A Secure Recommendation System for Providing Context-Aware Physical Activity Classification for Users

by Roy Setiawan

Submission date: 23-Nov-2022 02:19PM (UTC+0700)
Submission ID: 1961901010
File name: A_Secure_recomendation.pdf (3.18M)
Word count: 8917
Character count: 47931

Hindawi
Security and Communication Networks
Volume 2021, Article ID 4136909, 15 pages
https://doi.org/10.1155/2021/4136909

WILEY | Hindawi

Research Article

A Secure Recommendation System for Providing Context-Aware Physical Activity Classification for Users

Sudhakar Sengan,[1] Subramaniyaswamy V,[2] Rutvij H. Jhaveri,[3] Vijayakumar Varadarajan,[4] Roy Setiawan,[5] and Logesh Ravi[6]

[1]*Department of Computer Science and Engineering, PSN College of Engineering and Technology, Tirunelveli, India*
[2]*School of Computing, SASTRA Deemed University, Thanjavur, India*
[3]*School of Technology, Pandit Deendayal Energy University, Gujarat, India*
[4]*School of Computer Science and Engineering, University of New South Wales, Sydney, Australia*
[5]*Department of Management, Universitas Kristen Petra, Indonesia*
[6]*Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India*

Correspondence should be addressed to Rutvij H. Jhaveri; rutvij.jhaveri@sot.pdpu.ac.in

Received 24 June 2021; Accepted 22 October 2021; Published 12 November 2021

Academic Editor: Feiran Huang

Advances in Wireless Body Area Networks, where embedded accelerometers, gyroscopes, and other sensors empower users to track real-time health data continuously, have made it easier for users to follow a healthier lifestyle. Various other apps have been intended to choose suitable physical exercise, depending on the current healthcare environment. A Mobile Application (Mobile App) based recommendation system is a technology that allows users to select an apt activity that might suit their preferences. However, most of the current applications require constant input from end-users and struggle to include those who have hectic schedules or are not dedicated and self-motivated. This research introduces a methodology that uses a "Selective Cluster Cube" recommender system to intelligently monitor and classify user behavior by collecting accelerometer data and synchronizing with its calendar. We suggest customized daily workouts based on historical user and related user habits, interests, physical status, and accessibility. Simultaneously, the exposure of customer requirements to the server is also a significant concern. Developing privacy-preserving protocols with basic cryptographic techniques (e.g., protected multi-party computing or HE) is a standard solution to address privacy issues, but in combination with *state-of-the-art* advising frameworks, it frequently provides far-reaching solutions. This paper proposes a novel framework, a Privacy Protected Recommendation System (PRIPRO), that employs HE for securing private user data. The PRIPRO model is compared for accuracy and robustness using standard evaluation parameters against three datasets.

1. Introduction

Physical Activity (PA) is defined by the World Health Organization (WHO) as the body's movement using skeletal muscles while consuming energy. These activities can be working, playing, performing domestic chores, wayfaring, and merrymaking activities. Routine PA demanding the average workforce like walking, cycling, or sports practices gives remarkable health benefits. However, inadequate PA is also one of the risk factors for worldwide mortality and keeps escalating in most countries, increasing the Non-Communicable Diseases' (NCDs) burden and affecting general health globally. The inadequately active people are at a high risk of death, 20%–30% compared to adequately active people. Many researchers and scholars from different spheres have been inclining towards health-oriented topics, commissioned by incorporating technological devices and tools in healthcare service platforms, called e-Health [1, 2]. These systems drive a growing number of users, and the stimulation is mainly due to the arrival and dispersal of smart devices and the pursuit of intelligent life.

The outreach of the smartphone has been an excellent potential for a personalized Activity Recommender System (ARS) for individuals. Explicitly, many smartphone applications and wearable devices associated with Wireless Body Area Network (WBAN) track step count meticulously. Only a subtle difference was identified in the data collected from smartphones than the monitored step counts. However, the step counts could be either higher or lower. Simultaneously, the wearable devices showed huge discrepancies, and the step counts in 1 device were above 20%, which was relatively lesser than monitored. Step counts are the usual means for measurement calculation of PA, such as distance or calories burned. The substantive difference in the precision of the device may be fused in these measures. These devices eased increased PA, leading to clinical benefits unapprehend by low adoption of pedometers.

Usually, the users are endowed with elaborate interfaces by smartphone applications that visually track users' activity levels. The MD and wearable devices used for the study proved to be very accurate for tracking step counts. The accelerometer data was used in other studies to recognize/differentiate static and dynamic user states, day to day activities like running, leisurely walking, and riding bicycle [3, 4], and some physical movements (sitting or standing, lying, walking, etc.) [5].

More Mobile apps to track physical activities have access to MD. The rapid development of cutting-edge Mobile Devices (MD) solutions such as Wi-Fi/GPS has prompted the development of Location-Based Social Network (LBSN), factors such as Loopt, Brightkite, Foursquare, Gowalla, and Whrrl, which subsequently increases the ability to evaluate to multiple locations as a novel trend for smartphone users [6, 7], and it encourages users to leave comments, tips, or ratings of the visited sites/activities performed depending on their satisfaction level. All these facilities gradually expedite the growth of enormous data accumulation, which is the means to enhance user characteristics. Similarly, it facilitates experts in designing valuable services for users to compete with contemporary living standards.

Apart from the Point of Interest (POI) recommendation, which has received much attention in research and business [8, 9], a great deal of services is being developed based on LBSN data that appear to be promising to users as well. At the same time, compared with various conventional encryption algorithms, there is a high level of confidentiality with a smaller key size. In the security analysis part, the suggested security strength [10, 11] against various harmful security threats is demonstrated to ensure greater security. Recommendation Systems (RS) for outdoor activities such as playing, bowling, or strolling to an American fast-food place are examples of these services. There is an increase in the performance of a variety of activities during leisure time. The growing demand for e-healthcare systems requirements is due to increased technologies for a sporty and healthy lifestyle. Stability in an individual's health awareness is caused by an integrated health care system consisting of functional capabilities [12, 12, 13]. A headway in personalized technologies has elaborated the scope of research to achieve Digital Data-Driven Decision-Making Systems (DDDMS) connected with real-time health data. Digital health MD such as the Apple Watch, Google Fit, and Samsung Health, which accurately monitor personal Health and fitness tracking, is a key component of today's modern e-healthcare systems. These devices are very supportive, as they suggest recommended features that efficiently analyze the human body, which include footsteps, heart rate, and hours of sleep [14–16]. These systems additionally focus on fitness tracking.

Though Regular Physical Activity (RPA) benefits are testimonial, they have minimal effect in making inactive people cling to an activity. The surveys carried out in various industrialized nations show that 10% of inactive adults start a regular exercise program in a year, and 50% of the people who begin sports or RPA withdraw from the program in 6 months. Hence, increasing involvement or continuation of RPA has been a flourishing research area in sport medicine [17]. Though sufficient proofs exist regarding the reasons and the possible methods for increasing involvement, these proofs vary from country to country. For instance, self-efficacy is one of the leading causes of exercise adherence [10, 18, 19]. General Perceived Self-Efficacy Scale is a ubiquitous method for measuring self-efficacy. This has been used across diverse cultures and has been authorized through usual statistical analysis for diversified languages, including Japanese [20–22].

This paper proposes PRIPRO and a privacy-protected activity recommendation system that utilizes a Homomorphic Encryption (HE) model to protect user details and furnish accurate activity recommendations that depend on the user's present scenario. The paper is organized as follows: Section 2 consists of related works about various methodologies for detecting and classifying humans' healthcare. Section 3 describes the working principle and process of system structure and data set included in the proposed method, and Section 4 produces the best outcome of our model with the best accuracy. Section 5 shows the conclusion part, Section 6 acknowledges all the authors, and Section 7 gives the references we have referenced for producing the best result by overcoming the drawbacks of existing methods.

2. Related Works

Designing a DDDMS for exercise and sports involves many practical difficulties, complicating using one of the well-known recommender systems [23, 24]. Firstly, it is a different experience to see people doing the same exercise at the same places, not to mention differences between gymnasiums. An easy exercise, like walking, can even give new feelings when done at different spots. Therefore, the proposed recommender system has been designed, so that people with a proven history of regular exercising and performing "similar" sports might also make "similar" inactive people active. In other words, the philosophy we have used in our design was the information associated with a lifestyle that we collected by doing complete health check-ups in Japan and Ningendoku, which might be quite good indicators that explain how similar people are. If an inactive

person wants to begin an activity, the best way is to discover a similar person and suggest the same exercise.

