Received: November 29, 2023. Revised: January 14, 2024. 22

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

# Human Activity Recognition for Elderly People Using Pseudonym-Based Conditional Privacy-Preservation Authentication

**Erita Cicilia Febrianti[1] Amang Sudarsono[1]* Tri Budi Santoso[1]**

[1]*Department of Informatics and Computer Engineering, Politeknik Elektronika Negeri Surabaya, Indonesia*
* Corresponding author's Email: amang@pens.ac.id

**Abstract:** As technological advancements continue to evolve, Human Activity Recognition (HAR) has emerged as a crucial area. This study aims to discern four human activities are sitting, standing, walking, and jogging while prioritizing user privacy by employing Elliptic Curve Cryptography (ECC) based blind signatures. The research focuses on predicting human activities through the Support Vector Machine (SVM) algorithm, utilizing data from accelerometer, gyroscope and Global Positioning System (GPS) sensors in smartphones. ECC, renowned for its shorter key length and faster processing, ensures data confidentiality. The SVM algorithm excels in categorizing human activities, achieving an impressive validation accuracy of around 99.16% with an average error of merely 3.33% in 30 real-time tests encompassing standing and walking. Notably, tests for sitting and running activities showed no errors. Moreover, the system's practicality is evident as the classification process requires only 1 ms. ECC's blind signature implementation effectively upholds user anonymity, fulfilling crucial criteria such as confidentiality, correctness, integrity, non-repudiation, blindness, unforgeability, and untraceability, without imposing substantial computational costs.

**Keywords:** Human activity recognition, Mobile crowd sensing, SVM, Blind signature, ECC.

## 1. Introduction

Globally, the proportion of adults aged 60 and above is growing faster than any other age group. It is expected that in 2025 there will be approximately 1.4 billion elderly people in the world, and in 2050 there will be 2.1 billion, especially in developing countries. Healthcare systems face major challenges from this growth, as aging is associated with decreased physical activity, impacting both physical and mental health. As more and more elderly people suffer from age-related diseases and malfunctions of body parts, the demand for intelligent health support systems is increasing year by year [1-3]. Because of this, there is a need to create a monitoring activity recognition that is used as an innovation that supports the well-being of the elderly [4]. As a result, several recent research projects in the HAR sector have focused on the sensor-based real-time monitoring system to promote independent living at home [2].

Activity recognition is the technique of classifying a series of human activities by interpreting sensor data [5]. One of the main applications of wearable technology in the field of healthcare is the identification of daily activities [6]. Over the last few years, research on HAR has grown significantly because of the development of low-cost, less intrusive mobile sensing platforms like smartphones. Smartphones are cutting edge HAR platforms because they come with a variety of wireless interfaces, are simple to use, have high processing and storage capacities, and have sensors like gyroscopes, accelerometers, and compass that satisfy the practical and technical requirements for HAR tasks [7-10].

As wireless communication technology advances and mobile smart devices become more commonplace, more individuals feel empowered to share their observations and insights with others, leading to the rise of Mobile Crowd Sensing (MCS) [11]. With the advancement of sensor technology and

mobile computing, HAR can be extended to MCS, where MCS is a new innovation in IoT that has advantages in the process of acquiring sensor data from the surrounding environment [12]. The availability of multiple sensors integrated with smartphones or wearable devices is one of the advantages of the MCS paradigm [13]. The paradigm of mobile crowdsensing will enhance HAR methods, systems, and approaches. This is caused by a number of factors, including the following: crowdsensing increases human mobility, supporting improved patient or elderly monitoring; and crowdsensing allows for the collection of large amounts of data that can be used to evaluate and monitor individuals [14]. In addition to several advantages, security, and privacy [15-17], the accuracy and dependability of sensed data [18], and participation incentives [19] are very important in the MCS system. In MCS, users' personal data including location and identity information is vulnerable to privacy attacks [20]. Consequently, it is critical to secure MCS participants' privacy [21], because mobile devices are controlled by selfish and autonomous users who can launch insider attacks such as raising privacy concerns and faked sensing attacks [22]. An attacker has the ability to intercept MCS transmission and get sensitive user data from sensor data. An adversary may, for instance, utilize GPS sensor readings to gather private data about MCS members, such as their home address and daily commute. Most MCS users are hesitant to take part in sensing jobs because they are aware that their sensitive data may be vulnerable [12]. Some kinds of attacks on MCS includes Spoofing, Malware, Jamming, Denial of Service (DoS), and etc [22]. Challenges to the security and privacy of user data become important using the MCS method, by adding security algorithms to the system.

So, in this research proposal, the contribution is using SVM for classification and employing pseudonym-based MCS with ECC based blind signature in enhancing the security and privacy of sensor data collected from 100 volunteers. Utilizing SVM can assist in accurately classifying various human activities from sensor data, while employing pseudonym-based MCS with ECC based blind signature can potentially enhance privacy and security by anonymizing user identities and securing the transmitted data. The proposed approach of combining SVM for classification and pseudonym-based MCS with ECC based blind signature aims to address several challenges in HAR security and privacy within the MCS paradigm. By utilizing SVM, the system can effectively classify diverse activities based on sensor data patterns. Integrating pseudonym-based MCS with ECC based blind signature enhances user protection identities and ensures secure transmission of sensitive data. SVM is a powerful machine learning technique useful for classifying data. Applying SVM in activity recognition can improve the accuracy of identifying daily activities among the elderly, thus aiding in better monitoring and support for their well-being. Integrating pseudonym-based MCS using ECC based blind signature ensures enhanced privacy and security for user data. This method allows volunteers to participate in data sensing without revealing their true identities or compromising sensitive information. The use of ECC enhances cryptographic security, while blind signatures further protect user anonymity. By combining these technologies and methodologies, our research can provide a robust framework for HAR in the context of elderly care, ensuring both accuracy in activity classification and strong privacy protection for the volunteers involved in the sensing process.

The rest of this paper is organized into the following sections. Section 2 contains related works. The proposed system will be explained in Section 3. The measurement and result will be discussed in Section 4. The performance analysis will be discussed in Section 5. The conclusion of this paper in Section 6.

## 2. Related works

Some research on Human Activity Recognition in Mobile Crowd Sensing included Alaa et.al. [14]. This research focuses on the development and evaluation of a particle swarm optimization (PSO) based algorithm called PSO-kNN for recognizing human activities in a mobile crowdsensing environment. The authors highlight the challenges in this research area, such as collecting and managing big, noisy data, and propose the PSO-kNN algorithm to address these challenges. The paper presents three main experiments: a simulated example to illustrate how the PSO algorithm searches for the optimal value of k, testing the proposed model using standard datasets, and recognizing human activities using the PSO-kNN algorithm. The results of the experiments demonstrate the effectiveness of the proposed algorithm in achieving competitive classification performance. The related data used in this paper includes standard datasets such as Iris, Wine, Pima Indians Diabetes, ORL, Yale, and Ovarian. These datasets vary in terms of the number of samples, classes, and dimensions, providing a diverse set of data for evaluating the proposed PSO-kNN algorithm. Additionally, the paper utilizes data obtained from

the University of California at Irvine (UCI) Machine Learning Repository for recognizing human activities. This dataset consists of feature vectors collected from eight subjects, each performing 19 activities using three different sensors: Accelerometer, Gyroscopes, and Magnetometer. The paper provides valuable contributions to the field of MCS and HAR, offering a novel algorithm and empirical evidence of its performance. The use of diverse standard datasets and real-world data from the UCI repository adds credibility to the findings and demonstrates the algorithm's applicability across different contexts. However, in this research user privacy is not addressed.

In other research of Lyu et.al. [23] discusses the privacy issues surrounding wearable data collection and reporting for mobile crowdsensing, a type of collaborative deep learning. The authors suggest RG-RP, a two-stage privacy-preserving technique that tries to lessen transmission energy and lessen maximum a posteriori (MAP) estimation attacks. A row-orthogonal random projection (RP) matrix is used in the second stage to project high-dimensional data to a lower dimension, while a nonlinear function known as repeated Gompertz (RG) is used in the first stage to perturb each participant's data. In order to improve upon standalone models, the paper also presents a novel LSTM-CNN model for collaborative learning that combines Long Short-Term Memory (LSTM) and Convolutional Neural Networks (CNN). Two real-world wearable datasets, the HAR dataset and the Mobile Health (MH) dataset, are given the accuracy results for the raw data and the perturbed data. The LSTM-CNN architecture produced raw data accuracy of 98.44% and perturbed data accuracy of 93.75% for the HAR dataset. This shows that, in comparison to the outcome from the raw data, the suggested privacy-preserving two-stage method reduced the accuracy by just 4.76%. The LSTM-CNN architecture produced raw data accuracy of 95.56% and perturbed data accuracy of 92.08% for the MH dataset. In a similar vein, accuracy was decreased by 3.64% when using perturbed data instead of raw data. The architecture of mobile crowd-sensing, privacy issues with sharing data from wearable sensors, and the need for privacy-preserving algorithms to promote data sharing while safeguarding user privacy are all covered in this paper. It presents the RG-RP scheme and assesses, using both artificial and real-world datasets, how well it defends against MAP estimation attacks. The paper also introduces and shows the efficacy of the LSTM-CNN model in collaborative learning for HAR. One potential disadvantage is that injecting noise directly into users' raw private data could compromise data integrity and introduce inaccuracies.

