




Article

# RFID Authentication System Based on User Biometric Information <sup>†</sup>

Yuanmu Huang <sup>1</sup> , Bin Fu <sup>1,\*</sup> , Ningwei Peng <sup>1</sup>, Yanwen Ba <sup>1</sup>, Xuan Liu <sup>1,2</sup> and Shigeng Zhang <sup>3</sup> <sup>1</sup> College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China<sup>2</sup> State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210023, China<sup>3</sup> School of Computer Science, Central South University, Changsha 410008, China

\* Correspondence: fubin@hnu.edu.cn

<sup>†</sup> This paper is an extended version of our paper published in 16th International Conference, WASA 2021, Nanjing, China, 25–27 June 2021.

**Abstract:** Traditional authentication technologies usually perform identity authentication based on user information verification (e.g., entering the password) or biometric information (e.g., fingerprints). However, there are security risks when applying only these authentication methods. For example, if the password is compromised, it is unlikely to determine whether the user entering the password is legitimate. In this paper, we subdivide biometric information into physiological and behavioral information, and we propose a novel user authentication system, RF-Ubia, which utilizes the low-cost radio frequency identification (RFID) technology to capture unique biological or behavioral information rooted in the user and can be used in two schemes for user authentication. Consisting of an array of nine passive tags and a commercial RFID reader, RF-Ubia provides double assurance for security of identity authentication by combining user information and biometric characteristics. It first verifies the user's password, and then identifies the biometric characteristics of the legitimate user. Due to the coupling effect among tags, any change in tag signal caused by the user's touch will affect other tag signals at the same time. Since each user has different fingertip impedance, their touch will cause unique tag signal changes. Therefore, by combining biometric information, the tag array will uniquely identify users. The evaluation results show that RF-Ubia achieves excellent authentication performance with an average recognition rate of 93.8%.

**Keywords:** RFID; authentication; biometric information

**Citation:** Huang, Y.; Fu, B.; Peng, N.; Ba, Y.; Liu, X.; Zhang, S. RFID Authentication System Based on User Biometric Information. *Appl. Sci.* **2022**, *12*, 12865. <https://doi.org/10.3390/app122412865>

Academic Editor: Mario Lucido

Received: 27 October 2022

Accepted: 8 December 2022

Published: 14 December 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

With the rapid development of modern technology, new automatic identification technologies emerge in endlessly, among which radio frequency identification (RFID) technology has become the core technology of the Internet of Things with its excellent advantages.

With the commercialization of RFID, its application is becoming more and more widespread, including item tracking, motion detection [1,2], goods security and so on [3–7]. As the increasing demand on protection for security industry and personal privacy, user authentication technology has become particularly important. The purpose of user authentication is to verify whether a user is indeed a legitimate user registered in the system, which is a vital task in many applications, such as area or event access control and electronic payment.

In the existing work, user authentication methods are mainly divided into two categories: device authentication and user authentication. Authentication devices such as personal identity cards, authentication users such as fingerprints, etc.; both authentication technologies are each facing many potential risks and hidden dangers due to imperfect security mechanisms. Device authentication may have the risk of being lost, stolen, or copied. When users set their passwords too short or simple, their accounts can easily be stolen,

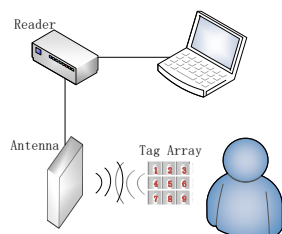
leading to insecure accounts on other systems as well. If complex passwords consisting of numbers and letters are used alternately, it can increase the security strength of the password, but it will increase the complexity of the system usage and is very unfriendly to users. When the system uses ID cards to identify and verify user identity, the cards may be at risk of being copied or lost. As in the Hu-Fu (Wang et al. [8,9]) authentication scheme, if the authentication tag is stolen by an attacker, the attacker can pass the authentication without any hindrance; with RF-Mehndi (Zhao et al. [10]), although the personal card is also able to resist the attacker's counterfeit when it is lost or stolen, the user card needs to be recreated and the information collected will still cause trouble to the user. User authentication-based schemes to verify users' biological information, such as Vauth (Feng et al. [11]), Cardiac Scan (Lin et al. [12]), BioTag (Hu et al. [13]), and TrueHeart (Zhao et al. [14]) continuous authentication schemes, mostly require the use of dedicated sensors, which have major limitations in terms of cost and applicability. While the mainstream user authentication methods now use biometric features such as the user's fingerprint, face (Xu et al. [15]), and iris to authenticate the user's identity, biometric features such as fingerprints provide a more excellent authentication performance compared to traditional authentication techniques. However, it is by nature a static image or data matching and still has the possibility of being copied. To overcome these problems, cutting-edge research has proposed a concept of continuous authentication, i.e., using some device to continuously extract dynamic human biometric features for authentication, such as breathing (Wang et al. [16]), heart rate (Zhao et al. [14]), and sound resonance (Feng et al. [11]). However, continuous authentication requires a very high acquisition rate and computational power of the device, leading to excessive cost and difficulty, and it can still only be implemented in an experimental setting.

In summary, although many user authentication methods have been proposed [5,8–10], they have some contradictions and drawbacks in terms of application target, deployment scope, cost, system complexity, and security resistance. It is a new challenge to find a simple and secure authentication method. To address the shortcomings of current user authentication methods, we subdivide biometric information into physiological and behavioral characteristics, and we design and implement RF-Ubia, which is a simple and secure user authentication method for different people, supports both password and passwordless authentication methods, and can achieve high recognition accuracy and at a much lower cost than existing work.

RF-Ubia consists of nine passive tags forming a cryptographic array, with each tag acting as a cryptographic button, as shown in Figure 1. Users only need to touch the tag surface once to enter a password number. When the user touches multiple tags continuously, the digital sequence obtained is used as the user authentication password. In the process of touching, we also skillfully incorporate the biometric information into tag signals. When different users touch the RFID tags, distinctive phase changes will occur as a result of users' different body impedance. The closer these tags are in the array, the stronger the coupling effect among them will become [8–10]. When a tag is touched, not only its signal will change, but also the signals of the other eight tags will change due to the coupling effect. These signal changes are highly correlated with the user's body impedance. Normally, the impedance of the human body is about 300–1000  $\Omega$ . Different users have different body impedance, which leads to different changes in the phase signal of the tags. Combined with user's biometric information, different users who entered the same password can be distinguished. The main contributions of our work are summarized as follows:

- We propose a low-cost simple user authentication method called RF-Ubia, which allows users to effectively resist password theft even with simple passwords.
- We propose an extension of the RF-Ubia system that fuses user impedance and behavioral features, allowing users to authenticate users even if they forget their passwords, and ensures security that is largely immune to environmental interference, achieving an average recognition accuracy of 0.94. We improve the traditional anomaly detection and feature extraction algorithms to obtain more fine-grained feature information to improve accuracy. We used Random Forest in Wake to classify, and RF-Ubia was

able to achieve an average recognition accuracy of 0.96 while existing work based on template matching or convolutional neural networks (CNN) was below 0.92 under the same conditions.