With the advancement of wearables in WBAN, like various Internet of Things (IoT) smart devices such as fitness trackers and smartwatches, the quantity and prototype of gathered health care data have expanded. As a result, this needs new and scalable structures to ensure user privacy and real-time medical data used for analytical purposes. This is extremely crucial, because the gathered multimedia data enable more number applications resulting in data leakage. For example, an average fitness tracker can collect information regarding the user's location, timestamp, heart rate, daily activities, nutrition, and sleep cycles. These real-time health data are fetched from the whole user base and thoroughly analyzed for DDDMS to offer personalized recommendations. As the user real-time health data is wholly accessible by commercialized e-health solutions, this may become a hurdle for mass adoption of fitness devices, as DDDMS are driven by Machine Learning (ML) applications that are only beneficial by exploring huge volumes of medical data. Exploring the use of cryptographic techniques and differential privacy is done to enhance privacy in medical data communication systems and RS as a countermeasure [25–29]. Anyhow, to our knowledge, a bound privacy RS for the collection of real-time health data by MSs is mainly unexplored. The predominant challenge for designing privacy bound big-DDDMS, or health RS, includes the following (Table 1):

(1) Opting for distributed and cost-efficient privacy maintenance solutions

(2) The capability to back up a vast range of input data formats

(3) Design of smart incentive models to motivate data sharing by users

The PA-RS's biggest challenge is to make quality decisions by not compromising the active target user's privacy. Indeed, just about half of all individuals and a quarter of people over 65 years of age meet the minimum PA level needed to stay healthy (Dept. of Health in 2011). Inactivity is the leading cause of deterioration in physiological fitness and disease in the elderly. When the RS deals with a considerable quantity of sensitive user multimedia data, conventional recommendation approaches proved ineffective because of the generated data's scarcity and heterogeneous nature—with the evolving nature of the user's PA data, storing and computing the conventional data processing methods cost high. For decreasing computational overheads, it is highly suggested to shift the recommendation framework into a cloud environment. While getting into the cloud to produce quality recommendations, it is necessary to ensure user data privacy, especially when susceptible. Therefore, there is a need for a secured RS to maintain the user's privacy with a fool-proof mechanism. For expressing the privacy and security problems of RS, a new encryption approach is warranted by not adding the computational costs. With the desperate need to protect heterogeneous user data, an entirely new HE is proposed considering the RS research requirements. The use of the cloud paradigm guarantees a trusted computational environment and produces secure and quality recommendations [30]. For IoT-based WBANs, an efficient and secure anonymous authentication architecture is designed with location privacy protection [31]. The detailed study demonstrates that the proposed approach overcomes the security flaws of existing schemes while simultaneously reducing computing costs.

3. Proposed Methodology

3.1. PRIPRO System Design. Figure 1 demonstrates the system structure of PRIPRO. Mobile Devices furnish users' data for application recommendations. A Mobile app is fixed in every mobile device, and various functional modules are part of this application. The function of Reliability Monitor is to monitor the user's usage patterns of Mobile app usage and input user's data regarding their Access Patterns (AP), Usage Time (UT), and Activity Data (AD) into Device Database (DD).

The calculator performs necessary computations in MDs, e.g., summing AP, UT, AD, encryption, and decryption. Signature and anonymization of user identity are the responsibility of the Identity Manager. The Local Key Auditor performs the generation and management of related keys. Mobile data distributor passes encrypted data to cloud-based Recommendation Service Provider (RSP) and obtains data response. Device Database stores all the data in a secure way. RSP offers preprocessing data service (e.g., for recommendation purposes). RSP, basically a cloud service provider, possesses potential storage capacity, and computational capacity through user privacy is its primary concern. User Identity Manager (UIM) verifies the MD's ID and the processing of encrypted data correspondingly. The Privacy Protection Agency (PPA) manages smartphone access control and key management. Data Distributor enables the communication between MD and PPA in PPA. Figure 1 shows that the arrows present in each entity signify the flow of internal data. It is believed that MDs, RSP, and PPA communicate based on [32], which evaluates the application practice of users on their MD to find out their PA states. When the application detects a dormant state in the current environmental contexts, it recommends appropriate activities.

The flowchart representing the RS comprises three parts: (1) Data collection, (2) Preprocessing, and (3) DDDDMS and recommendation, as shown in Figure 1. The description of each part is elaborated in the following sections:

3.2. Privacy Protected Recommendation System (PRIPRO)

3.2.1. Data Collection. The Activity Recorder Module (ARM) facilitates the Data Collection Module inside the Mobile app to collect personal and sensor information, real-time medical data, and activity history. The first-time users of the proposed system are asked to fill out a questionnaire on the smartphone and maintain their personal information like age, gender, occupation, office hours, etc. The users would also fill out a scenario questionnaire that requires

Table 1: A review of context-aware RS.

Reference	Research findings	Limitations
A. M. Khan et al. (2010)	An accelerometer sensor depends on human-activity recognition	A single triaxial accelerometer connected to the chest produced an average accuracy of 97.9%.
J. Parkka *et al.* (2006)	Classification of activities using wearable sensor-based MD	Less classification accuracy using decision tree classifier and also for Artificial Neural Network (ANN)
M. A. Case *et al.* (2015)	Tracking activity and health of humans while walking on treadmill using MD	Results did not produce significant clinical benefit for patients having chronic knee pain
Mao Ye *et al.* (2011)	POI recommendation service through social networks	Social and geographical influence produces less effectiveness due to miscommunication through the social network.
Q. Tang *et al.* (2016)	A privacy-preserving hybrid RS using incremental matrix factorization and user-based collaborative filtering component	Feature vector components produce less efficient for privacy-preserving
S.L. Wang *et al.* (2016)	A hybrid predictive model that combines Markov chain and Grey Theory for predicting moving object's path	The cost for tracking errors is more for moving objects
Samsung, Apple (2017)	They have developed a wearable device for monitoring the heartbeat.	Less accuracy while measuring the heartbeat of human
D. Singh *et al.* (2015)	E-healthcare monitoring applications that require secure 6LoWPAN networks	Communication through protocols produces more challenges through embedding services.
A.H. Sodhro et al. (2018)	A novel framework for highly prevalent healthcare that manages to combine data transmission control and duty-cycle adaptation.	Produces more energy consumption while processing through the on-WBAN channel.
T. Shaw *et al.* (2017)	Developed a conceptual practice-based model of e-health to assist health professionals	Thermotical analyses produce less specific by restrictive ease of translation.
Samir Mustapha *et al.* (2020)	Continuous structural health monitoring systems to detect damage assessment and failure prediction.	Costlier while moving for real-time monitoring system

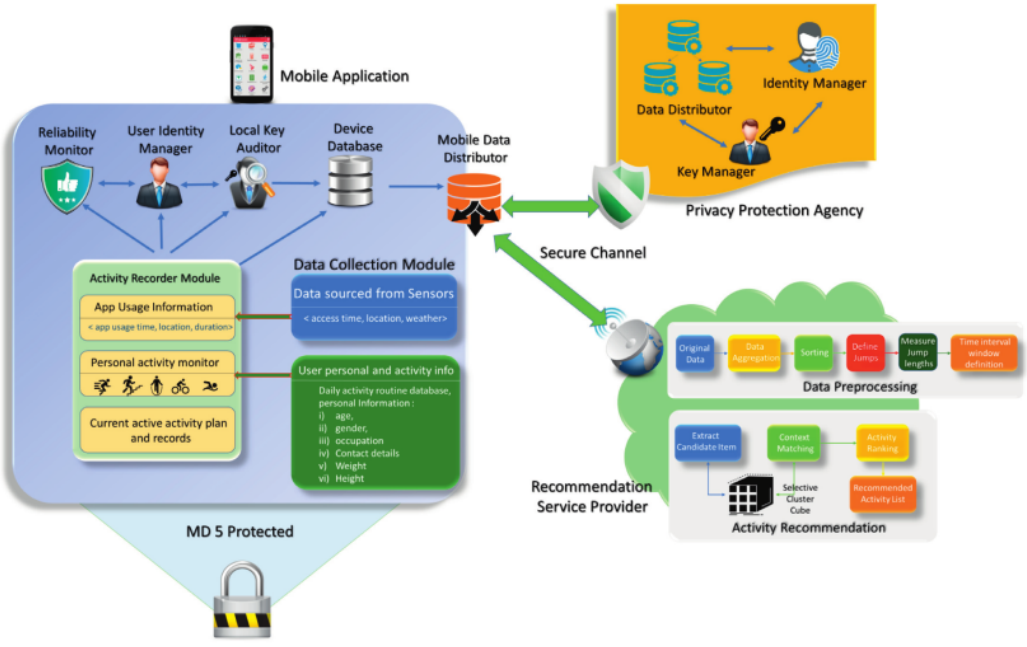


Figure 1: PRIPRO–privacy protected recommendation system.

them to select their interested activities under a different context. This paper defines context as a blending of environmental factors (e.g., office hours, workplace, and weather). Each Recommended Activity (RA) is recorded in the RS. The labelling of activity levels was 3D of the participant's PA regular, occasional, and rare.