Research of Owoh et.al. [24] examines the security and privacy issues in mobile crowd sensing applications. Mobile crowd sensing utilizes sensors on smartphones and other mobile devices to collect environmental and user activity data at scale. As this emerging paradigm grows in usage, protecting sensitive personal information contained in the collected sensor data becomes critically important. The paper analyzes 40 Android-based mobile crowd sensing applications from three categories: smart city applications, health applications, and fitness applications. These apps leverage common smartphone sensors like GPS, accelerometer, and gyroscope to gather location and motion data from users. The smart city category includes 20 transportation and traffic monitoring apps. 10 health apps related to activity tracking, diet, and more were selected. The final 10 apps focused on fitness tracking of activities like running and cycling. All 40 apps transmit the collected sensor data to backend servers over the internet for analysis and insights. The paper provides a table outlining each application, the sensors utilized, and communication method. This contextualizes the scope and data sources considered in the study. To evaluate security, the researchers used a dynamic analysis approach intercepting network traffic between the apps and servers using Burp Suite. This allowed analyzing how sensor payloads were transmitted and whether sensitive user information could be disclosed. Analysis findings showed location and sensor data for all 40 apps was sent unencrypted in cleartext over the internet, allowing full disclosure of private user GPS location traces and activity information. The researchers also achieved a 100% success rate intercepting traffic, demonstrating a lack of effective security controls. In response, the paper proposes a novel encryption and authentication scheme for crowd sensed data based on the AES-256/GCM algorithm. This aims to securely transmit location and motion sensor data streams with confidentiality, integrity, and authentication guarantees.

However, this research does not address the issue of user anonymity privacy, where it only focuses on the location of user data by encrypting the data using AES-256/CGM Algorithm.

Research of Wang et.al. [25] presents a privacy-preserving collaborative computation framework for HAR using edge computing, secure aggregation algorithms, and blockchain. The framework aims to enable data owners to collaboratively train an accurate HAR model while ensuring the privacy of

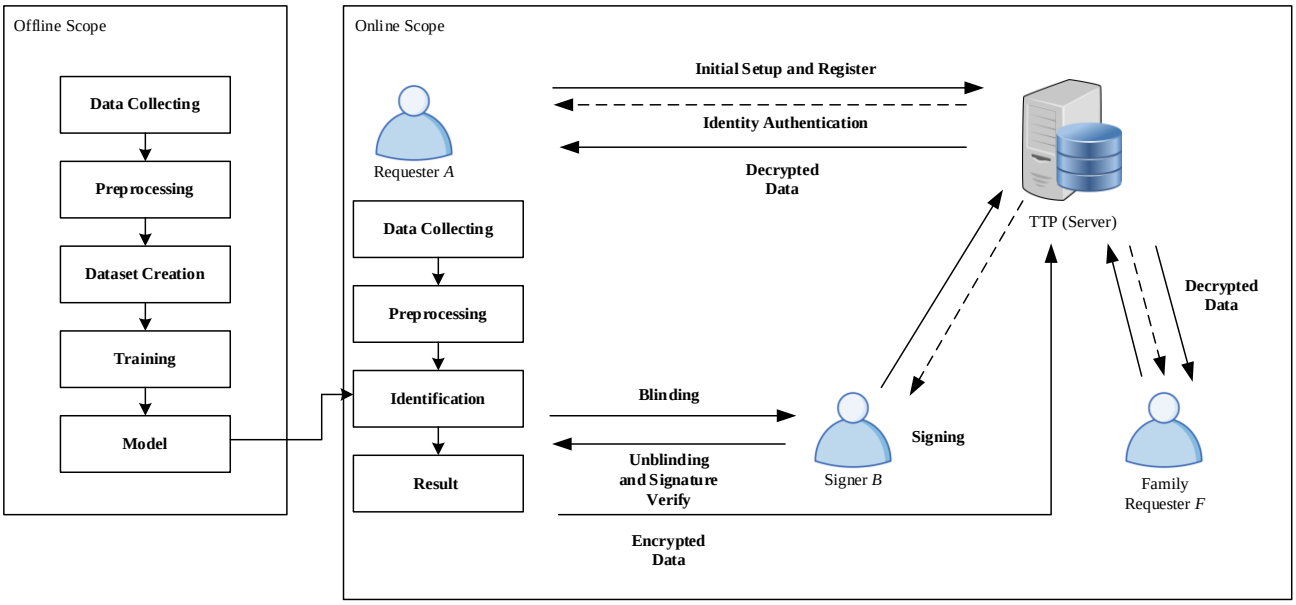



Figure. 1 Proposed Scheme

training data. It leverages federated learning to keep model training procedures on local devices without transmitting data to a central server, thus addressing issues related to data privacy, storage, and bandwidth. The use of secure multiparty computation techniques and blockchain enhances the security and verifiability of the system. The experimental results demonstrate the effectiveness of the proposed framework, achieving an accuracy of 93.24% in the HAR model training process. The framework consists of several key components and processes. It begins with data collection from smart devices, followed by local training of the model on edge nodes using the collected data. The local updates are then aggregated using a secure aggregation algorithm, and the results are stored in a new block on the blockchain. The block structure includes the global model, updates after aggregation, hash value of the previous block, and commitments of the node updates. The framework's performance was evaluated through experiments, demonstrating its usability and efficiency. While the framework presents several advantages, such as privacy protection, efficient training, and security features, there are also some potential disadvantages and limitations to consider include: the use of secure multiparty computation techniques increases the training time, with a round of iterations taking 36.4 seconds to execute. Although this is deemed acceptable, it still represents an increase in training time compared to traditional methods.

From some of the shortcomings of some of the research above, including the problem of user anonymity, the addition of noise to user raw data, the problem of data training time and accuracy. In our research, we propose not adding noise to the raw user data so that it still produces high accuracy values and fast training times using the SVM algorithm by ensuring user anonymity by using ECC-based blind signatures with security attributes of blindness, untraceability, confidentiality, correctness, integrity, nonrepudiation, and unforgeability.

## 3. Proposed system

The proposed system integrates two main components: a machine learning scheme using Support Vector Machine (SVM) algorithms for activity recognition and a secure blind signature using Elliptic Curve Cryptography (ECC) for preserving user anonymity. In the machine learning scheme using supervised learning techniques has two main phases: training phase and testing phase. During the training phase, the input data is used to determine the classifier parameters, i.e., training samples, and the corresponding output, i.e., target. While in the testing phase according to Luts et.al. [26], a classifier can then be used to estimate the class labels of unknown samples with certain parameters that control the accuracy of the classifier [27]. In the blind signature scheme, the server as the Third Trusted Party (TTP) will generate as many keys as users, in this case 100 users. On generating public and private keys in the ECC algorithm using curve secp256k1 with equation $y^2 \equiv x^3 + 7 \, (mod \, p)$ with a bit length of 256 bits. The public key will be stored in the database. While the private key will be stored in the server's local storage which will be provided

when the user makes a registration request. The classifier results obtained previously by the user will be blinded to preserve the user's anonymity. The integration of SVM for activity recognition and ECC-based blind signatures with a focus on user anonymity in a healthcare context, particularly for the elderly, is novel. Preserving privacy while conducting accurate activity recognition is a significant contribution.

Our proposed scheme consists of two scopes: offline scope and online scope. The offline scope consists of 4 phases, namely data collecting, preprocessing, dataset creation, training data. While in the online scope there are 10 phases namely initial configuration and registration, identity verification, data collecting, preprocessing, identification result, blinding phase, signing phase, unblinding phase and signature verification, encryption phase, and decryption phase and the Notations and Descriptions" section provides a summary of the mechanism's notations and descriptions of abbreviations. There are three participants in our blind signature protocol, namely, a Requester *A*, a Signer *B*, and a family Requester *F*. Then the server *S* as a Third Trusted Party (TTP) is responsible for issuing a secure identity to the user and generating the system parameters.

## 3.1 Offline scope

In the offline scope, data is collected which will then be labelled according to the activities carried out by the user. Data that has been obtained during data collection will be pre-processed which consists of 3 stages, namely filtering, feature extraction and normalization. The data that has been obtained after the normalization process will be trained on Machine Learning to carry out the classification process and obtain a model from the training results.

### 3.1.1 Data collecting

In collecting raw data using accelerometer and gyroscope sensors on smartphone. The data collected will be labelled according to the activities. This sensor value will be retrieved and used for data processing. On the accelerometer sensor, 3 values will be obtained namely (x, y, z). While on the gyroscope will also get 3 values namely ($\phi$, $\theta$, $\psi$). The smartphone used is Samsung Galaxy A54 which has an accelerometer and gyroscope. In this research the smartphone will be placed in the fixed position on the right thigh. An illustration of smartphone placement can be seen in Fig. 2. In this research, a data 3, including:

Figure. 2 Illustration of Smartphone Placement

1. Sitting and standing activities will be sampled with a period of 1000ms as much as 50 data, so that 1 data/second is obtained.
2. Walking activities will be sampled with a period of 500ms as much as 50 data, so that 2 data/second is obtained.
3. Jogging activity will be sampled with a period of 250ms as much as 50 data, so that 4 data/second is obtained.

### 3.1.2 Preprocessing

In the data collection process, the data is not filtered. So, it needs to be filtered to make the data pattern more visible. Fig. 3 shows the raw data accelerometer.

In the raw data has a lot of high-frequency noise so it is necessary to be filtered using a low-pass filter. In this research, the filtering process uses variant IIR Filter. Low Pass filter is a good way to remove noise (Both mechanical and electrical) [28]. IIR Filter has a fast computation and has no delay, so there is no time delay. Since we don't want any time delays, an IIR filter might be appropriate [29].