**Figure 1.** Illustration of RF-Ubia. The user touches the surface of the tag array to enter the password, and the reader captures the signal integrating the user's biometric characteristics.

## 2. Related Work

User authentication methods can be divided into three main categories: information, possessions, physiological and behavioral characteristics.

*Information*, such as passwords or security codes. The information-based approach is designed to use traditional cryptographic algorithms to perform authentication and use encryption technology to protect tags from illegal access [17–21]. Most of these methods require modifications to commercial communication protocols or tag hardware, making it difficult to apply them to lightweight passive tags.

*Possessions*, such as various certificates or ID cards. The physical information-based approaches identify and verify the tags by taking advantage of the differences in the tag circuit characteristics, which will be reflected in the backscattering signal. Ding et al. propose a reader authentication solution based on physical layer signals, namely Arbitrator [22,23], which can effectively prevent unauthorized access to tags. Ma et al. [24] propose a new physical layer recognition system based on internal similarity, GenePrint. Yang et al. [25] use additional phase offset as a new fingerprint called Tagprint for identifying a pair of readers and tags. Chen et al. explore a new fingerprint called Eingerprint [26] to authenticate passive tags in the commodity RFID system, which uses the electrical energy stored in the tag circuit as a fingerprint. Wang et al. explore a verification method called Hu-Fu [8]. The authors observe inductive coupling between two adjacent tags [27,28]. When two tags are placed very close and the coupling effect occurs, Hu-Fu can achieve the purpose of verification.

*Physiological or behavioral characteristics*. In recent years, the mainstream user authentication methods are based on different biological characteristics (e.g., fingerprint, face and retina) for identification. Compared with traditional authentication technology, the biometric authentication technology (especially fingerprint authentication) has achieved more excellent performance owing to its universality, uniqueness, permanence and anti-counterfeiting characteristics. RF-Mehndi [10] uses the physical characteristics of the tag and the biometric characteristics of the holder to verify the user's validity. When the user touches the tag, the physical layer information of the tag and the user's body impedance are combined to achieve verification.

Although RF-Mehndi combines the physical characteristics of the tags with the user's biometric information, it still cannot handle the case where the user's ID card is lost, which brings trouble to the user. Therefore, we design a system that can verify the user by combining its password with its biometric information, without the need for an ID card.

## 3. Design Background and Overview

In this section, we will introduce passive tags and how they are coupled, as well as the implementation process of our system.

### 3.1. Passive Tag

Our system uses passive tags, which do not have their own energy source, and obtain working electric energy by reflecting the carrier signals emitted by the reader [29]. An RF tag consists of an antenna and a chip. The main functions of the antenna are: (1) to receive the radio frequency signal emitted by the reader; (2) to transmit it to the chip for processing; (3) to send the chip data to the reader. The antenna is a conductor structure specially designed for coupling radiated electromagnetic energy. In general, the smaller the size of the antenna, the lower its radiation impedance and the working efficiency. Considering the above factors, the tag layout should be as small and simple as possible while still meeting the efficiency requirements. The model of the tag we use is Alien-9629, which measures 22.5 mm × 22.5 mm, and operates at 840–960 MHz.

### 3.2. Tag Coupling

Tag coupling is actually the energy transfer and information exchange between two devices. There are two ways of tag coupling: Backscatter coupling and Inductive coupling.

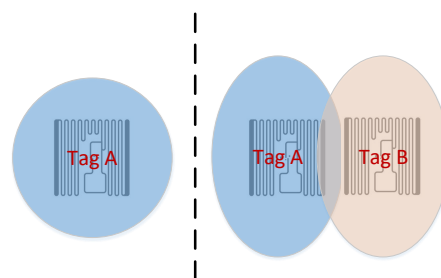
#### 3.2.1. Backscatter Coupling

After the user touches the target tag, the electromagnetic wave emitted by the antenna activates it and brings back the tag information. This process is based on the spatial propagation law of electromagnetic waves. The recognition range is greater than 1 m.

Passive tags require sustained energy from electromagnetic waves emitted by the reader to keep working. We know that a changing magnetic field creates an electric field, and a changing electric field creates a magnetic field. When magnetic flux changes, an induced current will be generated in the closed coil. The current in the signal transmitter radiates radio electromagnetic waves through the antenna, forming a changing electromagnetic field. The changing electromagnetic field is induced by the antenna coil at the receiving end, and the voltage is generated inside the coil. The tag can be thought of as a closed coil that generates an induced current inside when it senses the signal emitted by the reader. It should be noted that the induced current generated in the tag will also radiate electromagnetic waves back to the reader antenna after modulation, and generate signals that can be recognized by the reader antenna, also known as backscattered signals.

#### 3.2.2. Inductive Coupling

The inductive coupling is realized through the magnetic field of the tag according to the law of electromagnetic induction. Each tag, when activated, generates a magnetic field around its coil. When two tags are placed close to each other, their magnetic fields pass through each other's coils, resulting in a change in magnetic flux. The induced electromotive force will be generated inside the tag, thus affecting its power and signal. Figure 2 shows the state of a single tag state and the coupling state of two tags. When users touch the surface of one of the tags in the array, the tag circuit is then equivalent to adding an additional resistance, which causes the total resistance in the circuit to change and the tag power to change. Each user has a different body impedance, which makes it possible for the user to have unique biological information and to be distinguished from other users.



**Figure 2.** (Left) Single tag. (Right) Two tags are coupling.

### 3.3. System Architecture

In this part, we briefly describe the four steps for implementing the RF-Ubia system.

**Hardware Settings.** In order to realize the password function of RF-Ubia, we need to arrange nine RFID tags into a  $3 \times 3$  layout first. The tag array is then fixed to prevent signal changes caused by the relative movement of the tags from affecting the user authentication results.

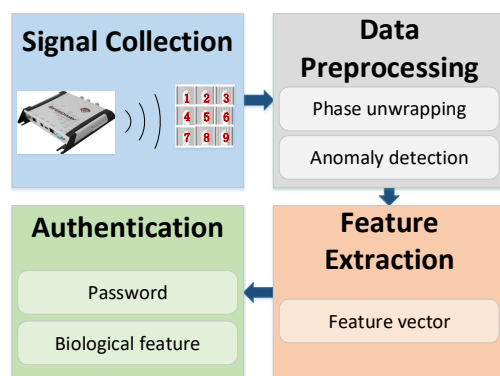
**Tag Identification.** The reader sends a signal to activate the nine tags in the array, then carries out a preliminary identification according to the EPC [30] of the tag. After the reader obtains the signal of the legitimate tag, it waits for the user to touch the corresponding tag and collects the signal data.

**Data Processing.** The purpose of this step is to process the tag data acquired by the reader to eliminate the inverted  $\pi$  phenomenon and periodic signal surround (i.e., phase unwrapping) of the tag phase. Then, we extract the characteristic information we need and identify the password sequence entered by the user.

