Usable Identity and Access Management Schemes for Smart Cities

Preprint · September 2022

DOI: 10.13140/RG.2.2.24407.75683

2 authors:

Sandeep Gupta
Università degli Studi di Trento
62 PUBLICATIONS **384** CITATIONS
SEE PROFILE

Bruno Crispo
Università degli Studi di Trento
306 PUBLICATIONS **6,600** CITATIONS
SEE PROFILE

Usable Identity and Access Management Schemes for Smart Cities

Sandeep Gupta and Bruno Crispo

Abstract Usable Identity and Access Management (IAM) schemes are highly required to control and track users' identity and access privileges for a safe and secure smart city. Any safety or security breach in critical infrastructures, e.g., smart financial solutions, smart transportation, and smart buildings, can disrupt the normal life of its residents. Studies have reported that traditional knowledge- and token-based IAM schemes are unable to fully secure these emerging use cases due to inherent security and usability issues in them. This chapter presents multi-modal biometric-based IAM schemes for smart payment apps, smart transportation, and smart buildings that can partially address the safety and security concerns of residents. We also describe the framework for designing risk-based, implicit, or continuous verification IAM schemes for such use cases.

Key words: Identity and Access Management, Biometrics, Smart financial solutions, Smart transportation, Smart buildings, Smart city

1 Introduction

The success of a "smart city" extensively depends on smarter and secure cyber-physical systems (CPS) for improving people's quality of life. Among various CPS, smart financial solutions, smart transportation, and smart buildings are some of the most important for the sustainability of smart cities. However, any security breach in these strategic solutions could pose considerable risks to the prospects of smart cities.

Sandeep Gupta
Department of Information Engineering & Computer Science (DISI),
University of Trento, Italy, e-mail: sandeep.gupta@ex-staff.unitn.it

Bruno Crispo
Department of Information Engineering & Computer Science (DISI),
University of Trento, Italy e-mail: bruno.crispo@unitn.it

Verizon's Data Breach Investigations Report (DBIR) [34] analyzed 29,207 real-world security incidents, claiming that 85% of breaches involved a human element, which is a pernicious trend. DBIR further reported that the top three breaches were social engineering (35%), basic web application attacks (24%), and system intrusion (18%).

Clearly, traditional knowledge- and token-based identity and access management schemes are not highly effective to secure emerging CPS [20, 37]. Impersonation-, observation- and brute force-attacks can easily exploit traditional verification mechanisms [13, 23]. Nonetheless, weak passwords remain the major cause of botnet-based attacks like Mirai resulting in Denial of Services (DoS) of CPS [24, 3]. Also, these traditional mechanisms have shown the inability to fulfill the usability requirements of the end-users [6, 33]. Therefore, a thorough investigation for usable identity and access management schemes that can secure smart cities and the underlying smart CPS is inevitable.

This chapter discusses biometric-based IAM schemes [14] for smart payment apps, smart transportation, and smart buildings. In addition to securing critical services, we take this opportunity to reify a safer and more secure smart city. The main contributions of this chapter are as follows.

1. Examples of multi-modal biometric-based IAM schemes for smart payment apps, smart transportation, and smart buildings to address the safety and security concerns of smart city residents.
2. Framework for designing risk-based, implicit, or continuous verification IAM schemes.

The rest of the chapter is organized as follows: Section 2 covers the drawbacks in traditional verification schemes and presents the building blocks of a biometric-based identity and access mechanism. Section 4 presents HOLD & TAP user verification scheme for smart payment apps. Section 5 presents DRIVERAUTH risk-based user verification schemes for smart transportation such as on-demand rides strengthening the security and safety of their customers. Section 6 presents STEP & TURN a secure and usable user verification scheme for cyber-physical space to secure access to their authorized users. Finally, section 8 concludes the chapter.

2 Background

The term "smart city" typically connotes an interplay of cyber-physical systems orchestrating smart financial solutions, smart transportation, smart buildings, etc., to deliver the residents a better quality of life. However, considering the substantial increase in security incidents [34], it becomes imperative to redesign IAM schemes that rely on traditional verification mechanisms by introducing biometrics for a secure and safer smart city [30].

2.1 Drawbacks in Traditional Verification Schemes

The biggest drawback of IAM schemes employing traditional verification schemes like personal identification numbers (PINs), passwords, or access cards is that they can give access to anyone knowing the PIN/password or having a genuine access card. Studies have shown that PINs and passwords can be easily guessed, shared, cloned, or stolen [23, 9]. Binbeshr et al. [5] described that PIN-entry methods are highly susceptible to observation attacks. The adversary can observe the login PIN directly or use a recording tool to gain illegitimate access later. Moreover, adversaries can exploit default usernames and passwords of IoT devices for installing botnets or worms to carry out DoS/DDoS attacks on CPS [25, 12].

