impact on subsequent feature extraction and classification recognition.

In this paper, the motion artifacts and high-frequency interference are removed by bandpass filtering, while baseline drift is eliminated by wavelet filtering for PPG denoising.

Before using filtering, the PPG signal needs to be zero-mean normalisation which ensures the signal follows standard normal distribution with mean 1 and standard deviation 1. Let $x(t)$ be normalised PPG signal. Generally, the useful information of PPG signals is distributed in the frequency range of 0.5–5 Hz, which is significantly different from high-frequency interference. FIR bandpass filter with Kaiser window is utilised to remove the high-frequency interference.

After bandpass filtering, the PPG signal filters out for power frequency interference caused by motion artifacts, random noise, etc., to retain the main part of the signal. However, the baseline drift problem caused by breathing, muscle micro motion, amplifier DC bias drift, etc., has not been properly addressed. Since the baseline drift mainly consists of low-frequency components in physiological signals, wavelet transform has strong adaptability and detail detection ability for non-stationary signals in both the time and frequency domains. This paper uses wavelet transform to decompose multiple scales of physiology to remove the baseline drift.

Before feature extraction of PPG signals, it detects feature points to divide the signal period. The feature point detection methods include sliding window, neural network, etc. An illustration of feature points is shown in Figure 3.

Figure 3 The period of PPG signal

In Figure 3, h_1 represents the amplitude of main wave, h_2 represents the amplitude of diastolic notch, h_3 represents the amplitude of diastolic wave, h_4 represents the difference between diastolic notch and diastolic wave, t represents the time of the whole period and t_1 represents the time from the starting of the period and main wave. Then, $t_2 - t_1$ is the time from main wave and diastolic notch, $t_3 - t_2$ is the time from diastolic wave and diastolic notch and $t - t_3$ is the time from the end of the period to diastolic wave.

As well as the above features, this paper also utilises the following time-domain features: the slope from the starting point of the pulse cycle to the peak of the main wave, the slope from the peak of the main wave to the end of the period, the slope from the peak of the main wave to the peak of the heavy pulse wave, the total area enclosed between the periodic waveform and the baseline, the area between the peak of the main wave and the baseline from the beginning of the cycle, the area enclosed by the main wave peak to the descending gorge and the baseline, the area between the peak of the descending gorge and the baseline of the heavy pulse wave and the area between the peak of the heavy pulse wave and the end of the cycle and the baseline. These features are classified as slope-based feature and area-based feature.

The time domain of PPG signal reflects the many important physiological and pathological features, while frequency domain plays an important role to reflect physiological state. As the source of amplitude, the heart ejects blood into various organs of the human body. The energy is generated due to continuous collisions between blood flow and the inner walls of blood vessels, resonating with physiological organs such as the liver, kidney and spleen. After multiple decomposition, various harmonic components are obtained. Therefore, the size and amplitude of each harmonic of pulse waves are closely related to the functional status of various organs in the human body. The use of frequency domain analysis can better reflect the individual's physical and health status, provides features that are difficult to obtain in the time domain and reflects the individual's state from another dimension.

The PPG signals of different individuals have significant differences in spectral energy. In the research process of identity recognition using PPG signals, frequency bands are usually divided based on the frequency distribution characteristics of the signals, and the spectral energy ratios of different sub band frequency bands are used as typical frequency domain features. The spectrum energy of sub band is obtained by combining downsampling and Short Time Fourier Transform (STFT). This paper considers the 0.5–10 frequency band of PPG signal. The spectral energy of band $i - j$ Hz is represented as equation (1).

$$E_i = \int_i^j P(f) df \quad (1)$$

In equation (1), $P(f)$ is the spectral density of the band $i - j$ Hz. In this paper, the PPG signal is divided as six sub-bands. The Power Spectral Energy Ratio (PSER) is represented as equation (2).