**User Authentication.** The system first determine whether the identified password sequence is a valid password. If the password sequence entered by the user is indeed registered in the system, the second stage of verification will be performed. In the second stage, the system verifies whether the user is legitimate to prevent an illegal attacker from stealing the password sequence of the legitimate users.

## 4. System Design

In this section, we will describe the working flow of RF-Ubia in four parts, including signal collection, data preprocessing, feature extraction and authentication. Figure 3 depicts these four key steps.



**Figure 3.** Work flow of the RF-Ubia system.

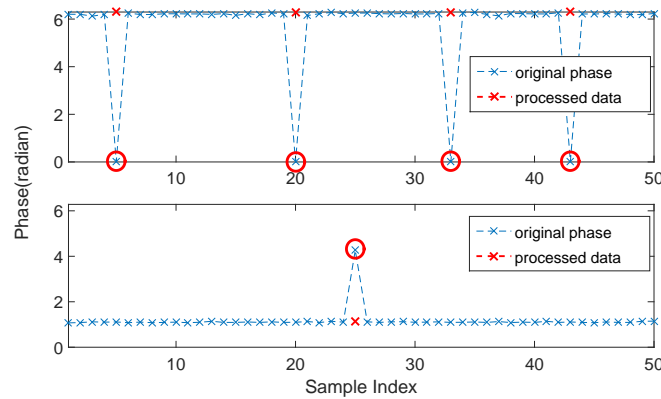
### 4.1. Signal Collection

The signal collection part of RF-Ubia is divided into registration stage and verification stage. In the registration stage, each user sets his or her password and touches the tag corresponding to the password in order. As users touch the tags multiple times, their identity information associated with their own password and body impedance is collected. Different impedance and passwords of different users make each person's identity information unique. In the verification stage, the user only needs to enter his or her password set in the registration stage, and the system back-end can obtain the relevant signal data of the tag and complete the authentication.

### 4.2. Data Preprocessing

The phase is a periodical function with the periodic signal surround and the inverted  $\pi$  phenomenon, which are the essential characteristics of the tag signal. As shown in Figure 4, the figure above shows the wrapped phase, and the figure below shows the inverted  $\pi$  phenomenon of the phase. In order to obtain usable phase characteristics, we need to

preprocess the data after getting the tag signal to obtain the tag information with the phase unwrapped and the inverted  $\pi$  phenomenon eliminated.



**Figure 4.** The 'x' symbols circled in red represent data with period wrap or phase inverted  $\pi$ , i.e. abnormal data, while the red 'x' symbols represent normal data after pre-processing. The figure above shows the wrapped phase. The figure below shows the inverted  $\pi$  phenomenon

In general, the first n data of the tag are the signal data when the tag is more stable, i.e., the tag signal without user touch interference. We select the phase average  $\theta_m$  of the first n data of the tag as the tag phase reference value. Thus, the difference between the first n phase values of the tag and the reference value, respectively,  $\Delta\theta_i = |\theta_i - \theta_m|$ , can be obtained.

We handle anomalies by setting thresholds. Since the phase of the tag fluctuates on its own and changes when touched by the user, if the threshold [3] is set too large or too small, it can lead to some data being processed incorrectly and ultimately affect the overall experimental data. We set the threshold value as

$$\begin{cases} thres_1 = \pi - thres, \\ thres_2 = \pi + thres, \end{cases} \quad \text{and} \quad \theta_i = \begin{cases} \theta_i, & \Delta\theta_i \leq thres_1 \\ (\theta_i + \pi) \bmod 2\pi, & thres_1 < \Delta\theta_i < thres_2 \\ \theta_i - 2\pi, & \theta_i - \theta_m \geq thres_2 \\ \theta_i + 2\pi, & \theta_i - \theta_m \leq -thres_2 \end{cases} \quad (1)$$

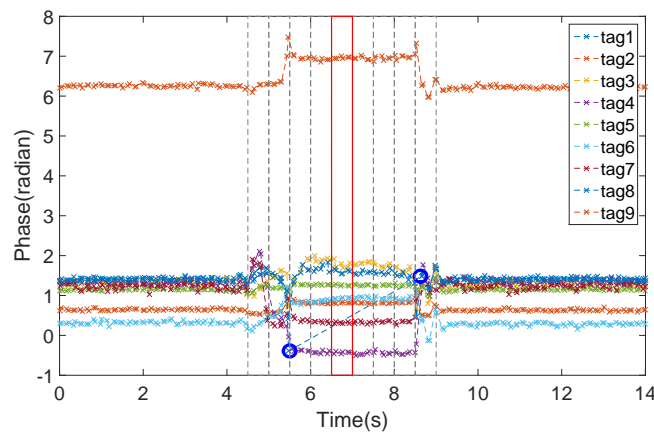
where the value of thres will be selected as the optimal value by iterative adjustment during the experiment. By comparing the difference  $\Delta\theta_i$  with the set threshold, if  $\Delta\theta_i \leq thres_1$ , then the phase is normal data; if  $thres_1 < \Delta\theta_i < thres_2$ , then it is judged to be an inverted  $\pi$  phenomenon; if  $\Delta\theta_i \geq thres_2$ , then it is judged to be the occurrence of a phase wrapping phenomenon, as shown in Equation (1).

After processing the first n stable phases of the tag, the subsequent data of the tag are processed using a sliding window. We improve and optimize the processing algorithm because the user touch operation may cause a large abrupt change in the tag phase; for example, touching the tag causes the tag phase to change beyond  $thres_1$ , which is a phase change caused by the touch operation and not an inverse  $\pi$  phenomenon or a phase wrapping phenomenon. In this case, as the user's touch has a continuous effect on the phase and the inverted  $\pi$  is an episodic phenomenon, we will use the data after this phase to make a judgment. As shown in Equation (2), the average value of this phase  $\theta_k$  and the m phases after it is taken, and if the difference between the phase value and the average

value is small compared to the threshold value  $thres_3$ , then the phase is not anomalous and does not need to be processed.

$$\left| \theta_k - \frac{\sum_{i=1}^m \theta_{k+i-1}}{m} \right| < thres_3. \tag{2}$$

When the user touches the tags in the array, we find that some of them cannot feedback the tag signal. In Figure 5, two adjacent pieces of data are connected by dashed lines. A large amount of signal data is missing between the two pieces of data surrounded by blue circles. This is because the tag power becomes relatively small due to the influence of body impedance and coupling when the user touches, so it cannot reach the threshold value for activating the tag. Therefore, the tag has no phase signal during this touch stage and the reader cannot read the tag data. We take advantage of this phenomenon as a feature when verifying the user’s identity. In order to preserve this feature, interpolation and data smoothing processing are not performed.



**Figure 5.** The dashed rectangle represents the window of abnormal phase signal, and the red rectangle represents the feature window. The line between the two blue circles indicates that these windows are more stable feature information. After phase unwrapping, some phase values will exceed the range of 0 to  $2\pi$ .