The Low Pass process using an IIR filter can be calculated using Eq. (1)

$$H(z) = \frac{b_0 + b_1 z^{-1} + \cdots + b_n z^{-m}}{1 + a_1 z^{-1} + \cdots + a_n z^{-m}} \quad (1)$$

Fig. 4 shows the comparison between raw data and filtered data. As we can see the pattern of data looks smoother, this is because noise in the raw data signal has been removed.

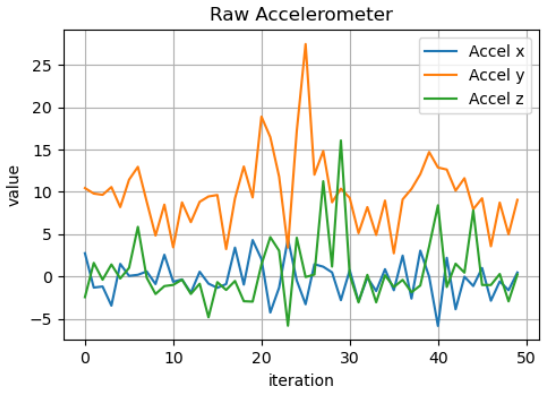



Figure. 3 Raw Data Accelerometer

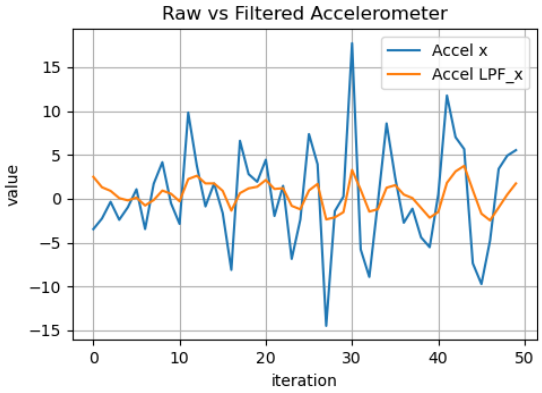



Figure. 4 Raw Data and Filtered Data Accelerometer *x*-Axis

The next process after the filtering process is feature extraction or selection of characteristics or features of each activity. From the filtering results, the main features obtained are accelerometer sensors *x*, *y*, and *z* axis and gyroscope $\phi$, $\theta$, $\psi$ axis which have been filtered. The feature data is then carried out feature mapping with the measurement function such as mean value, standard deviation, min value and max value.

The next step is the process of normalization using the z-score technique. This is because data has various ranges. A range that is too wide is feared to be a long computation process. Therefore, we need to normalize data. This normalization process using z-score. The results of normalization using the z-score are in the range between -3 until 3 but can be higher or lower. The equation of z-score can be seen in Eq. (2):

$$Z = \frac{x-\mu}{s} \quad (2)$$

Where $x$ is the raw data, $\mu$ is the average of the of the attribute population, $s$ is the standard deviation of the attribute population.

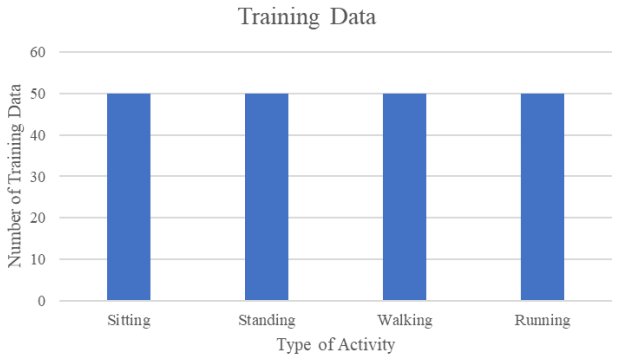



Figure. 5 Number of Training Data

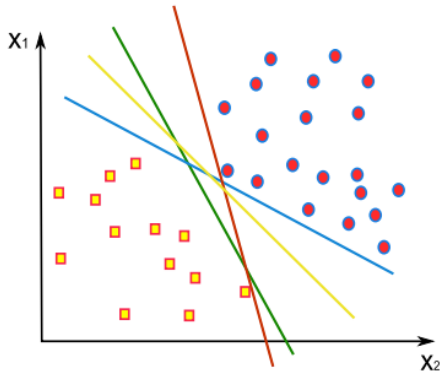



Figure. 6 SVM tries to find the best hyperplane that separates classes -1 and 1[31]

### 3.1.3 Dataset Creation

After the data data is normalized. The data will be used for the training process of the machine learning models. In creating the dataset, the dataset file will be converted into the .dat file format, which corresponds to the dataset format required in the data training process using libSVM. Following are the data formats used in libSVM [30] :

$< label >< index1 >: < value1 >< index >: ...$

where $< label >$is a binary (-1, 1) or multi-class class, $< index >$ is an attribute representing an integer from 1 to n and $< value >$is a feature value representing a real number

### 3.1.4 Training data

In the data training stage, the total data used in the training process is 200 data consisting of 50 sitting data, 50 standing data, 50 walking data, and 50 Jogging data. The training stage is used to obtain the coordinates of the support vector, weight, bias and distance of the support vector.

Support vector machine (SVM) is a supervised learning method commonly used for classification (such as support vector classification) and regression (support vector regression). SVM is a machine

learning method that works on the principle of Structural Risk Minimization with the aim of finding the best hyperplane that separates two classes in the input space. The basic principle of SVM is a linear classifier, which has been further developed to tackle nonlinear problems. By integrating the concept of kernel tricks into a high-dimensional workspace.

a. Pattern Recognition Using SVM

The SVM concept can be explained simply as an effort to find the best hyperplane that functions as a separator for two classes in the input space. Patterns belonging to class –1 are symbolized in orange, while patterns in class +1 are symbolized in red. The classification problem can be interpreted by trying to find the line (hyperplane) that separates the two groups.

Suppose there are 2 classes, denoted as $X \in R^d$ ($d$ is the number of classes), while the labels for each class are denoted $y_i \in \{-1, 1\}$, set $W = \{w_1, w_2, \dots, w_d\}$; $W$ is the weight, and the training tuple $X = \{x_1, x_2\}$, where $x_1$, $x_2$ are the attribute values $A_1$ and $A_2$, the hyperplane function can be denoted as follows:

$$f(x) = \vec{w}.\vec{x} + b \tag{3}$$

where $b$ is the bias which has a scalar quantity

b. Kernel Method

In general, the classification case is a non-linear case, so the kernel method is used to overcome this problem. Using the kernel method, a data $x$ input space is mapped to feature space F with a higher dimension via map $\varphi\left(\varphi : x \rightarrow \varphi\left(x\right)\right)$. Therefore, $x$ in input space becomes in feature space. Many times, the function is not available or cannot be counted. But the dot product of two vectors can be calculated, both in input space and in feature space.

$$K(X_i.X_j^T) = \varphi\left(X_i\right).\varphi\left(X_j\right) \tag{4}$$

## 3.2 Online Scope

In the online scope, the user first registers, then the server performs verification authentication, then the user can record the activities performed and the android performs activity classification where the model obtained from the training results will be compared with the feature extraction results obtained in real time. Furthermore, blind data and data encryption are carried out. Then testing the system that has been designed to evaluate the system as a whole.

### 3.2.1 Initial Configuration and Registration

In order to configure the system, we first specify the domain's specifications during the first registration step. The following are the default parameters, which consist of many important fields.

(i) Create a robust elliptic curve, denoted as $E\ (Fq)$ over the finite field $Fq$ where $q$ is represents a substantial prime number exceeding 256 bits. The size ensures a level of security equivalent to a 3072-bit RSA key. Next, on the elliptic curve $E\ (Fq)$, an order $d$ and base point $G$ will be chosen. The appropriate choice satisfies $d.G = O$, where $O$ is the point at infinity.

(ii) Generating a public-private key pair. The TTP (Server) randomly chooses a secret value $n_s$ from $[2, d-2]$ and public key as follows:

$$Pk_S = n_s.G \tag{5}$$

(iii) Publishing the Server's public key $Pk_S$ and keeping $n_s$ as a secret.

(iv) All users selecting private key $(n_A, n_B, n_F)$ and generating their public keys $(Pk_A, Pk_B, Pk_F)$

(v) Before accessing associated services, all users that is, $A$, $B$, and $F$ must register on the dedicated Server (TTP) as valid participants.

(vi) After registering, the user will receive a token obtained JSON Web Token or JWT which is used to authenticate users who use the application.

(vii) Each member receives a unique set of keys upon creation. Through a secure channel, the private key with the identifiers id$A$, id$B$ and id$F$ will be sent from TTP (Server) to the users.

### 3.2.2 Identity verification

After completion of the registration procedure, every entity can interact with the linked parties in an efficient manner. User authentication testing aims to give access to valid users and block access for users who are not registered with the system. When a user registers, the user data will be used to generate the authenticated user's JSON Web Token (JWT). If the user login is a valid user, the JWT will return a valid token, if the user is not a valid user, the JWT will return an invalid token, and if the user login but there is a time stamp problem, the JWT will return an expired token.

#### 3.2.3 Data Collecting

The process of collecting data in the online process, where raw data from the accelerometer sensor will be obtained 3 values (x, y, z) and the gyroscope sensor will be obtained 3 values (ϕ, θ, ψ). Raw data taken from the two sensors is not labeled, but is directly used as input for the next process, namely preprocessing.