Traditional verification schemes can also be an easy victim of phishing, impersonation, or insider attacks where the impostor misuses the information of legitimate users to reset the user pin/password or to get a duplicate access card [13, 28, 1]. Nevertheless, with the availability of enormous computation resources, brutal-force attacks can try a large number of users' identity-related information to generate different PINs/passwords, thus, to gain access to CPS [10]. To overcome such shortcomings, the system enforces stringent password policies (e.g., must have uppercase and lowercase letters and special characters), however, that adversely affect the usability of IAM schemes [37].

Service providers adopted two-factor verification, e.g., username/ password and one-time-passcodes (OTP), to strengthen the security of their online security-sensitive solutions. This further deteriorates the usability because the users are compulsorily required to manage additional hardware to access the services. Moreover, the idea of enhancing security with multi-factor verification perishes too due to side-channel attacks, e.g., MITM (Man-in-the-Middle), and MITPC/Phone (Man-in-the-PC/Phone) [8]. Overall, usability issues such as cognitive load, form-factor, additional hardware, etc., make traditional identity and access systems unsuitable for emerging use-cases.

Zhang et al. [36] presented a study on security and privacy issues that included privacy leakage, secure information processing, and dependability in control. The author emphasizes that any unauthorized access to urban public facilities in a smart city must be prevented. Consequently, IAM schemes require rethinking, with biometrics providing an appropriate alternative to overcoming the drawbacks present in traditional verification schemes.

2.2 Biometric-based Identity and Access System

Figure 1 shows the basic building blocks of a biometric-based identity and access system that primarily consists of five modules: 1) data acquisition module, 2) data processing module, 3) features processing module, 4) database module, and 5) classification module. The ISO standard:24741 [19] specified the term biometrics or

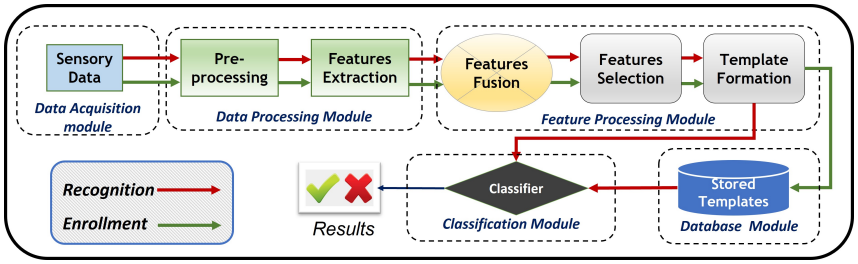

Fig. 1 Biometric-based Identity and Access System

biometric recognition as "*the automated recognition of individuals based on their biological and behavioral characteristics*."

1. **Data Acquisition Module:** This module consists of sensors that acquire one or more biometric traits of an individual. It is desired that the measured biometric traits are both distinctive between individuals and repeatable over time for the same individual. This module can also be referred to as a data collection module.

2. **Data Processing Module:** This module preprocesses the acquired data and subsequently, extracts the features from the processed data. Table 1 presents some of the common data preprocessing techniques to convert raw sensory data into an understandable format.

Table 1 Data preprocessing techniques

#	Technique	Description
1.	Data cleaning	Fill in missing values, smooth noisy data, identify or remove outlier, and resolve inconsistencies
2.	Data integration	Integration of data from multiple sensors
3.	Data transformation	Normalization and aggregation of sensor data
4.	Data reduction	Obtains reduced representation in volume but produces the same or similar analytical results
5.	Data discretization	A part of data reduction but with particular importance, especially for numerical data

3. **Features Processing Module:** In this module, the extracted features are fused and selected for the generation of a user biometric template. Biometric traits may be acquired separately or simultaneously and they are processed as per the fusion model used.

4. **Database Module:** Database module stores the users' biometric template generated during the enrollment process.

5. **Classification Module:** Classification module compares the input query and stored biometric template of an individual to accept or reject the claimed identity.

Ten et al. [32] stated that access to critical CPS should be validated through the biometric trait of an individual. Furthermore, Ross et al. [30] elaborated that smart cities have a nexus of interconnected IoT devices that require human-machine and machine-machine interaction. Human-machine interaction can be secured via biometric verification to provide personalized services as well as to ensure residents' safety.

3 Problem Description

This section analyzes the potential threats to CPS facilitating smart financial solutions, smart transportation, and smart buildings. The main purpose of IAM schemes is verification, authorization, administration of identities, and audit. Thus, IAM schemes should ensure an appropriate level of security for these strategic solutions while simultaneously keeping schemes usable for end-users and administrators.