Further, each dimension was divided into three levels: Low, Middle, and High. When an activity is recommended,

the user's current location (tracked using GPS/Wi-Fi) and time are detected to determine their environmental context. Activity item history maintains the user's current context and the selected activities (e.g., office hours, workplace, comfortable weather, music, etc.)

3.2.2. Data Preprocessing. A real-time data must be preprocessed to spot the features inside a particular time window, which will be used as input for the DDDMS. The system's parameter binds the time windows, and it is unique for every user and every activity. The original data store records are categorized according to the user ID and activity in the first step. After that, the records are grouped as a timestamp in ascending order. The second step identifies the *Jumps*, which are durations when there is no data collection. The parameter of the framework is the jump time interval, which is to be found out experimentally. The jump time interval was fixed as 5 minutes in our framework. Lastly, the length of each interval was determined, which requires the identification of user activity. Study experimentation was done with specified time intervals of 15 *Secs*, 10 *Secs*, and 5 *Secs*.

More amount of data is needed to be gathered as it is generated every 50 ms. Apache Kafka is used to streaming the data in real-time, whereas Cassandra is ideal for storing time-series data, because it can handle real-time requests. The feature calculation mechanism ingests stored data in Cassandra, and later it enables the application's classifier algorithm to sort out the user's activity in near real-time. High scalability with more number of users is achieved in decoupling between data generation and classifier via Kafka. In the existing implementation, user activities' classification was carried out in one of the following categories: running, stepping up the staircase, swimming, skipping, and cycling. The classifier should classify each category with maximum accuracy, because some activities present the same characteristics (for example, running, and jogging). For identifying user activity for a specific time interval, we adopted an approach of getting inspired by the work of [33, 34] and discovered the following features:

The analysis of the features was done for specific window sizes, and later, the user's activity was classified according to the count for each window.

3.2.3. Recommendation Module. The user's activity collected by the ARM was executed as the candidate item set in the recommended module:

$$A_s = \{\text{activity}_p | p \in \text{userset}\}. \quad (1)$$

Besides, we assume that three factors affect the activity rating. They are activity, user, and context. The 3D cube stores the activity rating, like the one shown in Figure 2. This cube is being named Selective Cluster Cube (SCC). The Selective Cluster Matrix *(SCM)* represents each candidate activity with different contexts. In a specific context, a candidate item is expressed as an array. Every element of the array is the selective probability $S_w(P_u, c_j)$ that the user "u" has chosen the activity w under the situation "c_j." In this paper, the selective probability was calculated from activity history. Users belonging to the same group consist of the same candidate activity Set A_s, and the users have shared a standard SCC.

For example, in Figure 2(a), "skipping" was the RA (item). The equivalent context c_0 was [non-office hour, home, comfortable weather]. The probability of user 1 for "skipping" under the context of the non-office hour, home, and comfortable temperature was 0.76. In the same way, the probability of user 2 for "skipping" was 0.64. If the participant is idle, the system consecutively detects the present context and asks all the activity arrays that match SCC's current context. For example, in Figure 2(b), if the system tracks situation c0, activity arrays with context C_0 will be obtained from the SCC.

The rating of candidate activity items was done according to a grade function, $g\text{Total}(S_w)$, and it measures the combined probabilities of the target user and the other users in the same group within the Time Window (T_w). This is shown as follows:

$$g\text{Total}(S_w) = S_w(P_u, c_j) + \pi \times S_w(P_{\text{userset}}, c_j), \quad (2)$$

where $S_w(P_u, c_j)$ indicates the probability of the target user "u" perform activity "w" under context j, and $S_w(P_{\text{userset}}, c_j)$ is the probability of the other users in the same group perform item "k" under the same context j. If "n" stands for the number of users in the user group, then $S_w(P_{\text{userset}}, c_j)$ is calculated as follows:

$$S_w(P_{\text{userset}}, c_j) = \frac{\sum_{a=1}^{n} S_w(P_u, c_j)}{n}, \quad n \neq u. \quad (3)$$

π is the influence parameter and is defined as

$$\pi = \begin{cases} 1, & \text{if } tw < 0, \\ \dfrac{1}{tw}, & \text{if } tw > 0. \end{cases} \quad (4)$$

At last, the item list was recommended to the user. The system also recorded the history of user interaction with the items. The participants' historical data consisted of the present context, and the things are opted by the participant from the recommendation list.

3.3. Proposed Security and Threat Model. The following are the description of the security and threat model:

(i) For starters, smartphone users, RSPs, and PPAs do not discuss individual benefits and reputations. Furthermore, they execute each task and performance characteristics following the set design.

(ii) Secondly, the communication of mobile users with RSP using anonymous identities is done candidly. We believe that protected channels (e.g., SSL protocol or other encryption protocols) are used among system entities in the medical data communication process.

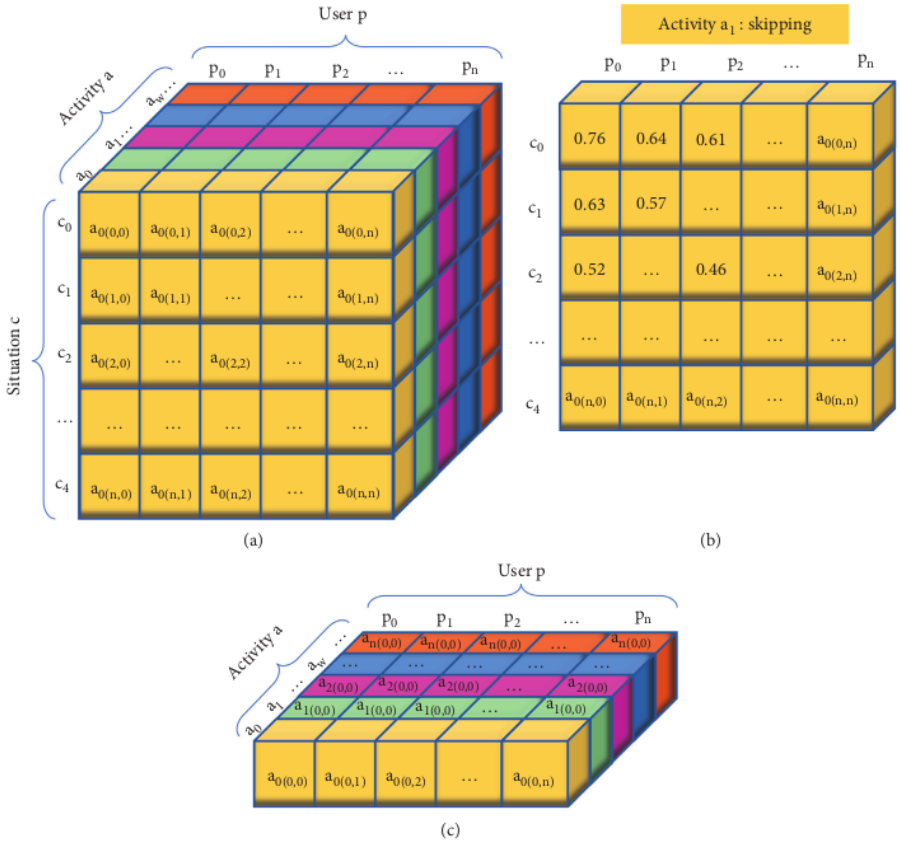


Figure 2: (a). "Skipping"-RA. (b) Array activities of system track the situation. (c) Selective Cluster cube.

(iii) Thirdly, privacy leakage is the biggest threat for mobile users (e.g., disclosing personal data of high sensitivity and mining personal privacy through data analytics) when the formalized data about AP, UT, PA, and other similar data are transmitted to RSP. Yet, giving normalized data, to some extent, will protect user privacy. Nonetheless, user's private information (e.g., similarities of other's favorites) is also a botheration for mobile users when an application recommendation is requested for themselves.

(iv) Fourthly, the semitrusted nature of RSP can make it achieve the functionalities based on system design. But simultaneously, it is also conscious of user privacy, and there are possibilities of user privacy leakage when it obtains any helpful information.

(v) Lastly, PPA, which is also semitrusted, can complete allocated system tasks according to system design through PPA that is also conscious about protecting user privacy.

3.3.1. Encryption Schemes. This section consists of an introduction briefing HE and an application used in our schemes, followed by summarizing notation for easy reference. Finally, a description of the detailed protocol of the two proposed methods is given correspondingly.