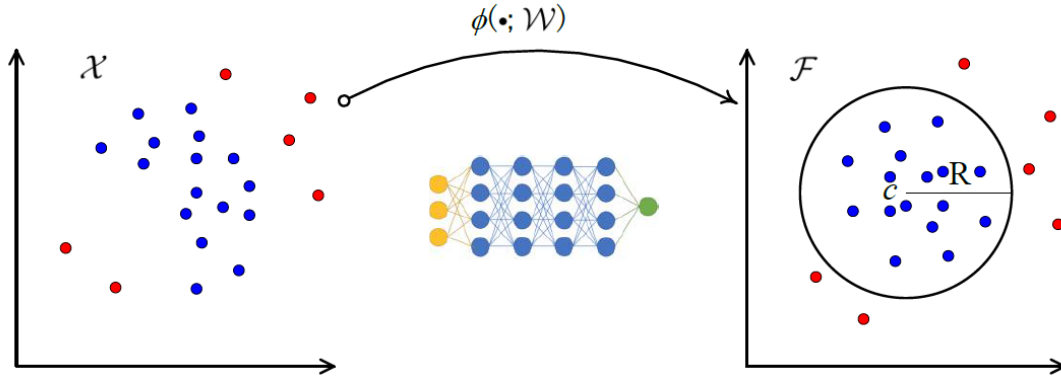
$$PSER_i = \frac{E_i}{\sum_{i=1}^6 E_i} \quad (2)$$

Then, there are 6 frequency domain features. Thus, a PPG period is represented as 17 time domain features and 6 frequency domain features.

3.3 Deep one-class classification for authentication and identification

For a user, the authentication answers whether the user is himself or herself. Thus, it is a one-class classification problem in which the PPG signals from the user are used as targets and the the PPG signals are regarded as anomalies. This paper adopts deep one-class classification as the one-class classifier. For user j , the PPG signal period is represented as $x_i \in \mathbb{R}^{23}$. The training set is represented as $X = \{x_i\}_{i=1}^n$. Then, the illustration of deep one-class classification is provided in Figure 4.

Figure 4 Illustration of deep one-class classification. The $\phi(\cdot; \mathcal{W})$ is the transformation through neural network from input space $\mathcal{X}$ to output space $\mathcal{F}$ which maps the representations of targets into a hypersphere with minimum volume. The centre and radius of hypersphere are denoted as c and R , respectively. In the mapping space, most of the targets are within the hypersphere, while the anomalies are outside the hypersphere



In Figure 4, the blue circles are targets, while the red circles are anomalies; the left part is the original space, the middle part is the neural network transformation $\phi(\cdot; \mathcal{W}) : \mathcal{X} \rightarrow \mathcal{F}$, while the right part is the output space. The neural network $\phi(\cdot; \mathcal{W}) : \mathcal{X} \rightarrow \mathcal{F}$ is with $l \in \mathbb{N}$ hidden layers. The associated weight are $\mathcal{W} = \{w^1, \dots, w^l\}$. The w^j is the weight of layer j . The $\phi(x; \mathcal{W})$ is the feature representation of x . Deep one-class classification aims to learn network weight $\mathcal{W}$ and as well as the minimum volume hypersphere (c, R) which encloses most of the targets after neural network transformation. Here, $c \in \mathcal{F}$ and $R > 0$ are the centre and radius of enclosing hypersphere. The soft-boundary deep OCC is formulated as equation (3).

$$\min_{R, \mathcal{W}} : \frac{\lambda}{2} \sum_{j=1}^l \|w^j\|_F^2 + R^2 + \frac{1}{\nu n} \sum_{i=1}^n \max \{0, \|\phi(x_i; \mathcal{W}) - c\|^2 - R^2\} \quad (3)$$

In equation (3), $\|\cdot\|_F$ represents the l_2 -norm, the first term is the weight decay regulariser, the second term is the square of radius of hypersphere, the last term punishes the points which locate outside the hypersphere, parameter ν is a balance factor to trade off the hypersphere volume and violated points and $\lambda > 0$ represents parameter to control the weight decay regulariser and hypersphere volume.