#### 3.2.4 Preprocessing

In data preprocessing, just like data preprocessing during offline scope, it consists of 3 stages, namely filtering, feature extraction, and normalization. Data preprocessing results will be used as input to the machine learning identification process on android application.

#### 3.2.5 Identification Result

In the decision-making stage, the results of normalization will be used as input for activity prediction on the model that has been loaded. The model will be compared with the data that has been inputted, so that it will produce output in the form of predictions of each activity.

#### 3.2.6 Blinding Phase

The main purpose of blindness is to protect communications without the Signer's knowledge. To accomplish this, the Requester A uses the public and private keys as a blind factor $(n_A, Pk_A)$ along with the message digest $h(m)$ and hash of ID user $h(ID)$. These elements are combined to blind the message according to Eq. (6). Subsequently, the blinding operation, as described in Eq. (7), is computed. Once completed, the blinded message $\alpha$ is received by the Signer *B* and other family Requesters $F'$

$$m = h(m) \,||\, h(ID) \tag{6}$$

$$\alpha = m.n_A.Pk_A \tag{7}$$

#### 3.2.7 Signing Phase

Upon receiving the corresponding message $\alpha$, the Signer *B* and other Family Requester $F'$ selects a random integer $\beta \in [2, d-2]$ to determine secret element *R* as Eqs. (8) and (9) and the blind signature *S* as Eqs. (10) and (11). The message signature pair $(\alpha, (R, S))$ sends it back to the Requester *A*.

$$R_B = \beta_B.\alpha \tag{8}$$

$$R_{F'} = \beta_{F'}.\alpha \tag{9}$$

$$S_B = (n_B + \beta_B).\alpha \tag{10}$$

$$S_{F'} = (n_{F'} + \beta_{F'}).\alpha \tag{11}$$

#### 3.2.8 Unblinding and Verification Phase

To reveal the received hidden signature, the Requester *A*, uses the blind signature $S_B$ , the previously generated message '*m*', private key $n_A$, and public key $Pk_B$ of the signer to extract the blind signature $S_{B'}$ by following the expression in Eq. (12). Likewise, for the other Family Requester $F'$ expressed in Eq. (13). Additionally, Requester *A* computes the message digest value $m'$ and conducts the unblinding process outlined in Eq. (14). Then $S_{B'}$, $S_{F'}$ and $m'$ are testified by Requester *A* that the message alleging the signature request while being blinded is genuine.

$$S_{B'} \equiv S_B - m.n_{A\,.}Pk_B \tag{12}$$

$$S_{F'} \equiv S_{F'} - m.n_{A\,.}Pk_{F'} \tag{13}$$

$$m' \equiv n_{A\,.}(n_A - 1).m + m \tag{14}$$

Requester *A* verifies the authenticity of the signature and the transmitted message digest using the Signer's public key $Pk_B$ and the public keys $Pk_{F'}$ of other family Requesters after obtaining the message signature. The validity of Eqs. (15) and (16) is checked during this verification process.

$$R_B.Pk_B \stackrel{?}{=} S_{B'} - m'.Pk_B \tag{15}$$

$$R_{F'}.Pk_{F'} \stackrel{?}{=} S_{F'} - m'.Pk_{F'} \tag{16}$$

#### 3.2.9 Encryption Phase

The encryption phase objective is to prevent sensitive information from leaking against the desires of snoopers. We take more measures to improve operational security, particularly when data is transferred across networks. The result of data encryption will be stored in the database.

(i) To send digital information securely over the internet to Signer *B*, Requester *A* breaks down a data into a sequence $\bar{v}$, consisting of multiple plaintext blocks $v_i\,(\geq 1)$ , and each data segment's individual blocks can be expressed as Eq. (17)

$$\bar{v} = \{v_1, v_2, \dots, v_i\} \quad (17)$$

(ii) If the message length is not a multiple of the AES block size (256 bits), may need to add padding to make it fit. Common padding schemes include PKCS#5 padding, which appends bytes to the message to fill the last block.

$$pv = block_{size} - ([v_i \,| mod\ block_{size}) \quad (18)$$

If $v_i$ is not multiple of the block size, append bytes to the last block $v_i$ to fill the block:

$$pad = \begin{cases} pv & if\ [v_i \,|\, mod\ block_{size} \neq 0 \\ 0 & if\ [v_i \,|\, mod\ block_{size} = 0 \end{cases} \quad (19)$$

(iii) To increase the security of encryption by applying the concept of chaining and randomization (initialization vector) on data blocks. In this research using cipher block chaining (CBC). In CBC mode, each plaintext block is combined with the previous ciphertext block before encryption, using an XOR operation. Additionally, an Initialization Vector (IV) is used to initialize the chaining process for the first block. Calculate the intermediate value $IV_i$:

$$IV_i = v_i \oplus c_{i-1} \quad (20)$$

Encrypt the intermediate value $IV_i$, using the encryption function:

$$C_i = E_k(IV_i) \quad (21)$$

#### 3.2.10 Decryption Phase

Decryption refers to the inverse operation, converting the encrypted message back to its original state. This decryption process is performed on an android and displayed on an android application to see the results of user activity classification by Requester *A* and Requester Family *F*.

(i) For decrypt the ciphertext block $C_i$ using the decryption function with the same key *k*

$$IV_i = D_k(C_i) \quad (22)$$

(ii) Calculate the plaintext block $v_i$, using the intermediate value $IV_i$ and previous ciphertext block $c_{i-1}$

$$v_i = IV_i \oplus c_{i-1} \quad (23)$$

(iii) If padding was added during encryption (e.g., PKCS#5 padding), remove it to recover the original plaintext.

## 4. Measurement Result and Discussion

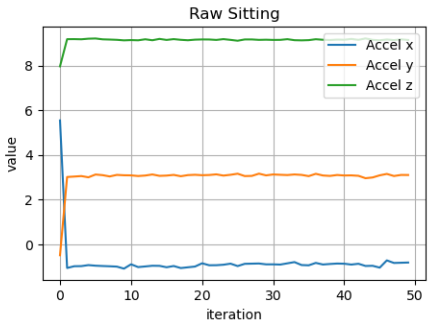
In this section, we introduce the results of the offline scope and the online scope. In the offline scope, the results of training machine learning from accelerometer and gyroscope sensors are presented. In the online scope, the results of testing the model from the training results and the results of the blind signature using the ECC algorithm are shown.

### 4.1 Offline Scope Result

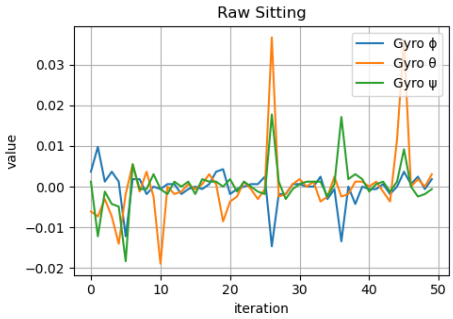
The first process is the process of collecting raw data from Accelerometer sensors (*x, y, z*) and Gyroscope sensors ($\phi, \theta, \psi$), as many as 50 data per axis using the application that has been made with different periods according to the activities carried out by the user. Figs. 7-10 shows four plots of raw data in each activity performed by a human subject participating in the experiment. In the graph, the *x*-axis shows the number of data or iterations, and the *y*-axis shows the measurement data on the accelerometer and gyroscope sensors. A zero or missing value check was performed before the three-axis accelerometer and three-axis gyroscope values were displayed in graph form. If there are no null values in the reading, thus ensuring that the data is properly filtered before representation [32].

From the result of raw data on each activity can be described in the form of a graphical signal which can be seen in Figs. 7-10. Figs. 7-8 show the results of the graphic signal representation of sitting and standing activities having almost the same pattern, both of which are activities with static movements. The walking and Jogging activities shown in Figs. 9-10 have a more varied data pattern. It can be seen that Jogging activities produce higher and sharper accelerometer and gyroscope graphic signals with more ripple than walking activity.

From the results of data collected that has been carried out for each activity, Figs. 7-10 shows the pattern of raw data, where many high-frequency signals are usually identified as noise so that the selection of features cannot be determined for each activity. Therefore, a preprocessing technique is needed to sort out the signal from noise, The following is the result of the Low Pass filter (*x*-axis) can be illustrated in the graph shown in Figs. 11-14. Where in the graph, the *x*-axis shows the number of data or iterations, and the *y*-axis shows the measurement data on the accelerometer and gyroscope sensors.