3.1 Smart Financial Solutions

A cashless environment for smart cities as an alternative to paper money can bring manyfold benefits to residents. It can provide hassle-free money transfers, bring down crimes like mugging, and even can restrict the spread of viruses in pandemic-like situations. Thus, smartphone-based payment apps like *Apple Pay Cash*, *Alipay*, *Google Pay*, *PayPal*, and *Samsung Pay* can be deemed essential for providing smart financial solutions.

Considering physical attacks, where (i) the adversary accidentally finds an unlocked smartphone, (ii) the adversary is a friend or colleague (who possibly knows the user's PIN/Passwords), and (iii) the adversary records users while they interact with their smart devices. Eventually, the adversary exploits the weaknesses of PIN/password-based verification schemes to gain access to users' smart payment apps.

Prior studies [31, 29] also demonstrated that the aforementioned scenarios are quite apparent, as users use their smart devices at commons places like offices, homes, meeting rooms, or streets, which may give opportunities to adversaries to target their smart devices, easily. As a consequence, smartphone users can be a victim of monetary fraud, identity thefts, or similar unfavorable incidents.

3.2 Smart Transportation

With the goals set for minimum congestion, accident-free travel, and safety of residents, smart transport is another important aspect towards the realization of smart

cities. Unarguably, on-demand ride and ride-sharing services have revolutionized the point-to-point transportation market. Customers can book these rides services on short notice with 24×7 availability in all major cities across the world.

However, the reliability of drivers has emerged as a critical problem, and as a consequence, issues related to riders' safety and security have started surfacing. News related to fake drivers and assaults by dishonest drivers is a severe safety and security risk for the riders [35]. Further, being a lucrative business and easy to start, on-demand rides and ride-sharing services are attracting people also with unclean police records to become driver-partners using false identities [4]. Eventually, there can be two types of malicious users: the first type of adversary can impersonate a driver-partner by imitating a legitimate driver. The second type of attacker colludes with a legitimate driver-partner and share with him/her the registration to provide rides on behalf of the legitimate driver.

3.3 Smart Buildings

In today's rapidly evolving smart cities, frictionless and smooth interactions for smart buildings are emerging as critical a requirement. Such requirements need to coexist with mandatory properties like physical security. Consequently, smart buildings require some form of physical access control (i.e., locks, doors, barriers, etc.) that must be both reliable and usable for the users [22]. Any unauthorized access to smart buildings maintaining public utilities, e.g., healthcare, electricity, water, or gas, can disrupt the day-to-day life in a smart city.

4 IAM scheme for Smart Financial Solutions

We design a bimodal behavioral biometric-based one-shot-cum-continuous user verification scheme that authenticates users based on *how* they enter the text instead of *what* they enter, thus strengthening `username/password`-based schemes used in smartphone-based payment apps without incurring additional cost to the smart financial solution providers.

HOLD & TAP [7] strengthens the widely used PIN/password-based verification technology by giving flexibility to users to enter any random 8-digit alphanumeric text and authenticates users based on their invisible tap-timings and hand-movements, instead of pre-configured PIN or Passwords. Moreover, the entire user session is *continuously* safeguarded by assessing risk. Thus, HOLD & TAP, not only authenticates users during the application sign-in process but also, throughout the entire active user session.

Figure 2 illustrates the framework of our one-shot-cum-continuous verification scheme explaining how it addresses security and usability issues in existing `user/password`-based, and 2-factor verification schemes. The scheme enables users

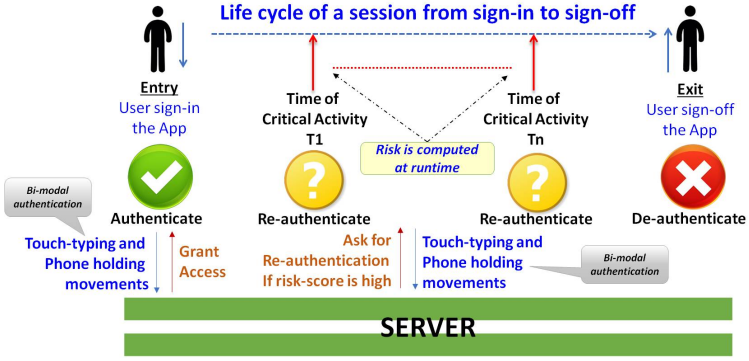

Fig. 2 HOLD & TAP verification scheme framework.

to enter any random 8 – *digit* alphanumeric text to access the application to enhance the usability of existing PIN/Password-based one-shot verification schemes. Consequently, the users' identities are verified based on timing differences between the entered keystrokes and their hand-movement in 3-dimensional space instead of just a binary comparison, to enhance security. After the successful sign-in, the scheme *continuously* monitors client attributes and computes the risk-score at the instant users initiate critical activities. Based on the risk-score, it permits users to perform that activity, otherwise, the scheme prompts for re-verification.