3.3.2. Homomorphic Encryption. Homomorphic Encryption (HE) permits computations to be performed over cipher texts. The decryption results are identical as if the HE operations had been carried out on the Plaintexts (PT) [34–37]. As an illustrative example, assume two plain texts Txt_1 and Txt_2, and their equivalent Ciphertexts (CT) $txt_1 \leftarrow \mathbb{HM}_{enc}(txt_1, key)$, $txt_2 \leftarrow \mathbb{HM}_{enc}(txt_2, key)$. An encryption scheme is additively homomorphic if $txt_1 + txt_2 = \mathbb{HM}_{dec}(txt_1 \boxplus txt_2, key)$/multiplicatively homomorphic if $txt_1 \times txt_2 = \mathbb{HM}_{dec}(txt_1 \boxtimes txt_2, key)$ where $\boxplus$ and $\boxtimes$ stand for the homomorphic addition and multiplication operations, correspondingly. A few HE schemes are either additively homomorphic/multiplicatively homomorphic, like [28]. The schemes that come into this category are said to be Partially Homomorphic Encryption (PSE). The schemes that support both additions and multiplications but are restricted only a few times are called Some What Homomorphic Encryption (SWHE). This is contrary to those that allow unlimited homomorphic operations, which are entitled as Fully Homomorphic Encryption (FHE) schemes [38]. The

competence of the techniques in each class is generally associated with the supported operations' expressiveness, which means that PHE schemes are more competent than SWHE schemes, which are more intelligent than FHE schemes. Besides, the additively or multiplicatively homomorphic nature of CTand HE methods also permit additions and multiplications between a CT and a PT, *i.e.*,$\text{txt}_1 + \text{txt}_2 = \mathbb{HM}_{\text{dec}}(\text{txt}_1 \boxplus \text{txt}_2, \text{key})$ and $\text{txt}_1 \times \text{txt}_2 = \mathbb{HM}_{\text{dec}}(\text{txt}_1 \boxdot \text{txt}_2, \text{key})$. (Table 2).

3.4. PRIPRO Recommendation System. This is an interactive procedure that is inclusive of the recommendation requestor, RSP, and PPA. As a first step, a request is sent to RSP by the recommendation requestor, and in turn, the PPA sends back a set of protected user dataset to the requestor on a condition [39] that the user validity check is positive. After that, the requestor processes user data embracing HE, and the processing result is sent to the RSP. Next, RSP does HEs on the processing result, which is necessary for producing recommendations for preserving privacy. Finally, the requestor creates final recommendations on his MD using the calculated results sent from RSP. In this way, HE user data are processed for making final decisions [40, 41].

A recommendation requestor, e.g., user p, sends his request $\{Mrk_p(\text{Uid}_p), Mrk_{\text{PPA}}(Mrk_p(\text{Uid}_p))\}$ to SP, where $Mrk_p(\text{Uid}_p)$ is the signature of p on his unknown identity and $Mrk_{\text{PPA}}(Mrk_p(\text{Uid}_p))$ is PPA signature on p's signature. RSP verifies the validity of p with the support of PPA. If the check is positive, RSP computes the correlation of the user p with the rest of the users (user k) $Crl(p, j)$ based on Equation (5); otherwise, RSP's performance is null.

$$Crl_s(p, j) = Enc(s_w) * \sum_{i' \neq i} \left(\frac{\sqrt{\left(F_{i'}^{p}(x(\text{AP})) - F_{i'}^{k}(x(\text{AP}))\right)^2 + \left(F_{i'}^{p}(x(\text{UT})) - F_{i'}^{k}(x(\text{UT}))\right)^2 + \left(F_{i'}^{p}(x(\text{PA})) - F_{i'}^{k}(x(\text{PA}))\right)^2}}{3} \right) \tag{5}$$

where $F_{i'}^{p}(\text{AP})$ User p's formalized AP value is related to application i', and the rest of the symbols imitate the same representation style. The correlations are preserved by $\text{Enc}(c_1)$ at context x (the concrete i of $\text{Enc}(c_i)$ is determined based on which context it is). Then, RSP encrypts$Crl_s(p, j)$ as $\text{Enc}(Crl_s^{p,j}) = \text{Enc}\{p(K_{\text{pub}}), Crl_s(p, j)\}$ with user p's public key $p(K_{\text{pub}})$ and returns a set of encrypted user's correlations$\{c, \text{Enc}(Crl_s^{p,j}),\ p \neq j\}$, to user j. After getting $\{c, \text{Enc}(Crl_s^{p,j}),\ p \neq j\}$, user j decrypts $\text{Enc}(Crl_s^{p,j})$ with his secret key $j(K_{\text{sec}})$. After that, it chooses $\text{Enc}(s_1)$ following time context c and obtains a set of user's accurate correlations $\{Crl(p, j),\ p \neq j\}$ by removing$\text{Enc}(s_w)$. It is to be noted that user "j" is anonymous of anyone correlative user's true identity, user "p," for instance, because none of the User's ID is known. Then, user "j" encrypts $Crl(p, j)$ into$\mathbb{HM}_{\text{enc}}\{j(K_{HM}), Crl(p, j)\}$ with his HE key $j(K_{HM})$ and transmits a set of encrypted values $\mathbb{HM}_{\text{enc}}\{j(K_{HM}), Crl(p, j)\}, p \neq j$to RSP. Consecutively, RSP sums up the encrypted user correlation based upon HE computations:

$$\mathbb{HM}_{\text{enc}}\left\{ j(K_{HM}), \sum_{p \neq j} Crl(p, j) \right\}, \tag{6}$$

by making use of homomorphic operation PaillierMul, refer to equation (6):

$$\mathbb{HM}_{\text{enc}}\left\{ j(K_{HM}), \sum_{p \neq j} Crl(p, j) \right\} = \prod_{p \neq j} \mathbb{HM}_{\text{enc}}\{j(K_{HM}), Crl(p, j)\}. \tag{7}$$

Then, RSP sums up the formalized values of AP, UT, and PA with user correlation by using homomorphic operation PaillierExp, refer to equation (7):

$$\mathbb{HM}_{\text{enc}}\left\{ j(K_{HM}), \text{Enc}(s_w) * \begin{Bmatrix} F_{i'}^{p}(x(\text{AP})) \\ F_{i'}^{p}(x(\text{UT})) \\ F_{i'}^{p}(x(\text{PA})) \end{Bmatrix} \right\} * Crl(p, j) = \mathbb{HM}_{enc}\{j(K_{HM}), Crl(p, j)\}\text{Enc}(s_w) * \begin{Bmatrix} F_{i'}^{p}(x(\text{AP})) \\ F_{i'}^{p}(x(\text{UT})) \\ F_{i'}^{p}(x(\text{PA})) \end{Bmatrix}. \tag{8}$$

RSP further sums up the encrypted cumulative result by using PaillierMul again (i.e., equations (8) and (9)):

$$\mathbb{HM}_{\text{enc}}\left\{ j(K_{HM}), \sum_{j \neq p} \left\{ \text{Enc}(s_w) * \begin{Bmatrix} F_{i'}^{p}(x(\text{AP})) \\ F_{i'}^{p}(x(\text{UT})) \\ F_{i'}^{p}(x(\text{PA})) \end{Bmatrix} \right\} \right\} * Crl(p, j) = \prod_{j \neq p} \mathbb{HM}_{\text{enc}}\{j(K_{HM}), Crl(p, j)\}\text{Enc}(s_w) * \begin{Bmatrix} F_{i'}^{p}(x(\text{AP})) \\ F_{i'}^{p}(x(\text{UT})) \\ F_{i'}^{p}(x(\text{PA})) \end{Bmatrix}. \tag{9}$$

Table 2: Parameters of HE.

Notations	Description
U_{IDp}	User_ID of a Person p
Mrkp(t)	Signature of person "p" on "t"
EC(K, t)	Pub_Key_Encryption on PT with key K
$\mathbb{HM}_{enc}$ (t, K)	HE on text "t" with key K
P(Kpub)	Person P's Pub_Key
P (Ksec)	Person P's secret key
Ep(t)	Person P's encrypted Data
T	Time
Fp(AP)	Formalized value of person P's mobile app access patterns
FP(UT)	Formalized value of person P's mobile app usage time
FP(PA)	Formalized value of person P's PA

Input: $\mathbb{HM}_{enc}\{\mathbf{j}(\mathbf{K_{HM}}), \mathbf{Crl}(\mathbf{p}, \mathbf{j})\}, \mathbf{p} \neq \mathbf{j}$, the set of HE user correlations between user k and other users $\mathbf{Enc}(\mathbf{s_w}) * \begin{Bmatrix} \mathbf{F_{i'}^p}(\mathbf{x}(\mathbf{AP})) \\ \mathbf{F_{i'}^p}(\mathbf{x}(\mathbf{UT})) \\ \mathbf{F_{i'}^p}(\mathbf{x}(\mathbf{PA})) \end{Bmatrix}, \mathbf{p} \neq \mathbf{j}$, the set of data vectors of other users of application "i" at context "c," secured by Enc(s_1)