Minimising the objective in equation (3) ensures points are close to hypersphere centre c and the volume is as small as possible. The mappings of targets in the transformation space are close the hypersphere centre c , while the mapping of anomalies are further away the hypersphere centre c and outside the hypersphere.

Equation (3) can be simplified as equation (4) as follows:

$$\min_{\mathcal{W}} : \frac{\lambda}{2} \sum_{j=1}^l \|w^j\|_F^2 + \frac{1}{n} \sum_{i=1}^n \|\phi(x_i; \mathcal{W}) - c\|^2 \quad (4)$$

In equation (4), a quadratic loss is introduced to penalise the distance between neural network representation and hypersphere centre via the second term $\frac{1}{n} \sum_{i=1}^n \|\phi(x_i; \mathcal{W}) - c\|^2$, parameter λ balances network weight decay and quadratic loss. The soft-boundary deep OCC in equation (3) finds minimum hypersphere via directly penalise the radius, while equation (4) finds minimum hypersphere via minimising the mean of distances between neural network representations of targets and hypersphere centre.

For a test sample x , the associated anomaly score is defined as the distance of its neural network representation and the centre of hypersphere, which is written as equation (5).

$$Score(x) = \|\phi(x; \mathcal{W}^*) - c\|^2 \quad (5)$$

Here, $\mathcal{W}^*$ is network parameters through solving equation (5). Generally, the target has lower anomaly score, while the anomaly has higher anomaly score. For equation (4), the target has a anomaly score which is higher than R , while the anomaly has a anomaly score which is less than R . In the test stage, equation (5) is merely determined by network parameter $\mathcal{W}$ and the hypersphere centre c . Thus, the computation burden is acceptable.

The deep one-class classification generally utilises Stochastic Gradient Descent (SGD) to optimise network parameter $\mathcal{W}$ and radius R through backpropagation to obtain a local minimum. When optimising network parameter $\mathcal{W}$, hypersphere radius is fixed. When optimising hypersphere radius R , network parameter $\mathcal{W}$ is fixed.

For authentication using PPG signal in wearable IoT system, if there are p users, it needs p deep one-class classification models. Each model is associated a user. Therefore, for p user system, p deep one-class classification models are deployed in the cloud server of the IoT system. When a user uses the system, his or her PPG signal features are transmitted to cloud server to determine whether the user is himself or herself.

4 Experiments and simulations

This section first evaluates the effectiveness of deep one-class classification model for authentication on two public PPG data sets, BIDMC and TROIKA, then uses the authentication scheme in a simulation environment. The description of public PPG data sets is summarised as follows:

- BIDMC data set (Zhang et al., 2014) was obtained from critically ill patients during nursing care at Beth Israel Deaconess Medical Centre (Boston, Massachusetts, USA), and each breath in each record was manually annotated using specialised medical equipment. There are a total of 53 records from 53 patients in the data set, each lasting for 8 minutes, including physiological signals with a sampling frequency of 125 Hz, such as PPG signals, respiratory impedance signals and ECG signals; physiological parameters with a sampling frequency of 1 Hz, such as heart rate, respiratory rate and blood oxygen saturation; also some fixed information, including patient age, gender and manually labelled breathing segments.
- The TROIKA data set (Goldberger et al., 2000) records single channel PPG signals, triaxial acceleration signals and ECG signals from 12 yellow skinned male subjects aged 18 to 35. For each subject, the PPG signal is obtained from a blood oxygen meter with a green LED light (wavelength: 609 nm) worn on the wrist; The three-axis acceleration signal is recorded by the accelerometer on the wrist; The ECG signal is recorded from the chest using a wet electrocardiogram sensor. All signals are sampled at 125 Hz. During the data recording process, the subjects walked or ran on the treadmill at the following speeds: 1–2 km/h, lasting for 0.5 minutes; 6–8 km/h for 1 minute; 12–15 km/h, for 1 minute; 6–8 km/h for 1 minute; 12–15 km/h for 1 minute; 1–2 km/h for 0.5 minutes. Subjects can freely use their wristband to pull clothes, wipe sweat from their foreheads, press buttons on the treadmill and swing freely. Two experiments were conducted, with a total of 10 sets of data obtained for 8 subjects in the first experiment and 12 sets of data obtained for 12 subjects in

the second experiment. This article refers to two sets of data as TROIKA8 and TROIKA12.