We extract 30 touch-typing features from the 8-digit *random-text* entry using touchscreen sensor. Figure 3 shows touch-typing features that consist of 8 *Type0* (timing difference between each key release and key press), 7 *Type1* (timing difference a key press and previous key release, 7 *Type2* (timing difference two successive keys release), 7 *Type3* (timing difference two successive keys press), and 1 *Type4* (timing difference between last and first key press).

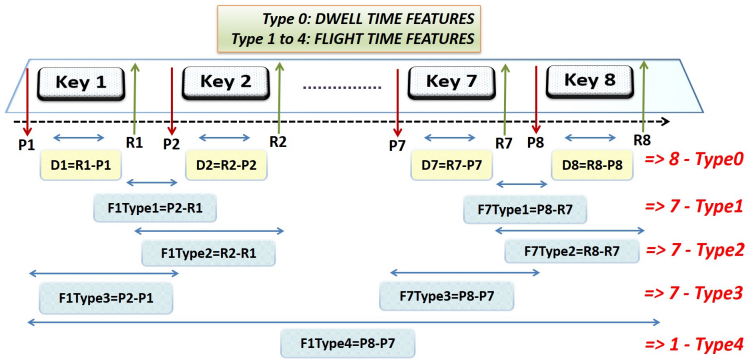

Fig. 3 Touch-typing features for 8-keys entry.

A user's hand-movement signature is constructed from 4 raw data streams obtained from each of the seven motion sensors (*i.e., the accelerometer, the high-pass sensor, the low-pass sensor, the orientation sensor, the gravity sensor, the gyroscope, and the magnetometer*) with the delay set at SENSOR_DELAY_GAME [2]. The 4 raw data streams are `X`, `Y` and `Z`, and `M`. However, `M` (Magnitude) is computed mathematically using Equation $Value_M = \sqrt{(Value_x^2 + Value_y^2 + Value_z^2)}$. Where, $Value_M$ is the Magnitude and $Value_x$, $Value_y$ and $Value_z$ are the values of `X`, `Y` and `Z` value of a sensor, at a time t. From each raw data stream, 4 statistical features, namely Mean (μ), Standard Deviation (σ), Skewness (s), and Kurtosis (k), are extracted that gives 16 statistical features per sensor as shown in Table 2. Overall, we extracted 112 hand-movements features from seven sensors.

Table 2 Statistical features per sensor for a hand-movement behavior.

No.	Hand-movement Features			
1-4	μ_X	μ_Y	μ_Z	μ_M
5-8	σ_X	σ_Y	σ_Z	σ_M
9-12	s_X	s_Y	s_Z	s_M
13-16	k_X	k_Y	k_Z	k_M

Finally, we concatenate 30 touch-stroke features and 112 hand-movements features to create a feature vector of size 142. Here, we prefer to choose the feature level fusion over the sensor level fusion because sensory data could have inconsistent and/or unusable data that may affect classifiers' accuracy [27]. Thus, HOLD & TAP [7] provides a multiclass classification based on users' two behavioral biometric modalities to secure smart payment apps throughout the life-cycle of a typical user session.

5 IAM scheme for Smart Transportation

DRIVERAUTH [15] is a risk-based multi-modal verification scheme that exploits three biometric modalities, i.e., swipe gestures, *text-independent* voice and face, to make the on-demand ride and ride-sharing services secure and safer for their customers. DRIVERAUTH enrolls the drivers at the time of registration and verifies every time a new ride-assignment is given to them. Each smart transportation provider has its dedicated system and application for its driver-partners, however, the core functionalities are the same. Thus, DRIVERAUTH can easily be integrated into these systems and provide the required safety and security to customers.

Figure 4 explains the framework of DRIVERAUTH. A person intended to work as a driver-partner is registered to the system at the time of $Entry$, i.e., the person's biometric traits are acquired and added to the database for a reliable $1 - to - 1$ verification. According to ISO 9000:2015 [18], *risk* is the "effect of uncertainty on objectives". Here, a service provider accepting a driver-partner's ride request ($T_1 ... T_n$)

can be considered as a critical activity. Therefore, verification of driver-partner to mitigate a potential risk must be performed. At the time of $Exit$, the driver-partner's biometric traits are deleted from the system and no more allowed to accept ride assignments.