### 4.3. Feature Extraction

After data preprocessing, we obtain a continuously available tag phase signal, and further extract the phase features related to user identity information. We find that the signal changes are relatively complex and chaotic at the moment when the user touches the tag, and the phase characteristics are also unstable. However, during touch, the phase signal of the tag tends to be stable. So, we propose an anomaly detection algorithm to extract the stable part in the middle of the tag phase signal. We first empirically set up a fixed-size window to detect the abnormal part. The average amplitude in the  $k$ -th window [2] of tag  $i$  can be expressed as

$$A_i(k) = \frac{\sum_{j=1}^l |\theta_j - \theta_m|}{l} \quad \text{and} \quad \theta_m = \frac{\sum_{j=1}^l |\theta_j|}{l}, \tag{3}$$

where  $l$  represents the data volume of the phase in the window,  $\theta_j$  represents the phase value, and  $\theta_m$  represents the average phase value of the tag obtained from the stable tag signal in the first window and is used as a metric to evaluate the anomaly. In Equation (4), the amplitude function  $G(k)$  is obtained [2] by summing the amplitudes of all tags in the same window.

$$G(k) = \sum_{i=1}^9 A_i(k). \quad (4)$$

After sliding window anomaly detection and comparison with the set threshold value, an anomaly sequence can be obtained. The first exception window detected is taken as the left exception window, which is caused by the user just touching the tag. The last one in a continuous set of exception windows starting from the left exception window is taken as the right exception window, which is caused by the user's finger leaving the tag surface. We take the middle window between the left exception window and the right exception window as our feature window. The purpose is to avoid using the more unstable signal caused by the user just touching the tag, and to obtain the relatively stable signal brought by the user's continuous touch. Figure 5 shows the feature window of the tag phase signal. The mean value of the nine tag phases in this window is

$$V = [A'_1, A'_2, A'_3, A'_4, A'_5, A'_6, A'_7, A'_8, A'_9]. \quad (5)$$

Then, the phase difference between any two of the nine tags is calculated to form an eigenvalue:

$$\Delta A_{ij} = |A'_i - A'_j|. \quad (6)$$

Since  $\Delta A_{ij}$  and  $\Delta A_{ji}$  are equal, and  $\Delta A_{ii}$  is equal to 0, we can obtain 36 effective eigenvalues from a feature window to form the eigenvector

$$F = [\Delta A_{12}, \dots, \Delta A_{19}, \Delta A_{23}, \dots, \Delta A_{29}, \Delta A_{34}, \dots, \Delta A_{89}]. \quad (7)$$

#### 4.4. Authentication

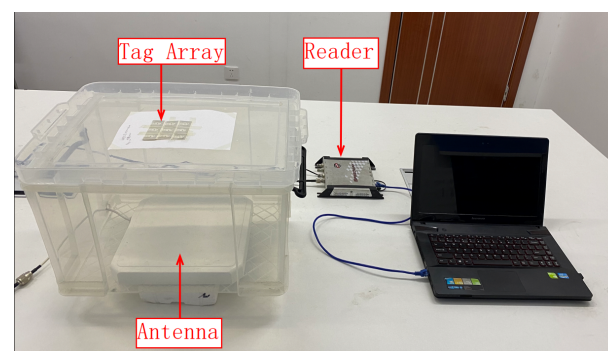
For authentication, we use the classification function in Weka to train the user information collected during the registration stage into the validation model. After collecting user data and extracting feature information, the classification model can determine whether the user is legitimate.

#### 4.5. Experiment and Evaluation

In this section, we first implement RF-Ubia, and then verify its performance through extensive experiments.

The RF-Ubia consists of a commercial reader, a directional antenna and several passive tags. The RFID reader we use is Impinj R420 commercial reader, the antenna model is Laird S9028PCR, and the tag model is Alien-9629. The software of RF-Ubia ran on a computer with an Intel(R) Core(TM) i5-3230M processor (2.60 GHz) and 12 GB RAM.

*Experimental setups.* We carry out the experiment in a conference room. As shown in Figure 6, the tag array formed by 9 Alien-9629 tags is fixed on the top of the box, and the antenna connected to the reader is placed at the bottom of the box to read the tag data. Finally, the data are processed by the computer.



**Figure 6.** Experimental environment for testing RF-Ubia system.

*Parameter Setting.* In the data preprocessing stage, we take the first 10 phases of the tag as the signal data when it is stable, and set the size of the sliding window to 6, that is,



there are six phases in the window. The sliding window size used in the anomaly detection algorithm is set to 0.5, indicating that the window contains 0.5 s of tag data. The settings for the remaining parameters in the preprocessing and exception detection algorithms are shown in Table 1.

**Table 1.** Algorithm parameter setting.

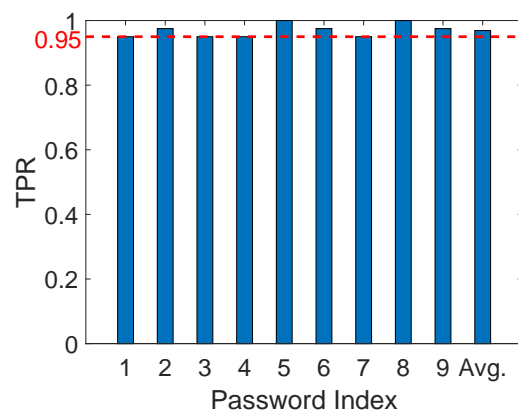
Parameter Name	Parameter Values
$thres_1$	$\pi - 1$
$thres_2$	$\pi + 1$
$thres_3$	1.5
$thres_4$	2
m	4

*Metric.* We use three major indicators to describe the performance of RF-Ubia, namely True Positive Rate (TPR), False Positive Rate (FPR) and Accuracy. TPR [4], as shown in Equation (8), is used to measure the accuracy of a single password identification performance. FPR, as shown in Equation (9), is used to measure the ratio of illegal users that pass the validation of RF-Ubia to all illegal users. Accuracy refers to the combination of the validation results, including the first stage and second stage of RF-Ubia.

$$TPR = \frac{ture\ positives}{ture\ positives + false\ negatives} \tag{8}$$

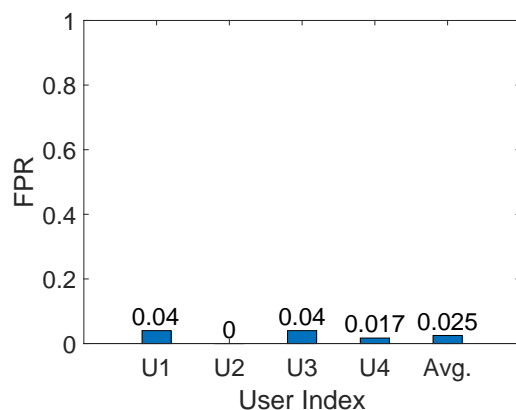
$$FPR = \frac{false\ positives}{false\ positives + ture\ negatives} \tag{9}$$

First, we evaluate the performance of the system for password identification (i.e., identifying the tags touched by the user). We collected 360 sets of data for evaluation. The TPR of each password (i.e., tag) from 1 to 9 is shown in Figure 7. The average accuracy of the system in identifying passwords exceeds 96.9%, indicating that RF-Ubia can effectively distinguish the tags touched by the user and enable the function of entering passwords.