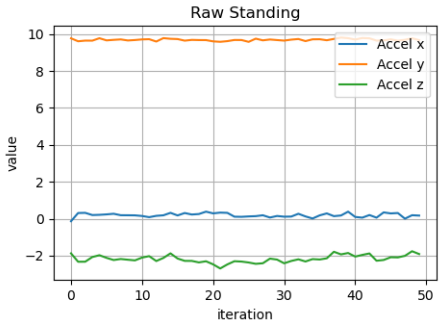



(a)

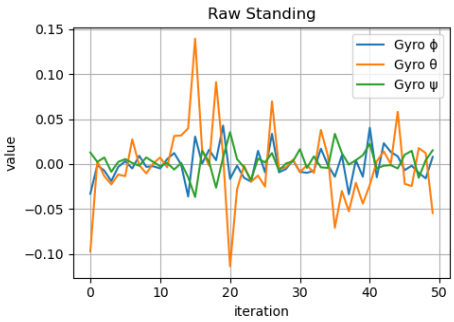



(b)

Figure. 7: (a) Accelerometer Raw Data Result in Sitting Activity and (b) Gyroscope Raw Data Result in Sitting Activity



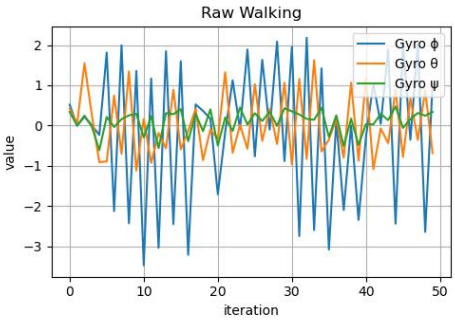

(a)




(b)

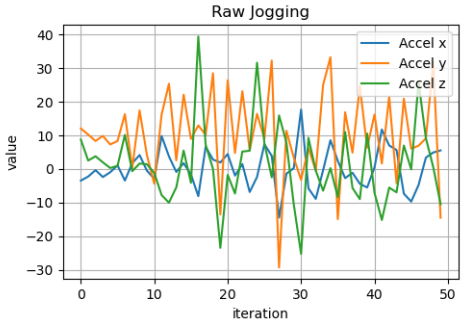
Figure. 8: (a) Accelerometer Raw Data Result in Standing Activity and (b) Gyroscope Raw Data Result in Standing Activity


(a)

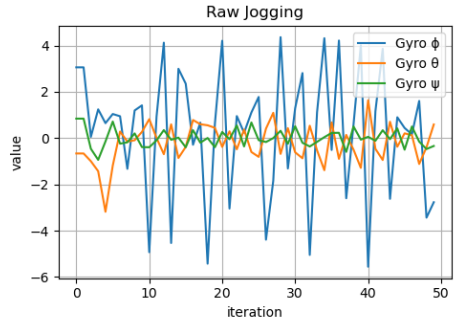



(b)

Figure. 9: (a) Accelerometer Raw Data Result in Walking Activity and (b) Gyroscope Raw Data Result in Walking Activity

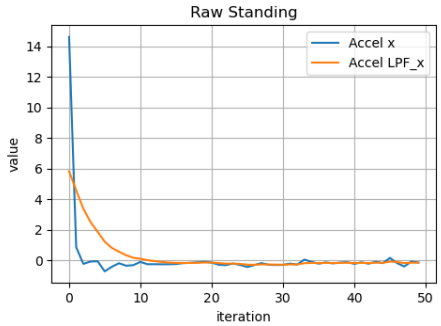



(a)

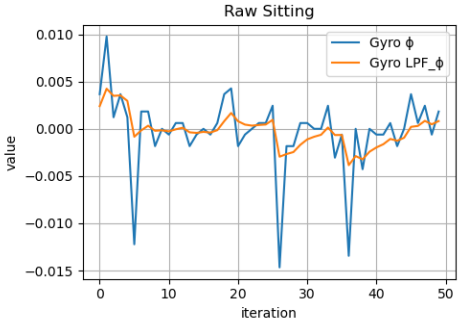



(b)

Figure. 10: (a) Accelerometer Raw Data Result in Jogging Activity and (b) Gyroscope Raw Data Result in Jogging Activity

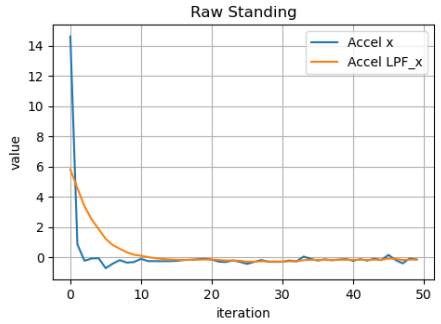



(a)

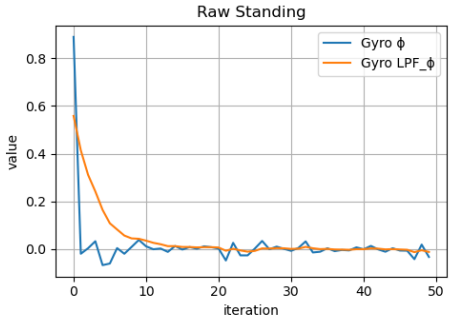



(b)

Figure. 11: (a) Filtering Accelerometer Data (*x*-axis) in Sitting Activity and (b) Filtering Gyroscope Data (*x*-axis) in Sitting Activity

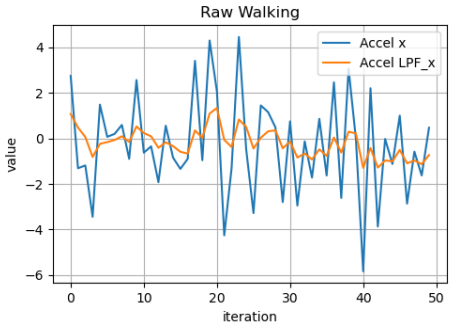



(a)




(b)

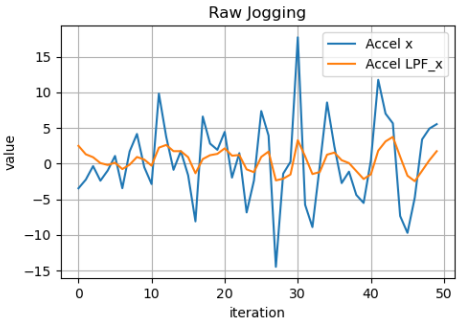
Figure. 12: (a) Filtering Accelerometer Data (*x*-axis) in Standing Activity and (b) Filtering Gyroscope Data (*x*-axis) in Standing Activity



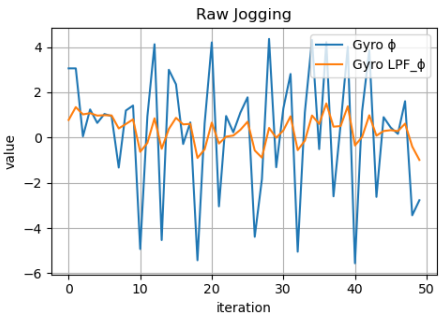

(a)


(b)

Figure. 13: (a) Filtering Accelerometer Data (*x*-axis) in Walking Activity and (b) Filtering Gyroscope Data (*x*-axis) in Walking Activity




(a)




(b)

Figure. 14: (a) Filtering Accelerometer Data (*x*-axis) in Jogging Activity (b) Filtering Gyroscope Data (*x*-axis) in Jogging Activity

Table 1. Feature Extraction Measurement Result

| acc_x _ min | acc_y _ min | acc_z _ min | acc_x _ max | acc_y _ max | … | gy_z _std |
|---|---|---|---|---|---|---|
| -0.96 | -0.48 | 7.972 | 5.557 | 3.117 | ... | 0.002 |

Table 2. Normalization Measurement Result

| acc_x _ min | acc_y _ min | acc_z _ min | acc_x _ max | acc_y _ max | … | gy_z _std |
|---|---|---|---|---|---|---|
| 1.919 | -1.027 | 1.648 | 0.515 | -1.558 | ... | -0.8 |
| -0.23 | 0.903 | -0.50 | -0.160 | 0.154 | … | 0.59 |
| -0.26 | 1.058 | -0.52 | 0.309 | 0.173 | … | 0.52 |
| … | … | … | … | … | … | … |
| … | … | … | … | … | … | … |
| 0.468 | 1.2749 | -0.215 | -0.772 | -0.176 | … | -0.8 |

Table 3. Support Vector Machine Tuning Parameters

| Parameter | Value |
|---|---|
| Kernel | RBF |
| C (cost) | 100 |
| Gamma | 1 |
| Tolerance | 0.001 |

Table 4. Metric Evaluation of Each Class

| Class | Accuracy | Precision | Recall | f1-score |
|---|---|---|---|---|
| 1.0 | 1 | 1 | 1 | 1 |
| 2.0 | 0.9830 | 0.9375 | 1 | 0.9670 |
| 3.0 | 0.9830 | 1 | 0.9411 | 0.9690 |
| 4.0 | 1 | 1 | 1 | 1 |
| Overall accuracy | 0.9916 | | | |

From the filtering results, the main features obtained, contained the x, y, and z axis accelerometer sensors and the gyroscope axes ϕ, θ, ψ which have been filtered, feature data are then carried out feature mapping with measurement functions such as mean value, standard deviation, min value, and max value. From the feature mapping, a total of 24 data features were produced. The results of the sitting activity feature extraction example are shown in Table 1.

The next step is the normalization process which uses the z-score technique. The normalization results are shown in Table 2.

The next step is the training. the total dataset used for the data modeling process is 200 data, each of which has the same data distribution.Based on the best results (tuning parameters) obtained from the

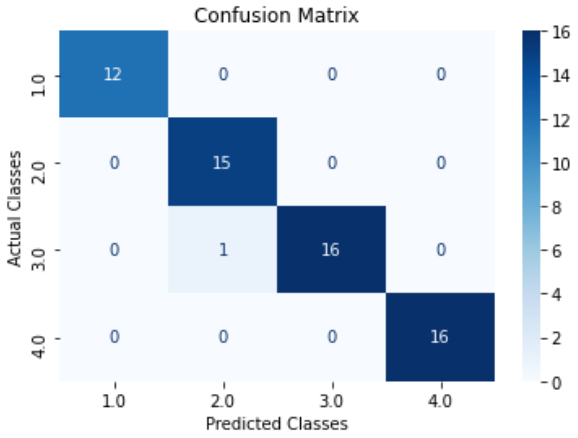



Figure. 15 Confusion Matrix Results

above analysis using the C-SVC type SVM algorithm with one vs one multiclass classification technique, parameter c (cost) is 100, gamma is 1, and RBF (Radial Basis Function) kernel with a data set comparison of 70% training data and 30% testing data. which is shown in Table 3.