Output: {M, N}: the data to calculate final recommendations

(1) **While** $p \neq j$ **Do**
(2) **For Each** activity "a" performed by "p" and "j," **Do**
(3) **Measure M:** the resultant value from the equations below steps (4) and (5)
(4) Measure the value as $\mathbb{HM}_{enc}\left\{ j(K_{HM}), \mathrm{Enc}(s_w) * \begin{Bmatrix} F_{i'}^p(x(\mathrm{AP})) \\ F_{i'}^p(x(\mathrm{UT})) \\ F_{i'}^p(x(\mathrm{PA})) \end{Bmatrix} \right\} * Crl(p, j) = \mathbb{HM}_{enc}\{j(K_{HM}), Crl(p, j)\}\mathrm{Enc}(s_w) * \begin{Bmatrix} F_{i'}^p(x(\mathrm{AP})) \\ F_{i'}^p(x(\mathrm{UT})) \\ F_{i'}^p(x(\mathrm{PA})) \end{Bmatrix}$.
(5) **Measure N:** the resultant value as $\mathbb{HM}_{enc}\left\{ j(K_{HM}), \sum_{j \neq p} \left\{ \mathrm{Enc}(s_w) * \begin{Bmatrix} F_{i'}^p(x(\mathrm{AP})) \\ F_{i'}^p(x(\mathrm{UT})) \\ F_{i'}^p(x(\mathrm{PA})) \end{Bmatrix} \right\} \right\} * Crl(p, j) = \prod_{j \neq p} \mathbb{HM}_{enc}\{j(K_{HM}), Crl(p, j)\}\mathrm{Enc}(s_w) * \begin{Bmatrix} F_{i'}^p(x(\mathrm{AP})) \\ F_{i'}^p(x(\mathrm{UT})) \\ F_{i'}^p(x(\mathrm{PA})) \end{Bmatrix}$.
(6) **End For**
(7) **End Do**
(8) Return (M, N)
(9) **End**

Algorithm 1: Homomorphic user correlation operations.

This encrypted sum will be sent to the user's MD to be used to compute a selection of features. Algorithm 1 explains those as mentioned above serial HE activities on encrypted user correlations.

3.4.1. Dataset. In recent times, datasets for distinct domain and context recognition have public accessibility. A real-time laboratory setup is done for the MIT Place Lab dataset. MD with integrated home settings was used to record the volunteers, and cameras fixed all over the houses were used for the annotation. In [42], the trial dataset was executed in a home system to monitor activity. This dataset utilization is effortless for binary sensing nodes (reed switches, pressure mats, etc.) and primarily comprises month-long readings. The dataset's existence in [43] spotlights individuals' *day-to-day* actions, recording a person's *everyday* life over 16 days. The Opportunity dataset [44] gives a tremendous recording of 12 subjects doing activities at dawn (activities of daily living (ADL)) in a room attached to a kitchen.

This dataset allows the use of sensors installed in the respondents' bodies and the environment, and it consists of over 25 hours of sensor information. At last, the TUM Restaurant database was collected and shared with the public for study purposes in fields such as markerless human performance capture, motion edge detection, and human activity recognition. Video data from 4-Cameras, Radio-Frequency Identification (RFID) tags, reed switch test results, and activity tags were included in the data source. Subsequently, the researcher [45] presented a standard dataset for estimating sensor migration in activity recognition. The data contains 33 PA identified using 9 inertial sensor units from 17 subjects.

(1) PAMAP Dataset. As part of the aerobic activity, monitoring uses specific instances, and the PAMAP recording was performed using a system developed in the previous Physical Activity Monitoring for Aging People (PAMAP) design [46]. The information was analyzed in August 2020. At the time of data collection, wired 3D-IMUs and an HR monitor were used as sensing devices, and a Sony Vaio Ultra-Mobile PC

(UMPC) was used a retrieve data from things. Each of the 8 test subjects implements a one-hour-long data collection task. Thus, the data collection comprises 8 hours of data roughly. The dataset is open access and can be downloaded from the research work website1 for research purposes.

(2) Data Set for Monitoring Physical Activity in PAMAP2. The PAMAP2 Physical Activity Monitoring datasets contain 18 comprehensive physical activities (such as stepping, riding a bicycle, and sporting events) undertaken by 9 subjects while wearing three inertial measurement systems and a heart rate sensor. More than 10 *Hrs.* of the survey was conducted in total, with approximately 8 hours labelled as one of the 18 activities. The data is accessible to the public and can be retrieved from the PAMAP research work's website2. Furthermore, the type of data labelled "PAMAP2 Physical Activity Monitoring Data Set" [47] is included in the UCI Machine Learning repository [48]. It measures by using 3 Colibri wireless inertial measurement units that consist of a timestamp, IMU hand, chest, and ankle. It contains temperature, 3D acceleration data, gyroscope data measured in rad/s, and magnetometer data (Î¼T).

(c) Real World (HAR). The dataset contains motion, location services, gyroscope, light, magnetic field, and environmental noise data from fifteen subjects age (31.9 ± 12.4⟶height; 173.1 ± 6.9⟶weight 74.1 ± 13.8; 8 Males and 7 Females) achieving behavior such as hopping, resting, standing, sitting, running/jogging, and walking. For each exercise, the rapid action of the chest, forearm, head, chin, thigh, shoulder blade, and waist was tracked in parallel. Each activity lasted approximately 10 minutes, excluding jumping (1.7 minutes) due to physical exercise.

4. Experimental Evaluation

Our approach's evaluation is done experimentally utilizing 3 real-time datasets and extensively used metrics with diverse parameters in this section. The experimental tests were carried out on a Desktop PC with a 2.9 GHz, 2.8 GHz, 2.2 GHz, Octa-Core CPU and 12 GB RAM, and a Galaxy S21 5G Android MD.

4.1. Accuracy Measures. The accuracy of the proposed method's generated recommendations is considered by using the Mean Absolute Error (MAE) and the Root Mean Square Error (RMSE) [31, 49]. Accuracy metrics were commonly used to assess the recommendation system. The MAE standard is defined in equation (10), with p_i representing the assumed score and r_i defining the overall score in the assessment. MAE is also used to measure the difference between the predicted and accurate scores. It should be acknowledged that lower values indicate a better prediction of guidelines. Equation (11), for instance, demonstrates RMSE [50, 51]. RMSE is the same as MAE but with squared values. As an outcome, lower values are recommendable to RMSE.

$$\mathrm{MAE} = \frac{1}{n}\sum_{i=1}^{n}\left|p_i - r_i\right|, \tag{10}$$

$$\mathrm{RMSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(p_i - r_i)}. \tag{11}$$

4.2. Results. Figures 3 and 4 demonstrate the MAE and RMSE values obtained from the 3 datasets. However, all the datasets show an initial deviation by the model since the K-value increases, and all the three models follow a similar pattern.

Top-K Mining (Figure 5). A metric that shows how well a user's favorite activities are protected. This metric is defined as $\mathrm{TKM} = 1/n\sum_{k=1}^{n}\mathrm{TPR}_k$, where TPR_k is the True Positive Rate (TPR) of the Top-K activities suggested by the data.

4.2.1. Robustness. The sturdiness of the 2 schemes was tested, taking into account the following attacks:

(i) Bad-Mouth Attack

- On–Off Attack

The impact of each attack over the dataset was calculated using the accuracy parameter, as shown in

$$\mathrm{Accuracy} = 1 - \frac{\sum_{i=1}^{n}(m + 1 - l_i)}{\sum_{j=1}^{m} w_j}. \tag{12}$$

(1) Bad-Mouth Attack. The results of 3 datasets of bad-mouth attack simulation are shown in Figures 6(a)–6(c). The 2 dataset's results are the same, and bad-mouthing attackers impact the 3rd dataset, Real World, but the impact has not increased with time flying. The technical details like misbehaving protocol like bad guy's bad breathing, crime attack, or escape sequences are included to identify vulnerabilities, defenses, and functionality. Thus, the outcome of the proposed method shows that it can resist bad-mouthing attacks to some extent.

(2) On-Off Attack. Figures 7(a) and 7(b) represent the outcome of on-off attack simulations of the proposed work. The on-off attack in PAMAP has a specific impact on recommendation accuracy initially. However, the impact reduces with time flying due to increased data volume for constructing the regular database in different time slots. The impact of the on-off attack on accuracy recommendation in PAMAP-2 and real-world oscillates with time flying, yet the oscillation range is quite admissible. The oscillation happens due to the database construction process that performs only at the time of generating recommendations.