**Figure 7.** The TPR of RF-Ubia's password identification.

We verify the validity of RF-Ubia when multiple users use the same password. As shown in Figure 8, the FPR of the RF-Ubia does not exceed 0.04 when the password length is 2, indicating that RF-Ubia can effectively distinguish different users. In addition, we also evaluate the accuracy of RF-Ubia in identifying users with the same password when the password is longer. When the password length is 3, the identification accuracy of users with the same password is 98.75%. When the password length is 4, the accuracy reaches 100%. The longer the password is, the more user features can be utilized and therefore the higher the accuracy of user identification is. Considering password identification and user differentiation, the average accuracy of RF-Ubia system exceeds 92.8%.



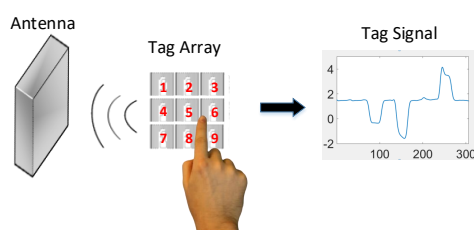
**Figure 8.** The FPR of RF-Ubia’s user validation when multiple users use the same password with a length of 2.

*Discussion.* In this section, we propose a solution that uses a fusion of user information and biometric information for user authentication, which achieves a high user identification accuracy rate even when using only a simple password. However, it has some drawbacks—we still need to use passwords, which is not friendly to people who usually forget their passwords, such as elderly people with poor memory and those who do not use the authentication system regularly. We also need to try out different experimental environments to improve the robustness of the system. In our experiments, it can be observed that RFID signals are susceptible to dynamic environmental changes (e.g., someone moving), and since the typical bandwidth of normal human finger movements is between 3 and 5 Hz, the use of low-pass filters (e.g., Butterworth filters) is possible to mitigate such effects. For other normal movements of people, they lie between 0 and 18 Hz. Therefore, we can use advanced signal processing techniques (e.g., empirical pattern decomposition) to filter out noise with overlapping frequencies.

### 5. Extension of Authentication System

In order to make up for the above shortcomings, we refine the biometric technology and propose an authentication method based on the user’s physiological and behavioral characteristics. Specifically, we authenticate users by allowing them to touch a specified sequence of tags without entering a specified password.

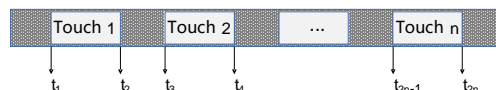
*Behavioral characteristics and time series of touch.* When the user touches a fixed tag sequence, he or she may touch it with unique habits or rhythm. As shown in Figure 9, the tag signal obtained by the user’s touch contains time information, so an anomaly detection algorithm can be used to detect the signal changes to get the fragments of the user’s touch and record the user’s touch situation at each moment. Then, the user’s touch rhythms, namely, the user’s behavioral characteristics, can be extracted using the time series of touch.



**Figure 9.** Description of the touch time schematic. The tag signal obtained from the user’s touch contains time information, recording the user’s touch at each moment.

*User Characteristic Information.* We use the physiological and behavioral characteristics of users to authenticate their identities. When the user touches the tag surface in the

specified order, the system collects information related to the user's body impedance and behavior. After extracting the phase values of the tag touched by the user, the phase difference between two tags is calculated to form the feature value. Each touch of the user generates a feature vector with a length of 36, and the phase features of all the touches form the physiological feature information of the user. In addition, the system can obtain two time values for each touch of the user, that is, the beginning and the end of each touch, as shown in Figure 10. Finally, the user's behavioral characteristic information includes four parts: the duration of each touch, the interval between each touch, the frequency of touch and the duration error of each touch corresponding to the tag.



**Figure 10.** Authentication scheme based on users' physiological and behavioral characteristics. The start and end time of each user touch on the tag can be obtained.

### 5.1. System Design

In this section, we will introduce the implementation process of the improved system, including five steps of data collection, data preprocessing, anomaly detection, feature extraction and authentication.

**Data collection.** When registering, the user needs to touch each tag in a tag sequence specified by the system in order. For example, "1379" means that the user needs to touch the four tags 1, 3, 7, and 9 in sequence. The system can collect multiple sets of data when the user touches the tag with its own habits or rhythms. In the authentication phase, the user still only needs to touch the tags according to the tag sequence. Since the tag signal can change drastically with the touch, the user should make each touch last for a short period of time so that the system can obtain relatively stable tag phase values. After collecting the user data, the system needs to perform preprocessing and anomaly detection, and further extract the characteristic information of different users, and finally perform user authentication.

**Data preprocessing.** The system needs to preprocess the raw data from the user to obtain continuous and stable tag signal. This part is consistent with the data preprocessing method used before the improvement scheme. Specifically, for each tag, the difference between its phase value and the average of the phases values of other tags around it should be calculated to distinguish whether the data are abnormal. Then, compare the value with the set threshold value to determine whether periodic signal surround or inverted  $\pi$  phenomenon occurs, and perform the corresponding data processing according to the determination result.

**Anomaly detection.** In this scheme, the label signal is detected by the sliding window. After obtaining the exception window using the previous anomaly detection algorithm, we can get the left exception window and the right exception window with fuzzy time characteristics. In the anomaly detection algorithm, if the size and moving step of the sliding window are both large, the time span of the left and right exception window is also large, so the exact time when the user touches the tag cannot be obtain. Therefore, it is necessary to further process the exception window to obtain more accurate time features.

For the left exception window  $left$ , the sum of its amplitude  $G(left)$  is larger than the threshold  $thres_4$ , while  $G(left - 1)$  is smaller than the threshold, indicating that the precise time of user touch must be between the left boundary  $(left - 1)$  of window and the right boundary  $left$  of the window. Take the beginning time of the window  $(left - 1)$  to the end time of the window  $left$  as the detection area of the exact time, and set the size and moving step of the sliding window to a smaller time granularity  $t$ , and then the average amplitude of the tag phase [2] in the window can be recalculated as

$$A'_i(k) = \frac{\sum_{j=1}^l |\theta_j - \theta_m|}{l} \quad \text{and} \quad \theta'_m = \frac{\sum_{j=1}^5 \theta_j}{5}, \tag{10}$$

where  $l$  represents the number of tag phases in the window of size  $t$ . The new amplitude function can be obtained [2] from the average amplitude of each tag in the window.

$$G'(k) = \sum_{i=1}^9 A'_i(k). \tag{11}$$

In anomaly detection, the time of the first window from left to right that detects an anomaly is taken as the precise time of the beginning of user’s touch. Similarly, for the right exception window  $right$ , when the sum of its amplitude  $G(right)$  is greater than the threshold  $thres_4$ , and  $G(right + 1)$  is less than the threshold, it means that the precise time of user touch must be between the left boundary  $right$  and the right boundary  $(right + 1)$  of the window. Take the beginning time of the window  $right$  to the end time of the window  $(right + 1)$  as the detection area of the exact time, then the time of the first window from right to left that detects an anomaly is taken as the precise time of the end of the user’s touch.