RBF (Radial Basis Function) with a comparison of 140 training data and 60 testing data, showing the results of measuring classification performance on the original data (ground truth) and predicted data from the classification model visualized in the Confusion Matrix shown in Fig. 15. Based on confusion matrix data, the results obtained with a testing accuracy is 99.16%. As for the results metric evaluation in detail from the first trial can be seen in Table 4 where each class is calculated and evaluated respectively.

### 4.2 Online Scope Result

The next step is system testing which aims to test the validated model using real-time data from accelerometer and gyroscope sensors. The data collection and data preprocessing stages in this testing process are the same as the data modeling stages using machine learning. At the decision-making stage, the results of normalization will be used as input for activity prediction against the model that has been loaded. The model will be compared with the data that has been inputted, so that it will produce output predictions of each activity. The testing process is carried out with the SVM C-SVC type and the RBF kernel. This testing process was carried out 30 times for each activity. Fig. 16 shows the sample decision results of sitting activities.

Fig. 17 shows the classification result evaluation graph on each activity with 30 tests.

Fig. 17, it can be explained that the average classification error in 30× testing each activity is very small, which is 3.33% in standing and walking

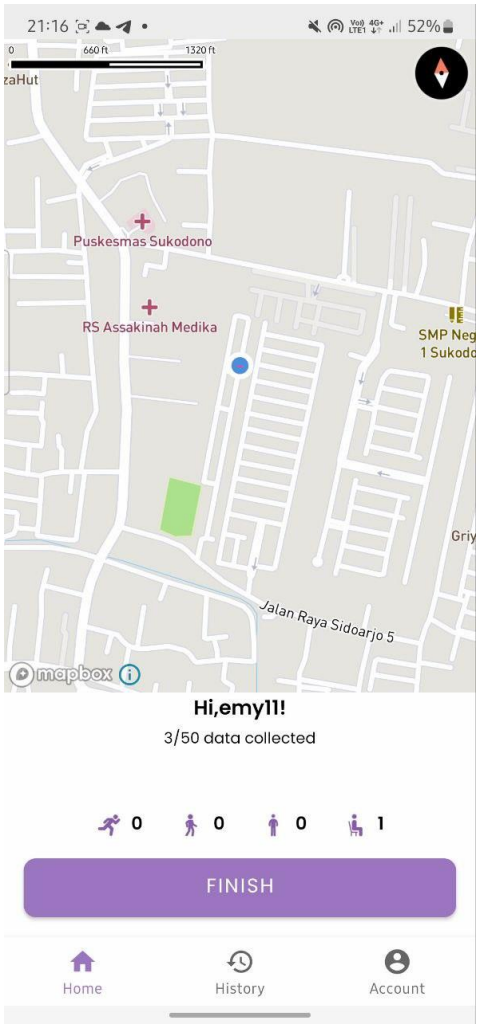



Figure. 16 Visualization in Sitting Activity

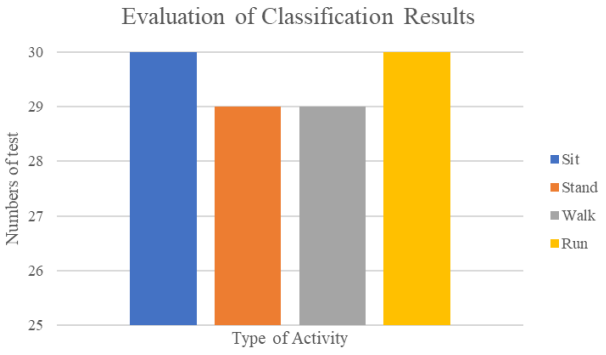



Figure. 17 Classification Result Evaluation Graph

activities. While sitting and Jogging activities have no error in 30× testing classification, it can be concluded that the metric in each activity is very good.

The next is the result of blind signature ECC. The challenge associated with solving the Blind Signature ECC determines the robustness of our method. At the same time, using the blind signature approach improves the overall security of data transmissions. The proposed scheme is strengthened and made more useful for a variety of applications by incorporating additional characteristics, such as confidentiality, correctness, integrity, nonrepudiation, and unforgeability, in addition to the essential properties of blindness and untraceability. We look at these security criteria for our plan in the following manner. *Blindness*, Blindness is the inability of the Signer to see the message's content while they are signing it. Our scheme's blinded message is created as $\alpha = m.n_A.Pk_A$ . Without the parameters the message digest ($m$) and the blinding factor ($n_A.Pk_A$) neither the Signer ($B$), other Family Requester $F'$ nor the opponent can deduce the message ($\alpha$). Because determining the blindness factor in this equation requires computing the number of points on the elliptic curve over fields, it becomes quite difficult to break the value of knowing desired points when solving the Blind Signature ECC. The attempt to invert a hash function with the other parameter value, $m$, is not simple. Because the Signer $B$ and other Family Requester $F'$ signs the blinded message without knowing its contents, the current approach can thus satisfy the blindness property.

*Untraceability*, in any blind signature system, untraceability is a critical security requirement. The Signer loses the ability to link a signature to a specific message once the message signature pair becomes public. In this experimental setup, steps (7), (8), (9), (10), and (11) are used to generate the message signature pair ($\alpha$, ($R$, $S$)). During a blind signature request, the Signer $B$, only has their private key $n_B$ and a randomly generated $\beta_B$ . The connection between the message and the blind signature is untraceable without knowledge of the secret factors, which include a unique message digest $m$, and A's private key $n_A$ from Requester $A$, Signer $B$, and other Family Requester $F'$ . As a result, this method effectively preserves the untraceability or unlinkability of a blind signature.

*Confidentiality*, requires hiding the message's contents from unauthorized entities or processes. In this investigation, all messages are blinded by Requester $A$, followed by signing from both Signer $B$ and other family Requester $F'$ , and then pass through a permutation procedure before returning to Requester $A$. Even if intercepted during transmission, the transmitted text should present an extremely difficult task for any adversary attempting to decode the messages. Determining the desired points in tackling the Blind Signature ECC presents a significant challenge for attackers because they must determine the number of points on the elliptic curve over fields. As a result, the current method ensures confidentiality by effectively safeguarding the message's contents.

Table 5. Comparison of The Proposed Scheme and Four Existing Similar Research

| **Goals** | **Alaa, et.al**[14] | **Lyu et.al**[23] | **Owoh et.al** [24] | **Wang et.al** [25] | **Our Scheme** |
|---|---|---|---|---|---|
| Good Accuracy | √ (Not Described) | √ (accuracy 93.75%) | NA | √ (accuracy 93.24%) | √ (accuracy 99,16%) |
| Good Classification Time | √ | NA | NA | √ (around 36.4 s) | √ (around 1 ms) |
| Blindness | NA | NA | NA | NA | √ |
| Untraceability | NA | NA | NA | NA | √ |
| Confidentiality | NA | NA | √ | NA | √ |
| Correctness | NA | NA | NA | NA | √ |
| Integrity | NA | NA | √ | NA | √ |
| Nonrepudiation | NA | NA | NA | NA | √ |
| Unforgeability | NA | NA | NA | NA | √ |

Table 6. Computational Complexity Symbols

| **Symbol** | **Definition** | **Operation Cost** |
|---|---|---|
| $T_{MUL}$ | The duration of a multiplication operation's execution | $= 37\mu s$ |
| $T_{ADD}$ | The duration of a addition operation's execution | Negligible |
| $T_{EXP}$ | The duration of a exponentiation operation's execution | $\approx 8ms$ |
| $T_{INVRS}$ | The duration of a addition modular multiplicative inverse execution | $\approx 8ms$ |
| $T_{ECMUL}$ | The duration of ECC point multiplication execution | $\approx 1ms$ |
| $T_{ECADD}$ | The duration of ECC point addition execution | $\approx 185\mu s$ |
| $T_h$ | The duration of ECC point hash operation's execution | $\approx 814\mu s$ |
| $t_h$ | The duration of basic hash function operation's execution | $\approx 15\mu s$ |

Table 7. Computational Cost in Our Proposed Scheme

| **Item** | **Computational Cost** | **Estimation** |
|---|---|---|
| Blinding | $1T_{ECMUL} + 1T_{MUL}$ | $1\ ms$ |
| Signing | $2T_{ECMUL} + 1T_{ADD}$ | $2ms$ |
| Unblinding | $2T_{ECMUL} + 2T_{ECADD} + 1T_h$ | $3ms$ |
| Signature Verification | $1T_{ECMUL} + 1T_{ECADD} + 1t_h$ | $1ms$ |
| Whole System (Data Collecting + Preprocessing + Identification + Blind Signature) | | $14s$ |

Table 8. Computation Time Performance of Generate Key

| **Number of User** | **Estimation ECC** | **Estimation RSA** |
|---|---|---|
| 10 | $1\ 42ms$ | $24009\ ms$ |
| 20 | $222ms$ | $63738\ ms$ |
| 50 | $411ms$ | $126275\ ms$ |
| 100 | $550ms$ | $202705\ ms$ |

*Correctness*, the correctness property ensures that anyone with access to the Signer's public key can authenticate the signature correctly. Public verification, on the other hand, may reveal the Signer's identity for each session via a distinct electronic link between the identity and the public key, potentially compromise-ing various secret messages. In our framework, Requester *A* is in charge of verifying the authenticity of the signature created by Signer *B* and other Family Requester $F'$. This is accomplished by authenticating the use of *B*'s public key, ensuring the correctness of the signed message. Requester *A* examines the validity of Eqs. (15) and (16) to determine the accuracy of the signatures from both Signer *B* and other Family Requester *F'*. If these equations are correct, the pair $(S', m')$ is recognized

as a valid message signature. Throughout this verification process, Requester $A$ uses the secret value $n_B$ to authenticate the identity of Signer $B$, and similarly uses the secret value $n_{F'}$, to authenticate the identity of Signer $F'$. These secret values are derived from $B$'s private key and used in Eqs. (10) and (11) for the other Family Requester $F'$. As a result, the proposed design effectively maintains the property of correctness.