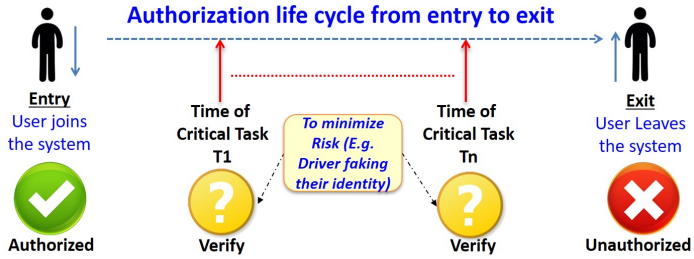

Fig. 4 DRIVERAUTH verification mechanism framework.

The driver-partner swipe's gesture, i.e., a sequence of touch-events, is collected and encoded as an input sequence of finite length (n). Each sequence contains several attributes like time-stamp of the touch event (t_n), x-and y-coordinate of the touch point (x_n, y_n), pressure calculating how hard the finger was pressed on the screen (p_n), and size of touch area (s_n). We process the collected sequences and extract 33 features as listed in Table 3.

Table 3 List of swipe features.

No.	Swipe Features			
1-4	Duration	Average event size	Event size down	Pressure down
5-8	Start X	Start Y	End X	End Y
9-12	Velocity X Min	Velocity X Max	Velocity X Average	Velocity X STD
13-16	Velocity X VAR	Velocity Y Min	Velocity Y Max	Velocity Y Average
17-20	Velocity Y STD	Velocity Y VAR	Acceleration X MIN	Acceleration X Max
21-24	Acceleration X AVG	Acceleration X STD	Acceleration X VAR	Acceleration Y MIN
25-28	Acceleration Y Max	Acceleration Y AVG	Acceleration Y STD	Acceleration Y VAR
29-32	Pressure Min	Pressure Max	Pressure AVG	Pressure STD
33	Pressure VAR	-	-	-

We acquire a two-second voiceprint of the driver-partner that contains 2 channels sampled at 44100 Hz with 16 bits per sample. The signal is first filtered using a band-pass filter to improve the signal-to-noise ratio. Then, we computed Mel Frequency Cepstral Coefficients (MFCC) from these filtered voice signals that are analogous to filters (vocal tract) in the source-filter model of speech. Figure 5 illustrates the MFCCs computation process. The scaling of the frequency axis to the non-linear Mel scale (using triangular overlapping windows) is done after applying the Fourier transform on a window of the voice signal. After that, a Discrete Cosine Transform (DCT) is performed on the log of the power spectrum of each Mel band. The

MFCCs are the amplitudes of the resulting spectrum, which is a $2-D$ vector of size $13 \times variable\ length$ (the length of vector depends on the voice signal duration).

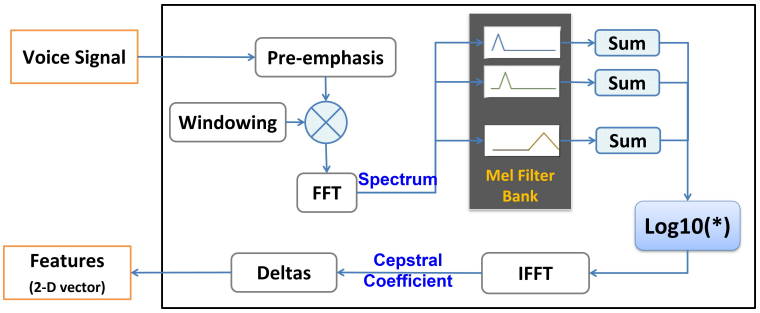

Fig. 5 Voice features: MFCC computation process.

We compute 4 statistical features, namely mean, standard deviation, kurtosis, and skewness, from a 2-D MFCC vector. Thus, the total 8 statistical features each of size 1×13 are generated from each left and the right voice channel. Finally, these 8 vectors of size 1×13 are concatenated to form a single $1-D$ feature vector of dimension 1×104.

Binarized Statistical Image Features (BSIF) extraction process for a face image is illustrated in Figure 6. First, the driver-partner face image is cropped to extract the region of interest (ROI). After that, each image is converted into an 8-bit grayscale format for obtaining statistical features using a BSIF filter bank [21]. Given an image

Fig. 6 BSIF features extraction process [26]

patch X of size $l \times l$ pixels and a filter W of size $n \times n$ pixels, where n is less than l. The filter response s_i can be obtained using Equation $s_i = X[l,l] * W[n,n]$. We extract 256 features per image using a filter of size 3×3 with 8 bits word-length. BSIF filter applies learning, instead of manual tuning, to compute a statistically meaningful representation of an image.

DriverAuth provides multi-model biometric-based user verification for proactive verification of driver-partners before allocating new ride assignments to them, thus, making smart transportation like on-demand ride and ride-sharing services safer and secure.