*Feature Extraction.* So far, we have obtained the tag phase value, the beginning time and the end time of each touch. Using Equations (5)–(7), we can calculate the user’s physiological characteristic information  $F_{user} = [F_{tag1}, F_{tag2}, \dots, F_{tagn}]$ . The time series of user’s multiple touches is

$$[t_1, t_2, t_3, t_4, \dots, t_{2n-1}, t_{2n}]. \tag{12}$$

Subtracting the start time from the end time of the  $K$ th touch gives the duration of the touch as

$$T_{persist}(k) = t_{2k} - t_{2k-1}. \tag{13}$$

Subtracting the start time of the  $(K + 1)$ th touch from the end time of the  $K$ th touch gives the time interval between two touches as

$$T_{interval}(k) = t_{2k+1} - t_{2k}. \tag{14}$$

We can obtain  $n$  touches,  $n$  touch duration and  $n - 1$  duration between two touches. Then, according to the total time of user touch and the number of touches, the user touch frequency can be calculated as

$$frequency = \frac{n}{t_{2n+1} - t_1}. \tag{15}$$

The user’s behavioral characteristic information is composed of the duration, time interval and the frequency of the touch. Therefore, the behavioral characteristic information can be defined as

$$F_{behavior} = [T_{persist}, T_{interval}, frequency]. \tag{16}$$

Finally, the user’s physiological and behavioral characteristic information are combined to form the user’s identification feature  $[F_{user}, F_{behavior}]$ .

*Authentication.* Our system identifies users based on their physiological and behavioral characteristics. Users do not need to remember their passwords, just touch the specified tags in order with their habits and rhythms, and the system can obtain their identity characteristics. In the registration phase, the system needs to collect multiple groups of data (at least 20 groups) as the training data for the classification model. In the authentication phase, users touch the same tag sequence, and the system extracts feature information from the user’s touch and uses the classification model to authenticate users. We use the Random Forest classifier in Weka to identify and classify user identities. For each user, there are 20 groups of data for training and 20 groups of data for testing.

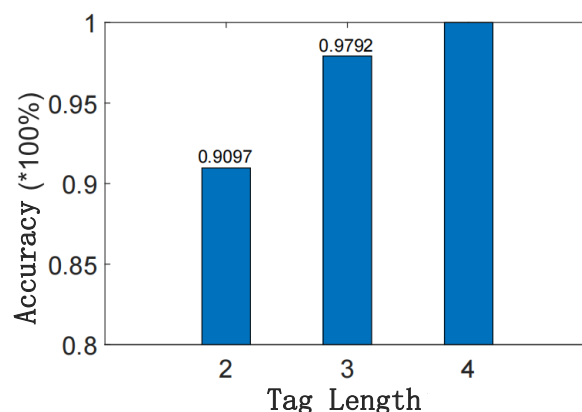
During the registration phase, users will need to collect multiple sets of data (a minimum of 20 sets) as training data for the classification model. In the authentication stage, users touch the same label order, the system collects user data and extracts feature information, and finally uses the classification model to authenticate users. User identity is identified and classified by using a Random Forest classifier in Weka. Twenty sets of data per user are used to train the classifier model and 20 sets of data are used as test samples.

## 5.2. Experiment and Evaluation

In the previous section, we describe the user's behavioral characteristics in detail and introduce how to extract it. We also improve the anomaly detection algorithm and obtain the precise time sequence of user's touches. In this section, we conduct specific experiments to verify the performance of the proposed system.

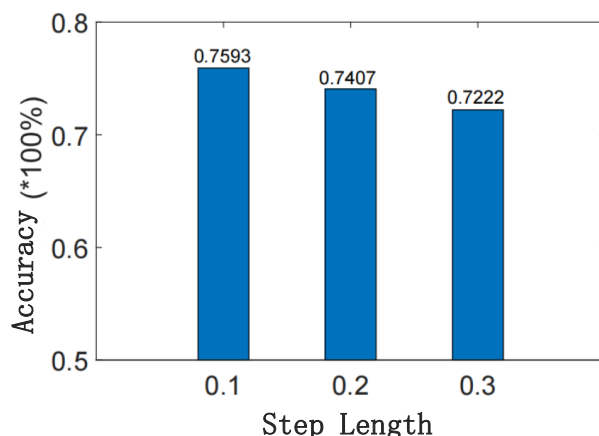
*Experimental setups.* The hardware part of the system consists of an RFID commercial reader, a directional antenna and nine passive tags. The RFID reader is an Impinj R420 commercial reader, the antenna model is Laird S9028PCR and the tag model is Alien 9629. We implemented the user interface and verification module on a Thinkpad laptop which collects data from the RFID reader through a low-level reader protocol-LLRP. The final data are processed and analyzed by a computer and MATLAB software.

*Metric.* We evaluate the impact of different lengths of the tag sequence that need to be touched on the performance of the scheme, and the lengths are set to 2, 3 and 4, respectively. In addition, with the sliding window's size is set to 0.3, we evaluate the impact of moving step size of the window on the performance. Different lengths will lead to changes in the amount of physiological and behavioral information of users. The longer the tag sequence, the more information about the user's physiological and behavioral characteristics. As shown in Figure 11, when the length is 2, the recognition rate of the system for users is 90.97%. When the length is 3, this figure increases to 97.92%. When the length is 4, this figure increases to 100%. The results show that the longer the sequence is, the more characteristic information is available, resulting in higher accuracy of user authentication.



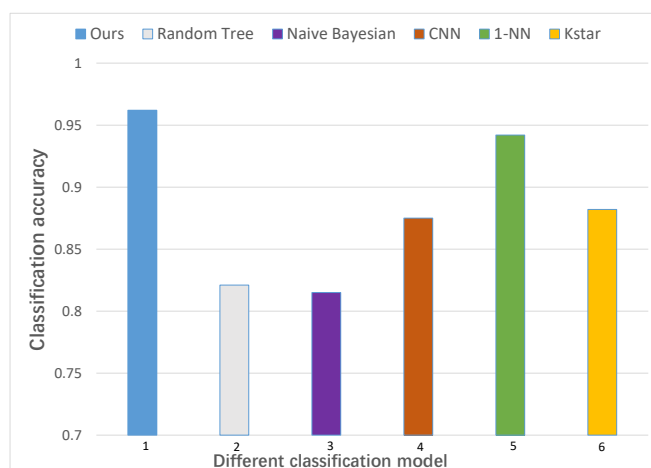
**Figure 11.** The effect of the length of the specified tag sequence on performance.

*Impact of moving step size of the sliding window.* In the anomaly detection phase, a different moving step size of the sliding window will lead to a different time accuracy of user's touch obtained by the algorithm, and different time series correspond to different behavioral characteristics of the user. Figure 12 shows the impact of different moving step size of the sliding windows on the performance of user authentication when only behavioral characteristics are used. The results show that the smaller the step size, the higher the accuracy of user authentication. A larger step size leads to poorer performance of authentication.