*Integrity*, Integrity means that no malicious or unintentional changes can be made to the data while it is being transmitted. It is difficult to tamper with the message segments if an adversary tries to change a specific piece of data, such as sections of blind text that are being communicated between the sender and the recipient. Additionally, every part of the blind text that is embedded in the encoded text and assigned a corresponding coordinate position depends heavily on every message block. When a deliberate action is taken to alter a specific message, the avalanche effect should follow with radically different outcomes. As a result, the suggested remedy offers the integrity property.

*Nonrepudiation,* Nonrepudiation refers to a Signer's inability to retract their signature from a genuinely signed message. In this case, Signer $B$ who claimed to have signed the document, electronically signed the blinded message. Normally, a signature with specific values is returned to Requester $A$ along with the classification result and user tracking. $B$ cannot refute the act of signing by using the random number $\beta_B$ and $B$'s private key $n_B$, which also applies to other Family Requesters $F'$. Furthermore, because Requester $A$ is required to use the corresponding public key $Pk_B$ for $B$ during verification, Requester $A$ can later confirm that the message's signature has been legitimately endorsed by the designated Signer $B$ and other Family Requesters $F'$. This is accomplished through the signature validation process described in Eqs. (15) and (16). As a result, the proposed method effectively ensures nonrepudiation.

*Unforgeability*, Unforgeability refers to an interactive signature protocol's ability to produce a valid signature for a given message only by the legitimate Signer. Furthermore, the Signer is not permitted to create additional signatures beyond the number of allowed signing instances (also known as non-reusability). Even if an adversary intercepts or eavesdrops on the blinded message $(\alpha, (R, S))$ in order to attempt signature generation without the designated Signer $B$'s private key $n_B$, they will not be able to obtain a valid pair $(\alpha, (R, S))$. This is due to an adversary's inability to convincingly impersonate Signer $B$ when forging a legally blind signature. Similarly, after interacting with Requester $A$ once, the likelihood of Signer $B$ successfully guessing a random signature $(R, S)$ in an attempt to create additional valid signatures is extremely low. Furthermore, Requester $A$ can use the signature verification procedure $R_B.Pk_B \stackrel{?}{=} S_{B'} - m'.Pk_B$ as defined in Eq. (15) to check any received message tuple $(S_{B'}, m', R_B)$ corresponding to that signature for forgery. An adversary Signer faces difficulties in reversing the one-way hash function and solving the Blind Signature ECC for these parameters as a result of this process. In essence, the proposed plan satisfies the unforgeability property.

The distinguishing characteristics are compatible with blind signatures, and we have detailed the intricate aspects of our proposed scheme in terms of security requirements. Table 5 provides a comparison of four similar existing studies. A "√" symbol in the table indicates that a security requirement has been met, while a "NA" or Not Available symbol indicates that the requirement has not been met as specified. The comparison shows how our current approach, which includes the above goals, improves security in comparable blind signature applications. Notably, while successful existing schemes have limitations in areas such as blindness, untraceability, and correctness, our proposed scheme stands out for its enhanced security.

Table 5 illustrates how our suggested strategy helps to satisfy the requirement for an authentication system that upholds machine learning accuracy values while safeguarding privacy and anonymity. In research [14], they used k-Nearest Neighbour (k-NN) as a recommended model. To get the ideal k parameters The k-NN Classifier value used in this research Particle Swarm Optimization (PSO) technique. This first research experiment shows experimentally how PSO enters. The recommended approach is to find the ideal $k$ parameter values to reduce the classification error rate of the k-NN classifier. But they do not explicitly mention the accuracy values. This research also does not discuss the privacy and anonymity of users. In research [23] outlines a privacy-preserving collaborative deep learning framework for HAR, employing a two-stage scheme called RG-RP. The first stage involves perturbing participant data using a repeated Gompertz function to thwart MAP estimation attacks, while the second stage projects the data to a lower dimension using a row-orthogonal random projection matrix. The proposed LSTM-CNN model for activity recognition, when used with the privacy-preserving scheme, achieves an accuracy of 93.75% for the HAR dataset and 92.08% for the MH dataset,

demonstrating competitive accuracy while providing significant privacy benefits. Where the result of adding noise to raw user data results in a decrease in accuracy in this research. In research [24] the paper primarily focuses on securing location data in mobile crowd sensing (MCS) applications, but it has limitations. It is limited to Android-based sensing applications, potentially limiting its generalizability. The proposed security scheme lacks comparative analysis with existing methods and does not thoroughly address implementation challenges or real-world deployment considerations. Additionally, the paper does not extensively evaluate the impact on user experience. While it provides valuable insights, there are opportunities to enhance the research by considering a broader perspective on security, privacy, and practical implementation considerations for securing location data in MCS applications. In this research only focuses on confidentiality, integrity and authentication guarantees, while user anonymity is not considered. In research [25] This paper proposes a privacy-preserving framework for collaborative HAR using federated learning, edge computing and blockchain technology. Multiple edge nodes collect data from smart devices and conduct local model training without sharing raw data. A secure aggregation protocol is used to aggregate local model updates in a privacy-preserving manner. Smart contracts on the blockchain network replace the central server for model aggregation to improve security and transparency. According to experiments, the proposed framework achieves 93.24% accuracy for activity recognition while preserving user privacy during collaborative training. The training time is increased by the use of secure multiparty computation techniques; a round of iterations takes 36.4 seconds to complete. And in our proposed, we improved the training accuracy results using the SVM algorithm, namely 99.16% with a classification time of 1 ms, and guaranteed user anonymity with the security attributes blindness of untraceability, confidentiality, correctness, integrity, nonrepudiation, and unforgeability.

## 5. Performance Analysis

In this section, we will first discuss the overall performance analysis of the system. The following section will investigate in quantitative detail the performance of our proposed SVM to classify and ECC blind signature algorithm. First, we will examine the results of analysing how much computing time is needed to classify smartphones in real-time, starting from inputting data in the model to making decisions. In addition, we will examine the

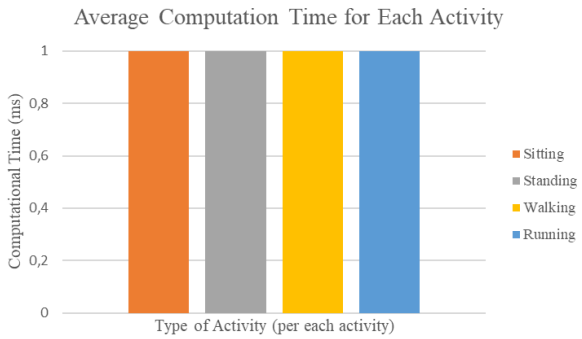



Figure. 18 Graph of Average Computational Time in Each Activity

theoretical results for solving the cryptological operations involved with respect to the computational and communication costs incurred by each task according to the concept of modular arithmetic operations [33]. Fig. 18 shows the process of classifying smartphones in real-time, starting from inputting data in the model to making decisions. The graph above shows that the average time interval for classification on smartphones in real-time is around 1 ms. With an average classification computation time of 1 ms, it can be concluded that the classification process starts from inputting data in the model until decision-making is very fast. This shows that the prediction system can work in real- time. Because of the fast classification computation time, there is no need to worry about data loss for further activities. In addition, with a short classification computational time, no large resources are needed to compute with the model that has been made. Table 6 shows the notations we use to evaluate performance, which include scalar multiplication, dot addition, hash construction, and modular arithmetic. Table 7 shows the computational cost of our scheme for each stage such as blinding, signing, unblinding, and verification. Table 8 shows Computation Time Performance of Generate Key, where the increasing number of users created, the longer the key generation time on the TTP (Server). However, the time difference between generating user keys in ECC-based blind signature is very small around 150 ms.

## 6. Conclusion

Based on the experimental results obtained from the study, it can be concluded that the proposed SVM C-SVC model with RBF kernel and the data normalization technique has achieved a high level of accuracy in predicting the four tested activities of sitting, standing, walking, and jogging. The experimental results obtained in the machine learning process were satisfactory with an overall accuracy of

99.16%. This is supported by the evaluation metrics obtained in detail from the confusion matrix analysis and the comparison of each class performance. The outcomes of the system testing conducted in the online scope demonstrated that the suggested model could effectively use accelerometer and gyroscope sensor data to classify and predict sitting, standing, walking, and jogging activities in real-time. Fig. 16's decision classification results and Fig. 17's classification result evaluation graph. The robustness and accuracy of the proposed SVM-C SVC model using RBF kernel and data normalization techniques may contribute to the development of more advanced intelligent systems in the healthcare and wearable device industries. This significantly improves the overall user experience due to the model's ability to accurately classify activity and predict potential health issues such as sedentary behaviour and fall risk, providing personalized recommendations. In addition, in maintaining anonymous users using blind signature ECC has fulfilled criteria such as confidentiality, correctness, integrity, nonrepudiation, and unforgeability, blindness and untrace ability at a low computational cost.