6 IAM scheme for Smart Buildings

Step & Turn [17] is a bimodal behavioral biometric-based verification system that utilizes two natural human actions, i.e., single footstep and hand-movement, to secure access to smart buildings. Step & Turn exploits *single footstep* and *hand-movement* behavioral biometric for securing smart buildings. Both the footstep and hand-movement modalities do not require explicit users' cooperation and can be collected unobtrusively.

The door handle is fitted with three motion sensors that are accelerometer, gyroscope, and magnetometer. To model a user's hand-movement trajectory in 3-D space, `X`, `Y`, and `Z` data streams are acquired from the three sensors at the sampling of 50 Hz and `M` is derived mathematically. Subsequently, 6 independent univariate statistical features, namely, minimum (Min), maximum (Max), mean (μ), standard deviation (σ), kurtosis (k), and skewness (s) are computed from each data-stream using Equation 1.

$$\begin{aligned} Min &= \min_{n=1}^{S} D_n & Max &= \max_{n=1}^{S} D_n \\ \mu &= \frac{1}{S}\sum_{n=1}^{S} D_n & \sigma &= \sqrt{\frac{\sum_{n=1}^{S}(D_i - \mu)}{S}} \\ k &= \frac{\frac{1}{S}\sum_{n=1}^{S}(D_n - \mu)^4}{\sigma^4} & s &= \frac{\frac{1}{S}\sum_{n=1}^{S}(D_n - \mu)^3}{\sigma^3} \end{aligned} \tag{1}$$

Where, S_i is the i^{th} sample in a data-stream. N is the number of samples in a data-stream. Min and Max are the minimum and maximum values respectively, in a given data-stream. Mean (μ) is the average of all samples. Standard deviation (σ) is the square root of the variance. Kurtosis (k) measures the degree of peakedness of a data-stream that helps in detecting the outlier-proneness of the distribution. Skewness (s) measures the degree of asymmetry of a data-stream from its mean value. We extract 6 statistical features from each data-stream. As there are 4 data-streams per sensor so 24 (4×6) features are obtained per sensor. Thus, with 3 sensors, a total of 72 ($3 \times 4 \times 6$) statistical features are extracted. The final feature vector for hand-movement consists of 73 features in total including 72 statistical features and handle-movement action time

Footstep pressure-data acquisition system consists of 88 high-density piezoelectric sensors to acquire the footstep data. After that, each pressure amplitude array of size 88×2200 into 4-independent time-series arrays, namely, Spatial Average (S_{ave}), Ground Reaction Force ($GRF_{cumulative}$), Upper (S_{upper}) and Lower (S_{lower}) Contours of size 1×2200 each [11], using Equation 2.

$$S_{ave}[t] = \sum_{i=1}^{N} S_i[t] \qquad GRF_{cumulative}[t] = \sum_{t=1}^{T_{max}} S_{ave}[t]$$
$$S_{upper}[t] = \max_{i=1}^{N} S_i[t] \qquad S_{lower}[t] = \min_{i=1}^{N} S_i[t] \tag{2}$$

Where, $S_i[t]$ is the differential pressure sample from the i^{th} piezoelectric sensors at the time t. N is the total number of piezoelectric sensors, i.e., 88. Then, 6 statistical features are computed from each time-series array by using Equation 1. In total, we get 48 statistical features (8×6) from 8 time-series arrays that were obtained from both left and right pressure amplitude arrays.

Ground Reaction Force (GRF_i) per sensor is computed by accumulating each sensor pressure amplitude from time T_1 to T_{max} by using 3.

$$GRF_i = \sum_{t=1}^{T_{max}} S_i[t] \tag{3}$$

Where, $S_i[t]$ is the differential pressure sample from the i^{th} piezoelectric sensors with i ranges from 1 to 88 and t ranges from 1 to 2200. In total, 176 features are obtained from both left and right pressure amplitude arrays.

Overall, Step & Turn leverages 297 features extracted for hand-movement and footstep behavioral modalities to provide a multi-class classification solution for securing access to smart buildings.

7 Challenges and Limitations

In this section, we discuss challenges and limitations that can adversely affect CIA principles, i.e., confidentiality (*ensuring access to legitimate users only*), integrity (*guaranteeing modification by legitimate users*), and availability (*ensuring uninterrupted availability to legitimate users*) for designing biometric-based IAM schemes.