4.3. User Interface of ARS with Implementation. The main goal of the experimental tests is to evaluate that the proposed mobile recommendation current study is better, practical, and novel. Evaluation tools are classified into two main

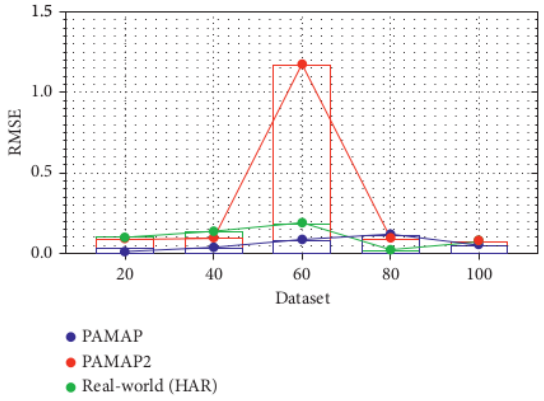


Figure 3: Three datasets were compared using the RMSE method.

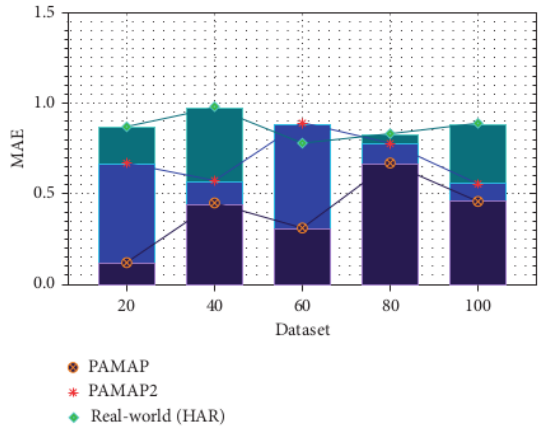


Figure 4: Three datasets were compared using MAE.

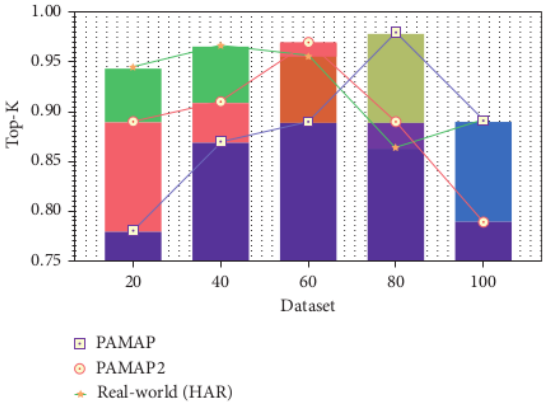


Figure 5: Top-K Mining value comparison.

categories: computational space and computational time. The processing time needed for DDDMS is a critical factor in determining the results of the developed framework. Processing time and the quality of DDDMS can both influence system efficiency. Offline and online data processing methods are used based on user requirements to reduce

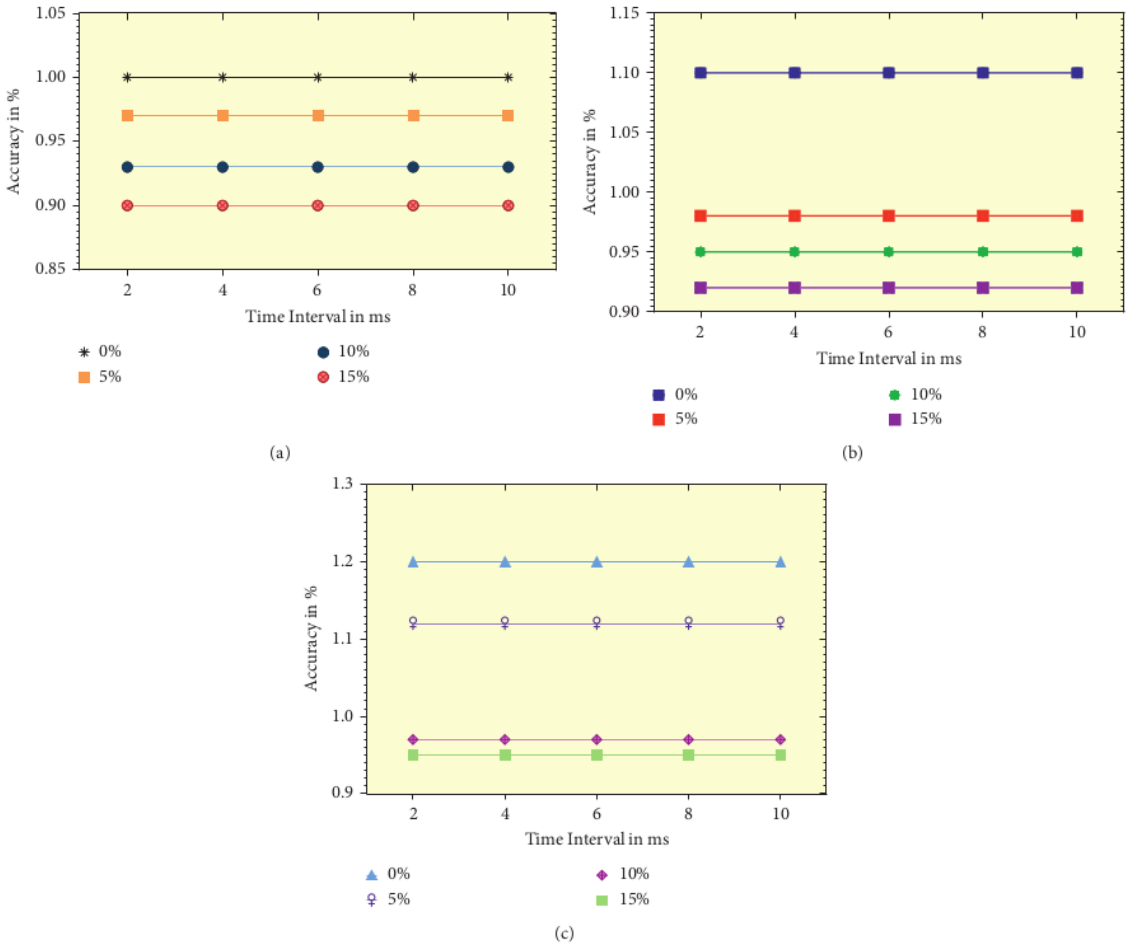


Figure 6: Accuracy value for the proposed model under bad-mouth attack for different datasets.

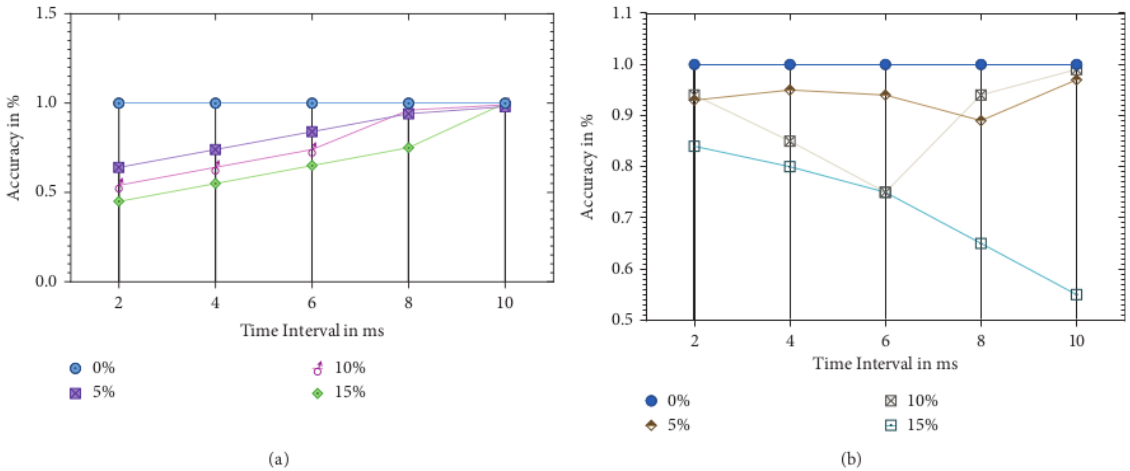
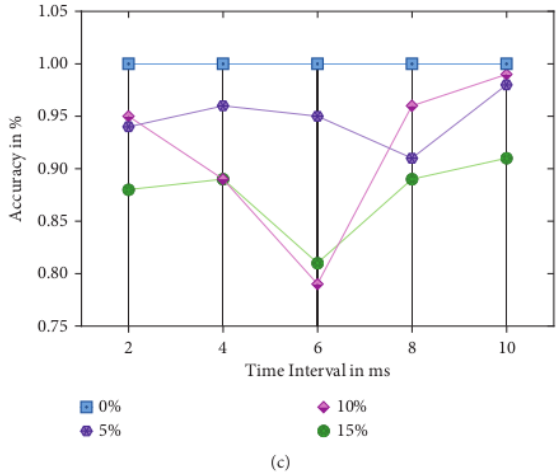
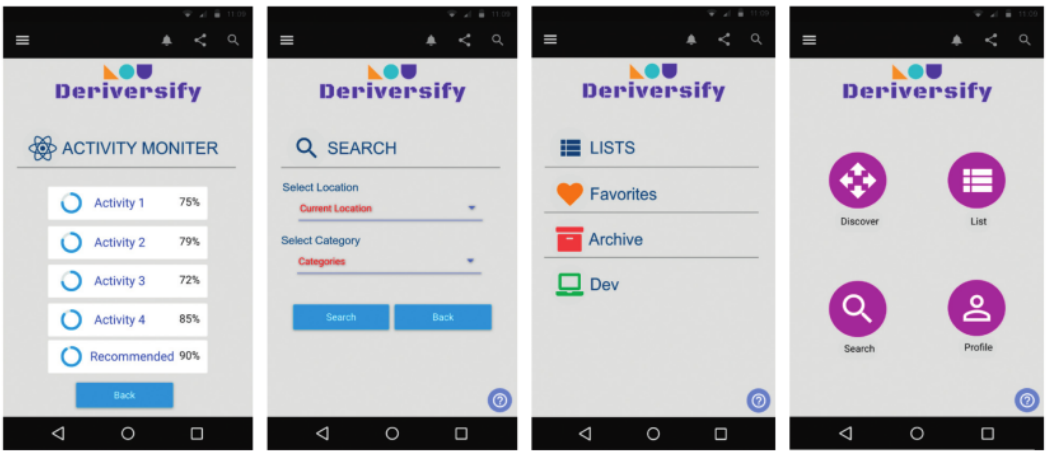