The PPG signals from both BIDMC and TROIKA are first processed by bandpass filter to remove motion artifact and high-frequency interference and wavelet filter to remove baseline drift. Then, each PPG period is represented as 6 frequency domain features and 17 time domain features. Five consecutive periods are treated as a sample. The samples are divided as two parts with three quarters and one quarter, respectively. One is for training, while the other is for testing. For each person, a deep one-class classification is learnt for authentication of this person. The training set is the large part of his PPG segments. The test set consists of the small part of his PPG segments and the PPG segments from other persons.

Compare with two class classification-based authentication, deep one-class classification merely uses targets for training, which is more suitable for real situation. In two class classification-based authentication, the targets from user are treated as positive class, while the samples from other persons are treated as negative class. It may encounters some issues. First, two-class classification may meet imbalance problem since the samples from other persons are much more than targets from a user. Second, it is difficult to collect the samples from all persons, thus the distribution of negative class is too complex to depict using limited samples. Third, it is hard to extend in wearable IoT system when new user is added.

For the comparison methods, deep one-class classification is compared with three one-class classification algorithms, including One-class Support Vector Machine (OSVM) (Zhu et al., 2014), Support Vector Data Description (SVDD) (Tax and Duin, 2004) and Isolation Forest (Liu et al., 2008) and three two-class classification algorithm, including Support Vector Machine (SVM) (Zhu et al., 2016/2016b), Random Forest (RF) (Biau and Scornet, 2016) and Extreme Learning Machine (ELM) (Huang et al., 2015). The OSVM, SVDD and Isolation Forest are shallow one-class classifiers which cannot disclose the deep features of the training set. The experimental results are reported in term of the accuracy and AUC value, which are reported in Tables 1 and 2 for BIDMC data set and Tables 3 and 4 for TROIKA data set, respectively.

Table 1 The accuracy results of BIDMC data set

	<i>Two-class classification (%)</i>			<i>One-class classification (%)</i>			
	<i>SVM</i>	<i>RF</i>	<i>ELM</i>	<i>OSVM</i>	<i>SVDD</i>	<i>Isolation forest</i>	<i>Deep OCC</i>
person 1	89.38	88.21	89.47	86.03	85.74	83.00	88.36
person 2	91.43	90.84	91.72	88.71	89.04	89.08	90.44
person 3	90.28	90.55	90.14	87.92	87.32	85.01	89.54
person 4	88.57	88.04	88.13	85.83	86.59	85.89	87.36
person 5	93.64	92.36	93.21	90.54	91.18	91.13	92.77
person 6	91.36	91.12	90.85	87.26	86.41	86.21	91.05
person 7	89.72	88.87	90.17	86.39	86.19	85.50	89.23
person 8	90.59	89.81	89.26	87.52	88.24	85.11	89.54
person 9	92.17	91.34	91.68	89.57	88.74	85.90	92.31
person 10	94.52	92.76	93.71	91.69	91.72	90.82	92.33
Avg.	91.17	90.39	90.83	88.15	88.12	86.76	90.29