- Security analysis of biometric-based IAM schemes can be a challenging task, therefore, a thorough testing strategy must be developed for mitigation of vulnerability-detection, intra-class variance, and common attacks (e.g., malware, mimics, impersonation, spoofing, replay, statistical, algorithmic, and robotics attacks).
- Factors like aging, fatigue, illness, injury, mood, stress, or sleep deprivation, may impede the effectiveness of biometrics. These factors require in-depth investigation to support the development of biometric-based IAM schemes.
- Behavioral biometrics datasets must consider all demographics covering different age groups, cultural factors, and ethnicity to provide better objectivity. More-

over, standards for behavioral biometrics and benchmarking of sensors must be developed and utilized.

- Quality control of the biometric template is a prerequisite before the enrollment or verification/identification phase. It can support the accuracy, stability, redundancy, and speed of IAM schemes to address problems arising from the environment, sensors, or the users themselves.
- Several privacy regulation laws such as General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Health Insurance Portability and Accountability Act (HIPAA) described biometric mandated an increase in responsibility and transparency for using and storing personal data [16]. Therefore, adequate measures like template protection and local template storage must be employed for complying with privacy laws.
- Ethical conduct in the use of behavioral biometrics is another important aspect that needs to be addressed carefully. For instance, acquiring and accumulating behavioral biometric data over time can lead to dynamic behavior profiling of an individual, providing insight into how the individual behaved in a certain context. This can be more problematic if behavioral biometric data is combined with soft biometrics, such as age, gender, height, weight, and ethnicity, to generate an individual's profile that can aggregate ethical risks.

8 Conclusions

Usable security emerged as a substantial requirement for a secure and safe smart city. We presented some next-generation biometric-based IAM schemes, namely, Hold & Tap, DriverAuth, and Step & Turn for smart financial solutions, smart transportation, and smart buildings, respectively. Hold & Tap can provide a pleasant and satisfying user experience by giving the flexibility to enter random alphanumeric text to access security-sensitive applications. Internally, users' invisible tap-timings and hand-movements are exploited to secure access to smart financial solutions. DriverAuth can contribute to preventing unforeseen incidents to secure smart transportation by implementing risk-based multi-modal biometric-based. It proactively verifies driver-partners before new ride assignments are allocated to them. Lastly, Step & Turn is a bimodal behavioral biometric-based verification system that can offer an easy access mechanism to secure smart buildings.

References

1. Aldawood, H., Skinner, G.: Educating and raising awareness on cyber security social engineering: A literature review. In: Proceedings of the IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), pp. 62–68. IEEE (2018)

2. Android: Motion sensors. https://developer.android.com/guide/topics/sensors/sensors_motion (*Accessed on 20-02-2022*)
3. Antonakakis, M.: Understanding the mirai botnet. In: Proceedings of the 26th USENIX Security Symposium), pp. 1093–1110 (2017)
4. BBC: Uber driver background checks not good enough. http://www.bbc.com/news/technology-34002051 (2015 *(Accessed on 20-02-2022)*). Online web resource
5. Binbeshr, F., Kiah, M.M., Por, L.Y., Zaidan, A.A.: A systematic review of pin-entry methods resistant to shoulder-surfing attacks. computers & security **101**, 102116 (2021)
6. Braz, C., Seffah, A., Naqvi, B.: Integrating a usable security protocol into user authentication services design process (2018)
7. Buriro, A., Gupta, S., Yautsiukhin, A., Crispo, B.: Risk-driven behavioral biometric-based one-shot-cum-continuous user authentication scheme. Journal of Signal Processing Systems (2021)
8. Choi, H., Kwon, H., Hur, J.: A secure otp algorithm using a smartphone application. In: Proceedings of the 7th International Conference on Ubiquitous and Future Networks, pp. 476–481. IEEE (2015)
9. Dasgupta, D., Roy, A., Nag, A., et al.: Advances in user authentication (2017)
10. Dilraj, M., Nimmy, K., Sankaran, S.: Towards behavioral profiling based anomaly detection for smart homes. In: Proceedings of the TENCON 2019-2019 IEEE Region 10 Conference (TENCON), pp. 1258–1263. IEEE (2019)
11. Edwards, M., Xie, X.: Footstep pressure signal analysis for human identification. In: Proceedings of the 7th International Conference on Biomedical Engineering and Informatics, pp. 307–312. IEEE (2014)
12. El-Hajj, M., Fadlallah, A., Chamoun, M., Serhrouchni, A.: A survey of internet of things (iot) authentication schemes. Sensors **19**(5), 1141 (2019)
13. Gamundani, A.M., Phillips, A., Muyingi, H.N.: An overview of potential authentication threats and attacks on internet of things (iot): A focus on smart home applications. In: Proceedings of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 50–57. IEEE (2018)
14. Gupta, S.: Next-generation user authentication schemes for iot applications. Ph.D. thesis, DISI, Univeristy of Trento, Italy (2020)
15. Gupta, S., Buriro, A., Crispo, B.: Driverauth: A risk-based multi-modal biometric-based driver authentication scheme for ride-sharing platforms. Computers & Security **83**, 122–139 (2019)
16. Gupta, S., Camilli, M., Papaioannou, M.: Provenance navigator: Towards more usable privacy & data management strategies for smart apps. In: Proceedings of the 11th International Workshop on Socio-Technical Aspects in Security, Affiliated with the 26th European Symposium on Research in Computer Security (ESORICS 2021), pp. 1–17. Springer (2022)
17. Gupta, S., Kacimi, M., Crispo, B.: Step & turn - a novel bimodal behavioral biometric-based user verification scheme for physical access control. Computers & Security (2022)
18. ISO9000:2015: Quality management systems — fundamentals and vocabulary. https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en (2015 *(Accessed on 20-02-2022)*). Online web resource
19. ISO/IEC24741:2018(en): Information technology — biometrics — overview and application. https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24741:ed-2:v1:en (2018 *(Accessed on 2020-07-28)*). Online web resource
20. Jain, A.K., Deb, D., Engelsma, J.J.: Biometrics: Trust, but verify. IEEE Transactions on Biometrics, Behavior, and Identity Science (2021)
21. Kannala, J., Rahtu, E.: Bsif: Binarized statistical image features. In: Proceedings of the 21st International Conference on Pattern Recognition (ICPR), pp. 1363–1366. IEEE (2012)
22. Krašovec, A., Pellarini, D., Geneiatakis, D., Baldini, G., Pejović, V.: Not quite yourself today: Behaviour-based continuous authentication in iot environments. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies **4**(4), 1–29 (2020)
23. Li, W., Wang, P.: Two-factor authentication in industrial internet-of-things: Attacks, evaluation and new construction. Future Generation Computer Systems **101**, 694–708 (2019)