**Figure 12.** The effect of moving step size of the sliding window on performance.

*Impact of the classification model.* We evaluated six different classification models. To ensure fairness, we used the network structure and used the default parameter settings used in [31]. As can be seen in Figure 13, Random Forest gives the highest relative accuracy (0.959) for our RF-Ubia, and its latency is small. The rest of the classification models were relatively poor.



**Figure 13.** Performance of the system using different classification models.

*Time Overhead Evaluation.* When the user touches tags for authentication, the time overhead of the system to process the tag signal data can be divided into three parts, including data preprocessing, anomaly detection and feature extraction. When the length of the tag sequence that users need to touch is 4, it takes 0.376 s on average and 0.52 s at most to process a single data sample, and 0.52 s at most, which can satisfy people’s daily authentication needs. The time cost of our method could be lower if a computer with better hardware equipment is available or the data processing algorithm can be further improved.

*Comparison with State-of-the-art Authentication System.* To be fair, we compared the Hu-Fu authentication scheme with other authentication systems in the same experimental environment. As shown in Table 2, in the Hu-Fu [8] authentication scheme, if the authentication tag is stolen by an attacker, the attacker can pass authentication without hindrance; in the RF-Mehndi [10] scheme, although the personal card is also resistant to counterfeiting by an attacker if it is lost or stolen, the need to recreate the user card and the collection of information can still cause problems for the user. Continuous authentication schemes such as VAuth [11] and Cardiac Scan [12], on the other hand, most require the use of specialized sensors, which have significant limitations in terms of cost overhead and applicability.

**Table 2.** Comparison with the performance of different authentication systems.

	Ours	HuFu [8]	Mehndit [10]	VAAuth [11]	Cardiac [12]
<i>Cost</i>	Low	Normal	Low	Higher	Higher
<i>Anti-interference</i>	Normal	Normal	poor	Normal	poor
<i>User Friendly</i>	good	Normal	poor	Normal	good
<i>Accuracy over Time</i>	Normal	Normal	poor	good	Normal
<i>Security Performance</i>	good	Normal	Limited	Normal	Normal
<i>Applicability</i>	good	Limited	Normal	Limited	Limited
<i>Mean Accuracy</i>	93.8%	92.6%	90.6%	89.2%	91.2%

### 5.3. Discussion

We have extended the previous authentication method to incorporate the user's physiological and behavioral characteristics, allowing the user to simply touch a specified sequence of tags in sequence without using a password, where the user's touch habits and rhythm constitute their behavioral characteristics. We have improved the anomaly detection and feature extraction algorithms to more accurately find the start and end points of the action to extract accurate user touch times and improve the accuracy of the system. More experiments are needed for the selection of the classification model, and it is desirable to design an adaptive classifier model to improve the robustness of the system. Experimental results show that the proposed scheme incorporates the physiological and behavioral characteristics of the user and can identify different users with a high degree of accuracy.

### 6. Conclusions

We propose RF-Ubia, a low-cost user authentication system that utilizes commodity low-cost RFID devices to authenticate based on the user's biometric characteristics. In this work, we take into account different population groups where users can authenticate with or without passwords. We also improve the traditional sliding window anomaly detection algorithm to obtain a more accurate user touch time and compute information about the user's behavioral characteristics. We use the Random Forest classifier in Weka to identify and classify user identities, and extensive experiments show that the proposed system requires only a little training to reliably perform user authentication and detect attackers under random and mimic attacks. Comprehensive experiments have confirmed the high security and practicality of RF-Ubia, with an average accuracy rate of 94% for both authentication methods. RF-Ubia also leaves room for further research, including exploring more potential user behavior and extending more experiments to enhance authentication performance.