Table 2 The AUC results of BIDMC data set

	Two-class classification (%)				One-class classification (%)		
	<i>SVM</i>	<i>RF</i>	<i>ELM</i>	<i>OSVM</i>	<i>SVDD</i>	<i>Isolation forest</i>	<i>Deep OCC</i>
person 1	88.31	88.29	87.21	87.55	89.52	88.51	89.64
person 2	89.23	90.26	90.23	89.68	90.40	88.57	89.36
person 3	88.72	88.08	87.24	88.25	88.26	89.40	88.46
person 4	87.26	87.29	87.06	85.74	87.64	87.80	87.80
person 5	90.58	91.69	90.42	92.46	90.08	90.22	91.72
person 6	89.84	90.01	89.33	91.55	89.95	90.24	91.44
person 7	88.49	86.86	88.48	88.66	87.06	87.98	90.81
person 8	89.23	89.70	89.38	90.42	90.61	89.38	90.44
person 9	90.36	88.92	89.87	91.32	88.71	89.49	91.08
person 10	91.27	89.68	90.62	91.89	90.04	91.70	92.77
Avg.	89.33	89.08	88.99	89.75	89.23	89.33	90.35

Table 3 The accuracy result of TROIKA

	Two-class classification (%)				One-class classification (%)		
	<i>SVM</i>	<i>RF</i>	<i>ELM</i>	<i>OSVM</i>	<i>SVDD</i>	<i>Isolation forest</i>	<i>Deep OCC</i>
person 1	83.54	84.78	83.26	81.49	81.42	81.35	83.76
person 2	85.39	85.66	86.26	83.63	84.50	83.52	84.66
person 3	82.87	81.91	81.77	82.32	82.34	80.58	81.64
person 4	84.36	85.16	85.00	82.23	82.06	82.80	83.43
person 5	85.29	84.85	84.17	84.58	84.67	82.76	85.57
person 6	83.72	82.67	83.77	82.60	83.06	81.46	84.33
person 7	84.63	84.17	83.71	83.27	83.72	83.42	83.33
person 8	85.17	84.65	84.64	84.15	84.36	82.86	84.20
person 9	81.49	80.77	81.08	80.79	79.32	79.89	80.55
person 10	83.27	83.91	83.22	81.27	81.79	81.61	83.66
person 11	82.54	82.58	82.21	81.97	80.65	80.91	81.32
person 12	81.87	81.39	81.29	80.28	79.82	79.51	81.55
Avg.	83.68	83.54	83.36	82.38	82.31	81.72	83.17

Table 4 The AUC results of TROIKA

	Two-class classification (%)				One-class classification (%)		
	<i>SVM</i>	<i>RF</i>	<i>ELM</i>	<i>OSVM</i>	<i>SVDD</i>	<i>Isolation forest</i>	<i>Deep OCC</i>
person 1	80.43	80.99	81.26	79.31	81.56	80.95	82.95
person 2	84.26	82.38	82.46	83.46	82.18	81.08	83.96
person 3	82.61	79.92	80.53	79.64	81.41	79.44	82.04
person 4	84.41	82.22	82.18	81.39	80.74	81.95	83.82
person 5	83.81	82.51	82.72	82.25	85.22	82.90	85.18
person 6	81.63	82.74	81.26	84.66	81.40	80.78	82.45
person 7	81.85	84.19	84.06	83.60	82.61	83.62	83.25
person 8	82.57	81.66	82.52	83.59	83.46	81.81	84.27
person 9	80.24	78.08	78.19	79.86	76.92	77.30	78.42
person 10	83.28	80.75	81.06	80.31	81.54	81.44	83.28
person 11	81.23	81.31	81.65	82.99	81.30	81.33	82.33
person 12	81.03	80.64	81.45	82.49	80.57	82.03	83.83
Avg.	81.78	81.67	81.72	81.59	81.93	82.10	82.98

The BIDMC data set has 53 records from 53 persons. In the experiments, merely 10 persons are used, who are denoted as person 1 to person 10, respectively. In order to eliminate the randomness during splitting the data from each person for training and testing, the experiments are repeated 20 times. The accuracy and AUC values in Tables 1 to 4 are reported as the mean of 20 times. The last row in Tables 1 and 2 is the average accuracy and AUC value of 10 persons in BIDMC data set, while the last row in Tables 3 and 4 is the average accuracy and AUC value of 10 persons in TROIKA.