24. Liang, X., Kim, Y.: A survey on security attacks and solutions in the iot network. In: Proceedings of the 11th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0853–0859. IEEE (2021)
25. Ling, Z., Liu, K., Xu, Y., Jin, Y., Fu, X.: An end-to-end view of iot security and privacy. In: Proceedings of the GLOBECOM 2017 - 2017 IEEE Global Communications Conference, pp. 1–7 (2017)
26. McCool, C., Marcel, S., Hadid, A., Pietikäinen, M., Matejka, P., Cernockỳ, J., Poh, N., Kittler, J., Larcher, A., Levy, C., et al.: Bi-modal person recognition on a mobile phone: using mobile phone data. In: Proceedings of International Conference on Multimedia and Expo Workshops (ICMEW), pp. 635–640. IEEE (2012)
27. Pires, I., Garcia, N., Pombo, N., Flórez-Revuelta, F.: From data acquisition to data fusion: a comprehensive review and a roadmap for the identification of activities of daily living using mobile devices. Sensors **16**(2), 184 (2016)
28. Ponnusamy, V., Regunathan, N.D., Kumar, P., Annur, R., Rafique, K.: A review of attacks and countermeasures in internet of things and cyber physical systems. Industrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital pp. 1–24 (2020)
29. Project, O.M.S.: Owasp mobile security project. `https://owasp.org/www-project-mobile-security/` (2020 *(Accessed on 20-02-2022)*). Online web resource
30. Ross, A., Banerjee, S., Chowdhury, A.: Security in smart cities: A brief review of digital forensic schemes for biometric data. Pattern Recognition Letters **138**, 346–354 (2020)
31. Shila, D.M., Srivastava, K.: Castra: Seamless and unobtrusive authentication of users to diverse mobile services. IEEE Internet of Things Journal **5**(5), 4042–4057 (2018)
32. Ten, C.W., Manimaran, G., Liu, C.C.: Cybersecurity for critical infrastructures: Attack and defense modeling. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans **40**(4), 853–865 (2010)
33. Van Oorschot, P.C.: User authentication—passwords, biometrics and alternatives. In: Proceedings of the Computer Security and the Internet, pp. 55–90. Springer, Cham (2021)
34. Verizon: Data breach investigations report. `https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf` (*Accessed on 20-02-2022*). Online web resource
35. Whosdrivingyou: Reported list of incidents involving uber and lyft. `http://www.whosdrivingyou.org/rideshare-incidents` (2018 *(Accessed on 20-02-2022)*). Online web resource
36. Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., Shen, X.S.: Security and privacy in smart city applications: Challenges and solutions. IEEE Communications Magazine **55**(1), 122–129 (2017)
37. Zimmermann, V., Gerber, N.: The password is dead, long live the password–a laboratory study on user perceptions of authentication schemes. International Journal of Human-Computer Studies **133**, 26–44 (2020)