**Author Contributions:** Conceptualization, B.F. and N.P.; methodology, Y.H. and N.P.; Formal analysis, Y.H. and N.P.; writing—original draft preparation, Y.H. and N.P.; writing—review and editing, Y.B.; supervision and project administration, X.L. and S.Z.; funding acquisition, X.L. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported in part by the National Natural Science Foundation of China (Grant Nos. 61772559, 61602167, 62172154), the Hunan Provincial Natural Science Foundation of China under grant No. 2020JJ3016. Xuan Liu's work is partially supported by the National Defense Science and Technology Innovation Special Zone Project of China.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** All data have been present in main text.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Liu, X.; Yin, J.; Liu, Y.; Zhang, S.; Guo, S.; Wang, K. Vital Signs Monitoring with RFID: Opportunities and Challenges. *IEEE Netw.* **2019**, *33*, 126–132. [\[CrossRef\]](#)
2. Zhang, S.; Liu, X.; Liu, Y.; Ding, B.; Guo, S.; Wang, J. Accurate Respiration Monitoring for Mobile Users With Commercial RFID Devices. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 513–525. [\[CrossRef\]](#)
3. Chen, Z.; Yang, P.; Xiong, J.; Feng, Y.; Li, X. TagRay: Contactless Sensing and Tracking of Mobile Objects using COTS RFID Devices. In Proceedings of the 39th IEEE Conference on Computer Communications, INFOCOM 2020, Beijing, China, 27–30 April 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 307–316.
4. Han, J.; Ding, H.; Qian, C.; Xi, W.; Wang, Z.; Jiang, Z.; Shangguan, L.; Zhao, J. CBID: A Customer Behavior Identification System Using Passive Tags. *IEEE/ACM Trans. Netw.* **2016**, *24*, 2885–2898. [\[CrossRef\]](#)
5. Pradhan, S.; Chai, E.; Sundaresan, K.; Qiu, L.; Khojastepour, M.A.; Rangarajan, S. RIO: A Pervasive RFID-based Touch Gesture Interface. In Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking, MobiCom 2017, Snowbird, UT, USA, 16–20 October 2017; ACM: New York, NY, USA, 2017; pp. 261–274.
6. Wang, C.; Xie, L.; Wang, W.; Chen, Y.; Bu, Y.; Lu, S. RF-ECG: Heart Rate Variability Assessment Based on COTS RFID Tag Array. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2018**, *2*, 85:1–85:26. [\[CrossRef\]](#)
7. Wang, C.; Xie, L.; Zhang, K.; Wang, W.; Bu, Y.; Lu, S. Spin-Antenna: 3D Motion Tracking for Tag Array Labeled Objects via Spinning Antenna. In Proceedings of the 2019 IEEE Conference on Computer Communications, INFOCOM 2019, Paris, France, 29 April–2 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 865–873.
8. Wang, G.; Cai, H.; Qian, C.; Han, J.; Li, X.; Ding, H.; Zhao, J. Towards Replay-resilient RFID Authentication. In Proceedings of the 24th Annual International Conference on Mobile Computing and Networking, MobiCom 2018, New Delhi, India, 29 October–2 November 2018; ACM: New York, NY, USA, 2018; pp. 385–399.
9. Wang, G.; Cai, H.; Qian, C.; Han, J.; Shi, S.; Li, X.; Ding, H.; Xi, W.; Zhao, J. Hu-Fu: Replay-Resilient RFID Authentication. *IEEE/ACM Trans. Mob. Comput.* **2020**, *28*, 547–560. [\[CrossRef\]](#)
10. Zhao, C.; Li, Z.; Liu, T.; Ding, H.; Han, J.; Xi, W.; Gui, R. RF-Mehndi: A Fingertip Profiled RF Identifier. In Proceedings of the 2019 IEEE Conference on Computer Communications, INFOCOM 2019, Paris, France, 29 April–2 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1513–1521.
11. Feng, H.; Fawaz, K.; Shin, K.G. Continuous Authentication for Voice Assistants. In Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking, MobiCom 2017, Snowbird, UT, USA, 16–20 October 2017; ACM: New York, NY, USA, 2017; pp. 343–355.
12. Lin, F.; Song, C.; Zhuang, Y.; Xu, W.; Li, C.; Ren, K. Cardiac Scan: A Non-contact and Continuous Heart-based User Authentication System. In Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking, MobiHoc'17, Snowbird, UT, USA, 16–20 October 2017; ACM: New York, NY, USA, 2017; pp. 315–328.
13. Hu, B.; Zhao, T.; Wang, Y.; Cheng, J.; Howard, R.; Chen, Y.; Wan, H. BioTag: Robust RFID-based continuous user verification using physiological features from respiration. In Proceedings of the 23th International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing, MobiHoc'22, Seoul, Republic of Korea, 17–20 October 2022; ACM: New York, NY, USA, 2022; pp. 191–200.
14. Zhao, T.; Wang, Y.; Liu, J.; Chen, Y.; Cheng, J.; Yu, J. TrueHeart: Continuous Authentication on Wrist-worn Wearables Using PPG-based Biometrics. In Proceedings of the 2020 IEEE Conference on Computer Communications, INFOCOM 2020, Beijing, China, 27–30 April 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 30–39.
15. Xu, W.; Liu, J.; Zhang, S.; Zheng, Y.; Lin, F.; Han, J.; Xiao, F.; Ren, K. RFace: Anti-Spoofing Facial Authentication Using COTS RFID. In Proceedings of the 2021 IEEE Conference on Computer Communications, INFOCOM 2021, Vancouver, BC, Canada, 10–13 May 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–10.
16. Wang, Y.; Zheng, Y. TagBreathe: Monitor Breathing with Commodity RFID Systems. *IEEE Trans. Mob. Comput.* **2020**, *19*, 969–981. [\[CrossRef\]](#)
17. Li, T.; Luo, W.; Mo, Z.; Chen, S. Privacy-preserving RFID authentication based on cryptographical encoding. In Proceedings of the IEEE INFOCOM 2012, Orlando, FL, USA, 25–30 March 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 2174–2182.
18. Lu, L.; Han, J.; Xiao, R.; Liu, Y. ACTION: Breaking the Privacy Barrier for RFID Systems. In Proceedings of the INFOCOM 2009, 28th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, Rio de Janeiro, Brazil, 19–25 April 2009; IEEE: Piscataway, NJ, USA, 2009; pp. 1953–1961.
19. Sun, M.; Sakai, K.; Ku, W.; Lai, T.; Vasilakos, A.V. Private and Secure Tag Access for Large-Scale RFID Systems. *IEEE Trans. Dependable Secur. Comput.* **2016**, *13*, 657–671. [\[CrossRef\]](#)
20. Weis, S.A.; Sarma, S.E.; Rivest, R.L.; Engels, D.W. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In *Security in Pervasive Computing*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2802, pp. 201–212.
21. Yao, Q.; Qi, Y.; Han, J.; Zhao, J.; Li, X.; Liu, Y. Randomizing RFID Private Authentication. In Proceedings of the Seventh Annual IEEE International Conference on Pervasive Computing and Communications, PerCom 2009, Galveston, TX, USA, 9–13 March 2009; IEEE Computer Society: Washington, DC, USA, 2009; pp. 1–10.



22. Ding, H.; Han, J.; Zhang, Y.; Xiao, F.; Xi, W.; Wang, G.; Jiang, Z. Preventing Unauthorized Access on Passive Tags. In Proceedings of the 2018 IEEE Conference on Computer Communications, INFOCOM 2018, Honolulu, HI, USA, 16–19 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1115–1123.
23. Ding, H.; Han, J.; Zhao, C.; Wang, G.; Xi, W.; Jiang, Z.; Zhao, J. Arbitrator2.0: Preventing Unauthorized Access on Passive Tags. *IEEE Trans. Mob. Comput.* **2022**, *21*, 835–848. [[CrossRef](#)]
24. Han, J.; Qian, C.; Yang, P.; Ma, D.; Jiang, Z.; Xi, W.; Zhao, J. GenePrint: Generic and Accurate Physical-Layer Identification for UHF RFID Tags. *IEEE/ACM Trans. Netw.* **2016**, *24*, 846–858. [[CrossRef](#)]
25. Yang, L.; Peng, P.; Dang, F.; Wang, C.; Li, X.; Liu, Y. Anti-counterfeiting via federated RFID tags' fingerprints and geometric relationships. In Proceedings of the 2015 IEEE Conference on Computer Communications, INFOCOM 2015, Hong Kong, China, 26 April–1 May 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1966–1974.
26. Chen, X.; Liu, J.; Wang, X.; Liu, H.; Jiang, D.; Chen, L. Eingerprint: Robust Energy-related Fingerprinting for Passive RFID Tags. In Proceedings of the 17th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2020, Santa Clara, CA, USA, 25–27 February 2020; USENIX Association: Berkeley, CA, USA, 2020; pp. 1101–1113.
27. Han, J.; Qian, C.; Wang, X.; Ma, D.; Zhao, J.; Xi, W.; Jiang, Z.; Wang, Z. Twins: Device-Free Object Tracking Using Passive Tags. *IEEE/ACM Trans. Netw.* **2016**, *24*, 1605–1617. [[CrossRef](#)]
28. Yang, L.; Chen, Y.; Li, X.; Xiao, C.; Li, M.; Liu, Y. Tagoram: Real-time tracking of mobile RFID tags to high precision using COTS devices. In Proceedings of the 20th Annual International Conference on Mobile Computing and Networking, MobiCom'14, Maui, HI, USA, 7–11 September 2014; ACM: New York, NY, USA, 2014; pp. 237–248.
29. Xi, Z.; Liu, X.; Luo, J.; Zhang, S.; Guo, S. Fast and Reliable Dynamic Tag Estimation in Large-Scale RFID Systems. *IEEE Internet Things J.* **2021**, *8*, 1651–1661. [[CrossRef](#)]
30. Liu, X.; Zhang, S.; Xiao, B.; Bu, K. Flexible and Time-Efficient Tag Scanning with Handheld Readers. *IEEE Trans. Mob. Comput.* **2016**, *15*, 840–852. [[CrossRef](#)]
31. Zou, Y.; Xiao, J.; Han, J.; Wu, K.; Li, Y.; Ni, L.M. GRfid: A device-free RFID-based gesture recognition system. *IEEE Trans. Mob. Comput.* **2017**, *16*, 381–393. [[CrossRef](#)]