Figure 7: Continued.

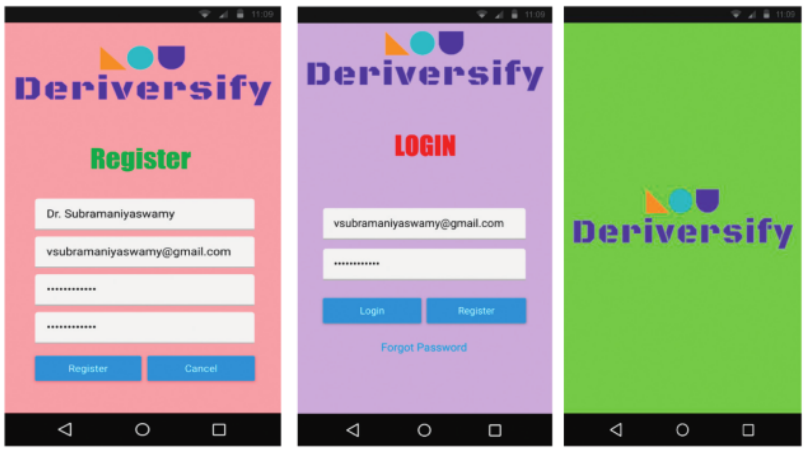


(c)

Figure 7: Accuracy value for the proposed model under bad-mouth attack for different datasets.



A Mobile App Implementation | User Data Screen: Login | User Data Screen: Register | User Application Screen



User Activity: Monitoring | User Activity: Analysis | User Activity Tracker

Figure 8: Activity recommender system with implementation.

computational time and make personalized decisions. Several works have aimed to go beyond classical accuracy metrics in the monitoring and development of RS design, focusing on recommendation diversification as a method of improving user serviceability. Because, in skipping alone, the user can attain breathing problems while doing exercise, so, here, we primarily consider understanding skipping alone. There will be some disturbance while calculating skipping in the user. This will be taken into consideration for RS. An ARS named "Diversify" was developed using the PRIPRO framework, illustrated in Figure 8, which includes both the GUI and deployment.

5. Conclusion

PRIPRO, a novel privacy security system for personalized fitness reviews, was introduced in this paper. Besides providing information on the device structure and module design, we quantitatively conduct an extensive experiments model against various datasets. We concluded that the proposed PRIPRO model is ideally suited to prescribe physical activity to the application user by considering the current context and maintaining the privacy of the user's data. PRIPRO is comprised of HE schemes in securing user data while making preferred decisions. PRIPRO model uses only arithmetic operations that are precisely accurate with HE methods. It can also make DDDMS using a pretrained model, while the client's data is not in the server training collection. The tests show that PRIPRO can provide high bandwidth recommendation solutions while still improving the *state-of-the-art* performance.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors thank the Department of Science and Technology, Science and Engineering Research Board for their financial support under the MATRICS Scheme (MTR/2019/000542). The authors also express their gratitude to SASTRA Deemed University for the infrastructure facilities and support provided to conduct the research.

References

[1] A. M. Khan, Y.-K. Young-Koo Lee, S. Y. Lee, and T.-S. Tae-Seong Kim, "A Triaxial accelerometer-based physical-activity recognition via augmented-signal features and a hierarchical recognizer," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 5, pp. 1166–1172, 2010.

[2] G. Adomavicius and A. Tuzhilin, "Toward the next generation of recommender systems: a survey of the state-of-the-art and possible extensions," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 6, pp. 734–749, 2005.

[3] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[4] M. Azees, P. Vijayakumar, and L. Jegatha Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intelligent Transport Systems*, vol. 10, no. 6, pp. 379–388, 2016.

[5] B. Attila Reiss, "PAMAP2 physical activity monitoring data set," URL http://archive.ics.uci.edu/ml/datasets/PAMAP2+Physical+Activity+Monitoring, 2013.

[6] M. Breyer, K. Nazemi, C. Stab, D. Burkhardt, and A. Kuijper, "A comprehensive reference model for personalized recommender systems," in *Human Interface and the Management of Information. Interacting with Information. Human Interface*, M. J. Smith and G. Salvendy, Eds., vol. vol 6771, Berlin, Heidelberg, Springer, 2011.

[7] D. M. Karantonis, M. R. Narayanan, M. Mathie, N. H. Lovell, and B. G. Celler, "Implementation of a real-time human movement classifier using a triaxial accelerometer for ambulatory monitoring," *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 1, pp. 156–167, 2006.

[8] D. Roggen, C. Alberto, M. Rossi et al., *Global Diffusion of eHealth: Making Universal Health Coverage Achievable: Report of the Third Global Survey on eHealth*, World Health Organisation, Geneva, Switzerland, 2017.

[9] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the forty-first annual ACM symposium on Theory of computing*, vol. 9, pp. 169–178, Bethesda, MD, USA, May 2009.

[10] Y. Liu, J. Yu, J. Fan, P. Vijayakumar, and V. Chang, "Achieving privacy-preserving DSSE for intelligent IoT healthcare system," *IEEE Transactions on Industrial Informatics*, 2021.

[11] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015–1028, 2015.

[12] A. Henriksen, M. Haugen Mikalsen, A. Z. Woldaregay et al., "Using fitness trackers and smartwatches to measure physical activity in research: analysis of consumer wrist-wornwearables," *Journal of Medical Internet Research*, vol. 20, 2018 [CrossRef] [PubMed].

[13] G. C. L. Hung, P. C. Yang, C. C. Chang, and J. H. Chiang, *Machine Learning-Based Analysis of Smartphone Usage Pattern and its Association with Negative Human Emotion*, Wireless Health 2014, Bethesda, MD, USA, 2014.

[14] J. Fan and F. Vercauteren, "Somewhat practical fully homomorphic encryption," *IACR Cryptology ePrint Archive*, vol. 2012, p. 144, 2012.

[15] J. P¨arkk¨a, M. Ermes, P. Korpip¨a¨a, J. M¨antyj¨arvi, J. Peltola, and I. Korhonen, "Activity classification using realistic data from wearable sensors," *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 1, pp. 119–128, 2006.

[16] J. Parkka, M. Ermes, P. Korpipaa, J. Mantyjarvi, J. Peltola, and I. Korhonen, "Activity classification using realistic data from wearable sensors," *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 1, pp. 119–128, 2006.

[17] J. R. Kwapisz, G. M. Weiss, and S. A. Moore, "Activity recognition using cell phone accelerometers," *ACM SIGKDD Explorations Newsletter*, vol. 12, no. 2, pp. 74–82, 2011.

[18] J. Sang, T. Mei, J.-T. Sun, C. Xu, and S. Li, "Probabilistic sequential POIs recommendation via check-in data," in *Proceedings of the 20th International Conference on Advances in Geographic Information Systems*, pp. 402–405, Redondo Beach, CA, USA, November 2012.

[19] K. Bache and M. Lichman, "UCI machine learning repository," 2021, http://archive.ics.uci.edu/ml.

[20] M. A. Case, H. A. Burwick, K. G. Volpp, and M. S. Patel, "Accuracy of smartphone applications and wearable devices for tracking physical activity data," *Journal of the American Medical Association*, vol. 313, no. 6, pp. 625-626, 2015.