**Notations and Descriptions**

| | |
|---|---|
| $E\ (Fq)$ | An elliptical curve $E$ over a finite field $Fq$ |
| $G$ | A base point of elliptic curve |
| $d$ | A prime order of $G$ |
| $Pk_S, n_s$ | A public and private key pair from Server |
| $Pk_A, Pk_B, Pk_F$ | All users' public keys as requester ($A$), signer ($B$), and Family Requester ($F$) |
| $n_A, n_B, n_F$ | All users' private keys as requester ($A$), signer ($B$), and Family Requester ($F$) |
| $idA, idB, idF$ | User identity data, including requester ($A$), signer ($B$), and Family Requester ($F$) |
| $m$ | a hash value obtained from the sequence of ciphertext |
| $\alpha$ | A blinded message |
| $\beta$ | A random integer number |
| $R_B, R_{F'}$ | Secret Element Signer B, Secret Element Other Family Requester |
| $S_B, S_{F'}$ | Blind Signature Signer B, Blind Signature Other Family Requester |
| $\bar{v}$ | A plaintext segment |
| $pv$ | Padding value |
| $pad$ | Padding |
| $C_i$ | Ciphertext block |
| $c_{i-1}$ | Previous ciphertext block |
| $IV_i$ | Intermediate value |
| $E_k$ | Encryption Process |
| $D_k$ | Decryption Process |
| ECC | Elliptic Curve Cryptography |
| SVM | Support Vector Machine |
| JWT | JSON Web Token |
| TTP | Third Trusted Party |

## Conflicts of Interest

Authors declare no conflict of interest.

## Author Contributions

Erita Cicilia Febrianti was conceptualized, implemented, collected data, and documented the paper. Amang Sudarsono and Tri Budi Santoso reviewed the works, made suggestions for improvements, and verified the results.

## References

[1] L. Schrader., A. V. Toro., S. Konietzny., S. Rüping., B. Schäpers., M, Steinböck., C. Krewer., F. Müller., J. Güttler., and T. Bock, "Advanced Sensing and Human Activity Recognition in Early Intervention and Rehabilitation of Elderly People", *Journal of Population Ageing*, Vol. 13, No. 2, pp. 139-165, 2020.

[2] R. Damaševičius, M. Vasiljevas, J. Šalkevičius, and M. Woźniak, "Human Activity Recognition in AAL Environments Using Random Projections", *Computational and Mathematical Methods in Medicine*, Vol. 2016, pp. 1-17, 2016.

[3] A. Hayat, F. Morgado-Dias, B. Bhuyan, and R. Tomar, "Human Activity Recognition for Elderly People Using Machine and Deep Learning Approaches", *Information*, Vol. 13, No. 6, p. 275, 2022.

[4] S. Fatima, "Activity Recognition in Older Adults with Training Data from Younger Adults: Preliminary Results on in Vivo Smartwatch Sensor Data", In: *Proc. of the 23rd International ACM SIGACCESS Conference on Computers and Accessibility*, New York, NY, USA: ACM, pp. 1-4, 2021.

[5] O. D. Incel, M. Kose, and C. Ersoy, "A Review and Taxonomy of Activity Recognition on Mobile Phones", *Bionanoscience*, Vol. 3, No. 2, pp. 145-171, 2013.

[6] V. Osmani, S. Balasubramaniam, and D. Botvich, "Human activity recognition in pervasive health-care: Supporting efficient remote collaboration", *Journal of Network and Computer Applications*, Vol. 31, No. 4, pp. 628-655, 2008.

[7] O. D. Lara and M. A. Labrador, "A Survey on Human Activity Recognition using Wearable

Sensors", *IEEE Communications Surveys & Tutorials*, Vol. 15, No. 3, pp. 1192-1209, 2013.

[8] M. Shoaib, S. Bosch, O. Incel, H. Scholten, and P. Havinga, "A Survey of Online Activity Recognition Using Mobile Phones", *Sensors*, Vol. 15, No. 1, pp. 2059-2085, 2015.

[9] J. L. R. Ortiz, *Smartphone-Based Human Activity Recognition*, Springer International Publishing. 2015.

[10] M. A. Awan, Z. Guangbin, H. C. Kim, and S. D. Kim, "Subject-independent human activity recognition using Smartphone accelerometer with cloud support", *International Journal of Ad Hoc and Ubiquitous Computing*, Vol. 20, No. 3, p. 172, 2015.

[11] R. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: current state and future challenges", *IEEE Communications Magazine*, Vol. 49, No. 11, pp. 32-39, 2011.

[12] N. Pius Owoh and M. Mahinderjit Singh, "SenseCrypt: A Security Framework for Mobile Crowd Sensing Applications", *Sensors*, Vol. 20, No. 11, p. 3280, 2020.

[13] D. Tao, P. Ma, and M. S. Obaidat, "Anonymous identity authentication mechanism for hybrid architecture in mobile crowd sensing networks", *International Journal of Communication Systems*, Vol. 32, No. 14, 2019.

[14] A. Tharwat, H. Mahdi, M. Elhoseny, and A. E. Hassanien, "Recognizing human activity in mobile crowdsensing environment using optimized k -NN algorithm", *Expert Systems with Applications*, Vol. 107, pp. 32-44, 2018.

[15] D. He, S. Chan, and M. Guizani, "User privacy and data trustworthiness in mobile crowd sensing", *IEEE Wireless Communications*, Vol. 22, No. 1, pp. 28-34, 2015.

[16] D. Zhang, L. Wang, H. Xiong, and B. Guo, "4W1H in mobile crowd sensing", *IEEE Communications Magazine*, Vol. 52, No. 8, pp. 42-48, 2014.

[17] N. P. Owoh and M. M. Singh, "Security analysis of mobile crowd sensing applications", *Applied Computing and Informatics*, Vol. 18, No. 1/2, pp. 2-21, 2022.

[18] M. Talasila, R. Curtmola, and C. Borcea, *Mobile crowd sensing*, 2015.

[19] H. Jin, L. Su, H. Xiao, and K. Nahrstedt, "INCEPTION", In: *Proc. of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, New York, NY, USA: ACM, Jul. 2016, pp. 341-350.

[20] B. Guo, Z. Yu, X. Zhou, and D. Zhang, "From participatory sensing to Mobile Crowd Sensing", In: *Proc. of 2014 IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM WORKSHOPS)*, pp. 593-598, 2014.

[21] Y. Wang, Z. Yan, W. Feng, and S. Liu, "Privacy protection in mobile crowd sensing: a survey", *World Wide Web*, Vol. 23, No. 1, pp. 421-452, Jan. 2020.

[22] L. Xiao, D. Jiang, D. Xu, W. Su, N. An, and D. Wang, "Secure mobile crowdsensing based on deep learning", *China Communications*, Vol. 15, No. 10, pp. 1-11, 2018.

[23] L. Lyu, X. He, Y. W. Law, and M. Palaniswami, "Privacy-Preserving Collaborative Deep Learning with Application to Human Activity Recognition", In: *Proc. of the 2017 ACM on Conference on Information and Knowledge Management*, New York, NY, USA: ACM, pp. 1219-1228, 2017.

[24] N. P. Owoh and M. M. Singh, "Security analysis of mobile crowd sensing applications", *Applied Computing and Informatics*, Vol. 18, No. 1/2, pp. 2-21, Mar. 2022.

[25] L. Wang., C. Zhao., K. Zhao., B. Zhang., S. Jing., Z. Chen., and K. Sun, "Privacy-Preserving Collaborative Computation for Human Activity Recognition", *Security and Communication Networks*, Vol. 2022, pp. 1-8, 2022.

[26] J. Luts, F. Ojeda, R. Van de Plas, B. De Moor, S. Van Huffel, and J. A. K. Suykens, "A tutorial on support vector machine-based methods for classification problems in chemometrics", *Analytica Chimica Acta*, Vol. 665, No. 2, pp. 129-145, 2010.

[27] L. Bedogni, M. Di Felice, and L. Bononi, "By train or by car? Detecting the user's motion type through smartphone sensors data", In: *Proc. of 2012 IFIP Wireless Days*, IEEE, Nov. 2012, pp. 1-6.

[28] K. Seifert and O. Camacho, *Implementing Positioning Algorithms Using Accelerometers*, 2007.

[29] Madison E. Martin, *Discrete Digital Filter Design For Microelectromechanical Systems (Mems) Accelerometers and Gyroscopes*, 2010.

[30] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines", *ACM Transactions on Intelligent Systems and Technology*, Vol. 2, No. 3, pp. 27:1-27:27, 2011.

[31] J. Cervantes, F. Garcia-Lamont, L. Rodríguez-Mazahua, and A. Lopez, "A comprehensive survey on support vector machine classification: Applications, challenges and trends", *Neurocomputing*, Vol. 408, pp. 189-215, 2020.

[32] A. Prasad, A. K. Tyagi, M. M. Althobaiti, A. Almulihi, R. F. Mansour, and A. M. Mahmoud,

"Human Activity Recognition Using Cell Phone-Based Accelerometer and Convolutional Neural Network", *Applied Sciences*, Vol. 11, No. 24, p. 12099, 2021.

[33] C.-H. Tsai and P.-C. Su, "An ECC-Based Blind Signcryption Scheme for Multiple Digital Documents", *Security and Communication Networks*, Vol. 2017, pp. 1-14, 2017.