In Table 1, it can be found that the average accuracy of 10 persons in BIDMC data set achieves 91.17%, 90.39%, 90.83%, 88.15%, 88.12%, 86.76% and 90.29% for SVM, RF, ELM, OSVM, SVDD, Isolation Forest and Deep OCC, respectively. The average accuracy of two-class classification models are better than one-class classification models, especially three shallow one-class classification models. The average accuracy of Deep OCC is very close to that of two-class classification models. The reason is that two-class classification models use both positive class and negative class for training.

In Table 2, it can be found that the average AUC value of 10 persons in BIDMC data set achieves 89.33%, 89.08%, 88.99%, 89.75%, 89.23%, 89.33% and 90.35% for SVM, RF, ELM, OSVM, SVDD, Isolation Forest and Deep OCC, respectively. Although the average accuracy of two-class classification models are higher than one-class classification models 3.02%~4.41% except Deep OCC, the difference of average AUC values of two-class classification models are very close to that of shallow one-class classification models. Especially, the average AUC value of Deep OCC is higher than two-class classification models and shallow one-class classification models. The reason is that two-class classification models considers negative class during training which is much larger than positive class. For an imbalance data set, the accuracy cannot reflect the true results. For instance, for a data set consisting of 100 positive samples and 9900 negative samples, if predicting all samples as negative samples, the accuracy still can reach 99%.

In Table 3, it can be found that the average accuracy of 12 persons in TROIKA data set achieves 83.68%, 83.54%, 83.36%, 82.38%, 82.31%, 81.72% and 83.17% for SVM, RF, ELM, OSVM, SVDD, Isolation Forest and Deep OCC, respectively. It can still obtain that the average accuracy of two-class classification models are better than one-class classification models, which is consistent with the conclusion from average accuracy results of BIDMC data set.

In Table 4, it can be found that the average AUC value of 10 persons in TROIKA data set achieves 81.78%, 81.67%, 81.72%, 81.59%, 81.93%, 82.10% and 82.98% for SVM, RF, ELM, OSVM, SVDD, Isolation Forest and Deep OCC, respectively. The average AUC value of 12 persons in TROIKA data set shows the same result as that from BIDMC data set.

In both BIDMC data set and TROIKA data set, Deep OCC shows comparative performance, especially the AUC

value. The performance of BIDMC data set is better than that of TROIKA data set. The reason is that the PPG signals in TROIKA are collected under different environment, which may cause the collected signals to contain more noises.

Then, the proposed authentication scheme is deployed in a wearable IoT environment that has 10 edge nodes and a cloud server. The associated Deep OCC models are deployed in the cloud server. There are 10 Deep OCC models which learn using the PPG signals from 10 persons. The edge nodes can get the authentication result from cloud server within 0.01 s on average, which can meet the real application.

5 Conclusion

Compared with traditional network, the Internet of Things (IoT) has limited resources for computing. It is impossible to deploy a large model in IoT environment directly. The terminal wearable devices are vulnerable to invasion. Thus, it has become a challenging task to implement security protection under limited computing resources in wearable IoT environment. In order to solve this issue, this paper designs a lightweight authentication scheme for security protection under wearable IoT environment. The scheme utilises PPG signal as biometric feature. Compared with face, iris, fingerprint, ECG signal, and EEG signal, the PPG signal is easy to obtain and hard to forged. In order to implement lightweight deployment at terminal devices, the authentication scheme adopts edge-cloud architecture. At the edge node, the PPG signal is collected using a finger tip and the collected PPG signal is merely processed to remove the noise and to extract identical features to reduce the computing burden. At the cloud server, the deep one-class classification models are deployed, which are trained using existing PPG signal library offline. Compared with shallow one-class classification models, deep one-class classification shows superior performance in terms of accuracy and AUC value. Compared with two-class classification models, deep one-class classification is more flexible. In this paper, for a system with p persons, it needs p independent Deep SVDD models. In the future, how to use a single model is a challenging task in authentication problem, which can be treated as a multi-class supervised novelty detection problem (Zhu et al., 2023).