[21] M.-K. Suh, A. Nahapetian, J. Woodbridge, M. Rofouei, and M. Sarrafzadeh, "Machine learning-based adaptive wireless interval training guidance system," *Mobile Networks and Applications*, vol. 17, no. 2, pp. 163–177, 2011.

[22] R. Maddison and H. Prapavessis, "Using self-efficacy and intention to predict exercise compliance among patients with ischemic heart disease," *Journal of Sport & Exercise Psychology*, vol. 26, no. 4, pp. 511–524, 2004.

[23] M. Ye, P. Yin, W.-C. Lee, and D. Lun Lee, "Exploiting geographical influence for collaborative point-of-interest recommendation," in *Proceedings of the 34th International ACM SIGIR Conference on Research and Development in Information Retrieval*, pp. 325–334, Beijing China, July 2011.

[24] E. McAuley and K. S. Courneya, "Self-efficacy relationships with affective and exertion responses to exercise," *Journal of Applied Social Psychology*, vol. 22, pp. 316–326, 1992.

[25] Millán, "Collecting complex activity datasets in highly rich networked sensor environments," in *Proceedings of the 7th International Conference on Networked Sensing Systems (INSS)*, pp. 233–240, Kassel, Germany, June 2010.

[26] M. Tenorth, B. Jan, and M. Beetz, "The TUM Kitchen data set of everyday manipulation activities for motion tracking and action recognition," in *Proceedings of the IEEE 12th International Conference on Computer Vision (ICCV), Workshop on Tracking Humans for the Evaluation of Their Motion in Image Sequences (THEMIS)*, Kyoto, Japan, September 2009.

[27] M. Oaklander, "The applewatch is the most accurate-wristwearable," Available online: http://time.com/4527843/accurate wearable-apple-watch-fitness-tracker (accessed on 12 October 2016), 2016.

[28] O. Baños, M. Damas, I. R. HéctorPomares, M. . A. Tóth, and A. Oliver, "A benchmark dataset to evaluate sensor displacement in activity recognition," in *Proceedings of the 14th International Conference on Ubiquitous Computing (UbiComp)*, pp. 1026–1035, Pittsburgh, PA, USA, September 2012.

[29] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proceedings of the Advances in Cryptology—Eurocrypt'99*, pp. 223–238, Springer, Zagreb, Croatia, October 1999.

[30] Pamap, PAMAP Project Website, 2013-09-16. URL http://www.pamap.org, 2013.

[31] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, "Efficient and secure anonymous authentication with location privacy for IoT-based WBANs," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2603–2611, 2020.

[32] L. Paul, G. Pirkl, D. Bannach et al., "Recording a complex, multi-modal activity data set for context recognition," in *Proceedings of the 23rd International Conference on Architecture of Computing Systems (ARCS), 1st Workshop on Context-Systems Design, Evaluation and Optimisation (CosDEO)*, Hannover, Germany, February 2010.

[33] P. Dixit, R. Kohli, A. Acevedo-Duque, R. R. Gonzalez-Diaz, and R. H. Jhaveri, "Comparing and analyzing applications of intelligent techniques in cyberattack detection," *Security and Communication Networks*, vol. 2021, Article ID 5561816, 23 pages, 2021.

[34] Q. Tang and H. Wang, "Privacy-preserving hybrid recommender system," [Online] Available:, 2016.

[35] R. Schwarzer and A. Born, "The assessment of optimistic self-beliefs: comparison of the Chinese, Indonesian, Japanese, and Korean versions of the general self-efficacy scale," *Psychologia: an International Journal Of Psychology in the Orient*, vol. 40, 1997.

[36] R. Panigrahi, S. Borah, A. Kumar Bhoi et al., "Performance assessment of supervised classifiers for designing intrusion detection systems: a comprehensive review and recommendations for future research," *MDPI- Mathematics*, vol. 9, no. 6, pp. 1–32, 2021.

[37] R. H. Jhaveri, A. Desai, A. Patel, and Y. Zhong, "A sequence number prediction based bait detection scheme to mitigate sequence number attacks in MANETs," *Security and Communication Networks*, vol. 2018, Article ID 3210207, 13 pages, 2018.

[38] S.-L. Wang, Y. L. Chen, A. M.-H. Kuo, H.-M. Chen, and Y. S. Shiu, "Design and evaluation of a cloud-based Mobile Health Information Recommendation system on wireless sensor networks," *Computers & Electrical Engineering*, vol. 49, pp. 221–235, 2016.

[39] S. Katzenbeisser and M. Petkovic, "Privacy-preserving recommendation systems for consumer healthcare services," in *Proceedings of the 3rd International Conference on Availability, Reliability, and Security (ARES)*, pp. 889–895, IEEE, Salzburg, Austria, March 2008.

[40] Samsung, "Start a Health Challenge," Available online: http://health.apps.samsung.com (accessed on 6 June 2017), 2015.

[41] D. Singh, "Secure 6lowpan networks for E-healthcare monitoring applications," *Journal of Theoretical and Applied Information Technology*, vol. 76, pp. 143–151, 2015.

[42] D. Singh, H. J. Lee, and W. Y. Chung, "Secure IP-ubiquitous sensor Network for healthcare applications monitoring in-home area," in *Proceedings of the 2nd International Conference on the Applications of Digital Information and Technologies (ICADIWT 2009)*, vol. 4–6, pp. 335–337, London, UK, August 2009.

[43] D. Singh, G. Tripathi, A. M. Alberti, and A. Jara, "Semantic edge computing and IoT architecture for military health services in battlefield," in *Proceedings of the 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 185–190, Las Vegas, NV, USA, January 2017.

[44] A. H. Sodhro, S. Pirbhulal, G. H. Sodhro, A. Gurtov, M. Muzammal, and Z. Luo, "A joint transmission power control and duty-cycle approach for smart healthcare system," *IEEE Sensors Journal*, vol. 19, 2018 [CrossRef].

[45] S. S. Intille, K. Larson, E. Munguia Tapia et al., "Using a live-in laboratory for ubiquitous computing research," in *Proceedings of the 4th International Conference on Pervasive Computing (PERVASIVE)*, pp. 349–365, Dublin, Ireland, May 2006.

[46] T. Shaw, D. McGregor, M. Brunner, M. Keep, A. Janssen, and S. Barnet, "What is ehealth (6)? development of a conceptual model for ehealth: qualitative study with key informants," *Journal of Medical Internet Research*, vol. 19, no. 10, p. 324, 2017.

[47] T. van Kasteren, A. Noulas, G. Englebienne, and B. Kröse, "Accurate activity recognition in a home setting," in *Proceedings of the 10th International Conference on Ubiquitous*

Computing (UbiComp), pp. 1–9, Seoul, South Korea, September 2008.

[48] T. Huynh, M. Fritz, and B. Schiele, "Discovery of activity patterns using topic models," in *Proceedings of the 10th International Conference on Ubiquitous Computing (UbiComp)*, pp. 10–19, Seoul, South Korea, September 2008.

[49] V. W. Zheng, B. Cao, Yu Zheng, X. Xie, and Q. Yang, "Collaborative filtering meets mobile recommendation: a user-centered approach," *AAAI*, vol. 10, pp. 236–241, 2010.

[50] R. S. Weinberg and D. Gould, *Foundations of Sport and Exercise Psychology*, Human Kinetics, Champaign, IL, USA, 4th edition, 2007.

[51] Y. Zheng, X. Xie, and Q. Yang, "Collaborative location and activity recommendations with GPS history data," in *Proceedings of the 19th International Conference on World Wide Web*, pp. 1029–1038, New York, NY, USA, April 2010.

A Secure Recommendation System for Providing Context-Aware Physical Activity Classification for Users

ORIGINALITY REPORT

14%	13%	2%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.researchgate.net Internet Source	4%
2	eudl.eu Internet Source	3%
3	deepai.org Internet Source	1%
4	works.bepress.com Internet Source	1%
5	kluedo.ub.uni-kl.de Internet Source	1%
6	Submitted to Govind Ballabh Pant Engineering College, Pauri-Garhwal Student Paper	1%
7	www.iadis.net Internet Source	1%
8	V. Subramaniyaswamy, V. Jagadeeswari, V. Indragandhi, Rutvij H. Jhaveri, V. Vijayakumar, Ketan Kotecha, Logesh Ravi. "Somewhat	1%

	Homomorphic Encryption: Ring Learning with Error Algorithm for Faster Encryption of IoT Sensor Signal-Based Edge Devices", Security and Communication Networks, 2022 Publication	
9	Submitted to UC, San Diego Student Paper	1 %
10	ejournal.um.edu.my Internet Source	1 %

Exclude quotes	Off	Exclude matches	< 1%
Exclude bibliography	On		