References

- Biau, G. and Scornet, E. (2016) 'A random forest guided tour', *Test*, Vol. 25, pp.197–227.
- Cao, Y., Zhang, Q., Li, F., Yang, S. and Wang, Y. (2020) 'Ppgpass: nonintrusive and secure mobile two-factor authentication via wearables', *Proceedings of the IEEE INFOCOM Conference on Computer Communications*, IEEE, pp.1917–1926.

- Ferreira, C.C. and Lind, F. (2023) 'Supplier interfaces in digital transformation: an exploratory case study of a manufacturing firm and iot suppliers', *Journal of Business and Industrial Marketing*, Vol. 38, No. 6, pp.1332–1344.
- Goldberger, A.L., Amaral, L.A.N., Glass, L., Hausdorff, J.M., Ivanov, P.C., Mark, J.E., Mietus, Moody, G.B., Peng, C-K. and Stanley, H.E. (2000) 'Physiobank, physiotoolkit, and physionet: components of a new research resource for complex physiologic signals', *Circulation*, Vol. 101, No. 23, pp.e215–e220.
- Gu, Y.Y. and Zhang, Y.T. (2003) 'Photoplethysmographic authentication through fuzzy logic', *Proceedings of the IEEE EMBS Asian-Pacific Conference on Biomedical Engineering*, IEEE, pp.136–137.
- Gu, Y.Y., Zhang, Y. and Zhang, Y.T. (2003) 'A novel biometric approach in human verification by photoplethysmographic signals', *Proceedings of the 4th International IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine*, IEEE, pp.13–14.
- Hansen, E.B. and Bøgh, S. (2021) 'Artificial intelligence and internet of things in small and medium-sized enterprises: a survey', *Journal of Manufacturing Systems*, Vol. 58, pp.362–372.
- Hassan, W.H. et al (2019) 'Current research on internet of things (iot) security: a survey', *Computer Networks*, Vol. 148, pp.283–294.
- Huang, G., Huang, G-B., Song, S. and You, K. (2015) 'Trends in extreme learning machines: a review', *Neural Networks*, Vol. 61, pp.32–48.
- Jaafar, N.A.L., Sidek, K.A. and Azam, S.N.A.M. (2015) 'Acceleration plethysmogram based biometric identification', *Proceedings of the International Conference on BioSignal Analysis, Processing and Systems (ICBAPS)*, IEEE, pp.16–21.
- Karimian, N., Guo, Z., Tehranipoor, M. and Forte, D. (2017) 'Human recognition from photoplethysmography (ppg) based on non-fiducial features', *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, IEEE, pp.4636–4640.
- Kavsaoğlu, A.R., Polat, K. and Bozkurt, M.R. (2014) 'A novel feature ranking algorithm for biometric recognition with ppg signals', *Computers in Biology and Medicine*, Vol. 49, pp.1–14.
- Laghari, A.A., Wu, K., Laghari, R.A., Ali, M. and Khan, A.A. (2021) 'A review and state of art of internet of things (iot)', *Archives of Computational Methods in Engineering*, pp.1–19.
- Lee, A. and Kim, Y. (2015) 'Photoplethysmography as a form of biometric authentication', *Proceedings of the IEEE SENSORS*, IEEE, pp.1–2.
- Li, D., Chen, X., Li, Q., Zhu, F., Lu, X., Routray, S., Ghosh, U. and AL-Numay, M. (2024a) 'Intelligent biomedical photoplethysmography signal cycle division with digital twin in metaverse for consumer health', *IEEE Transactions on Consumer Electronics*, Vol. 70, pp.2116–2128.
- Li, R., Li, Q., Huang, Y., Zou, Q., Zhao, D., Zhang, Z., Jiang, Y., Zhu, F. and Vasilakos, A.V. (2024b) 'Seiot: detecting anomalous semantics in smart homes via knowledge graph', *IEEE Transactions on Information Forensics and Security*, Vol. 19, pp.7005–7018.
- Liu, F.T., Ting, K.M. and Zhou, Z.H. (2008) 'Isolation forest', *Proceedings of the 8th IEEE International Conference on Data Mining*, IEEE, pp.413–422.
- Nadzri, N.I.M., Sulaimi, M., Umadi, L.F. and Sidek, K.A. (2016) 'Photoplethysmogram based biometric recognition for twins', *Indian Journal of Science and Technology*, Vol. 9, pp.1–9.
- Rejeb, A., Rejeb, K., Simske, S., Treiblmaier, H. and Zailani, S. (2022) 'The big picture on the internet of things and the smart city: a review of what we know and what we need to know', *Internet of Things*, Vol. 19. Doi: 10.1016/j.iot.2022.100565.
- Salanke, N.S.G.R., Maheswari, N., Samraj, A. and Sadhasivam, S. (2013) 'Enhancement in the design of biometric identification system based on photoplethysmography data', *Proceedings of the International Conference on Green High Performance Computing (ICGHPC)*, IEEE, pp.1–6.
- Sarkar, A., Abbott, A.L. and Doerzaph, Z. (2016) 'Biometric authentication using photoplethysmography signals', *Proceedings of the IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, IEEE, pp.1–7.
- Spachos, P., Gao, J. and Hatzinakos, D. (2011) 'Feasibility study of photoplethysmographic signals for biometric identification', *Proceedings of the 17th International Conference on Digital Signal Processing (DSP)*, IEEE, pp.1–5.
- Tax, D.M.J. and Duin, R.P.W. (2004) 'Support vector data description', *Machine Learning*, Vol. 54, pp.45–66.
- Xiao, L., Wan, X., Lu, X., Zhang, Y. and Wu, D. (2018) 'Iot security techniques based on machine learning: how do iot devices use ai to enhance security?', *IEEE Signal Processing Magazine*, Vol. 35, No. 5, pp.41–49.
- Yadav, U., Abbas, S.N. and Hatzinakos, D. (2018) 'Evaluation of ppg biometrics for authentication in different states', *Proceedings of the International Conference on Biometrics (ICB)*, IEEE, pp.277–282.
- Zhang, Z., Pi, Z. and Liu, B. (2014) 'Troika: a general framework for heart rate monitoring using wrist-type photoplethysmographic signals during intensive physical exercise', *IEEE Transactions on Biomedical Engineering*, Vol. 62, No. 2, pp.522–531.
- Zhao, T., Wang, Y., Liu, J., Chen, Y., Cheng, J. and Yu, J. (2020) 'Trueheart: continuous authentication on wrist-worn wearables using ppg-based biometrics', *Proceedings of the IEEE INFOCOM Conference on Computer Communications*, IEEE, pp.30–39.
- Zhu, F., Yang, J., Gao, C., Xu, S., Ye, N. and Yin, T. (2016a) 'A weighted one-class support vector machine', *Neurocomputing*, Vol. 189, pp.1–10.
- Zhu, F., Yang, J., Gao, J. and Xu, C. (2016b) 'Extended nearest neighbor chain induced instance-weights for svms', *Pattern Recognition*, Vol. 60, pp.863–874.
- Zhu, F., Ye, N., Yu, W., Xu, S. and Li, G. (2014) 'Boundary detection and sample reduction for one-class support vector machines', *Neurocomputing*, Vol. 123, pp.166–173.
- Zhu, F., Zhang, W., Chen, X., Gao, X. and Ye, N. (2023) 'Large margin distribution multi-class supervised novelty detection', *Expert Systems with Applications*, Vol. 224. Doi: 10.1016/j.eswa.2023.119937.