Proceedings of 2024 IEEE 12th International Conference on Intelligent Systems (IS)

BioDSSL: A Domain Specific Sensor Language for Global, Distributed, Biometric Identification Systems

Philipp Hofer
philipp.hofer@ins.jku.at
Johannes Kepler University Linz
Institute of Networks and Security
Linz, Austria

Michael Roland
roland@ins.jku.at
Johannes Kepler University Linz
Institute of Networks and Security
Linz, Austria

René Mayrhofer
rm@ins.jku.at
Johannes Kepler University Linz
Institute of Networks and Security
Linz, Austria

***Abstract*—With biometric identification systems becoming increasingly ubiquitous, their complexity is escalating due to the integration of diverse sensors and modalities, aimed at minimizing error rates. The current paradigm for these systems involves hard-coded aggregation instructions, presenting challenges in system maintenance, scalability, and adaptability. These challenges become particularly prominent when deploying new sensors or adjusting security levels to respond to evolving threat models.**

To address these concerns, this research introduces BioDSSL, a Domain Specific Sensor Language to simplify the integration and dynamic adjustment of security levels in biometric identification systems. Designed to address the increasing complexity due to diverse sensors and modalities, BioDSSL promotes system maintainability and resilience while ensuring a balance between usability and security for specific scenarios.

Furthermore, it facilitates decentralization of biometric identification systems, by improving interoperability and abstraction. Decentralization inherently disperses the concentration of sensitive biometric data across various nodes, which could indirectly enhance privacy protection and limit the potential damage from localized security breaches. Therefore, BioDSSL is not just a technical improvement, but a step towards decentralized, resilient, and more secure biometric identification systems. This approach holds the promise of indirectly improving privacy while enhancing the reliability and adaptability of these systems amidst evolving threat landscapes and technological advancements.

***Keywords*—Biometric Identification Systems; System Scalability; System Maintenance; Decentralization**

I. Introduction

Biometric identification systems have experienced widespread adoption in various domains due to their ability to accurately verify the identity of individuals using unique physiological or behavioral traits (Section I-A). For instance, India's Aadhaar program utilizes biometric data [1], China's Social Credit System incorporates facial recognition [2], and Moscow's Russian Metro employs face recognition for security and contactless payment purposes [3]. The European Union intends to implement an entry/exit system that will involve the collection of fingerprints and facial images from travelers originating from third-countries [4].

As these systems become increasingly prevalent, they also become more complex, incorporating a diverse range of sensors and modalities to minimize error rates and improve overall performance. However, the current paradigm for biometric identification systems suffers from limitations related to its rigid and hard-coded aggregation instructions, posing challenges in terms of system maintenance, scalability, and adaptability. Deploying new sensors or adjusting security levels to meet evolving threat models becomes a daunting task (Section I-B).

To address these concerns, we introduce BioDSSL, a flexible solution to these challenges, enhancing system maintainability and adaptability (Section I-D) without compromising security (Section I-C).

A. Overview of biometric identification systems

Biometric identification systems are a form of identification and access control technologies that rely on the unique physiological characteristics of individuals. These systems have gained significant traction over recent decades due to their ability to provide more reliable and convenient identification compared to traditional methods such as passwords or PINs. They compare biometric features collected from an individual to templates to either authenticate or identify the individual.

There are various types of biometric identification systems, leveraging diverse biological features. Some of the most common include fingerprint, facial, iris, and voice recognition. They are utilized for a wide range of applications, such as tracking students' attendance [5], opening doors [6], facilitating contactless payments for public transport tickets [7], [8], and even streamlining border control processes [9] (cf. Fig. 1).

Despite their advantages, biometric identification systems are not without challenges. As biometric traits are distinctive and unalterable, the potential misuse of such data raises significant privacy and security concerns. Furthermore, the complexity of integrating diverse sensors and modalities, along with the need for dynamic security levels, presents additional

DOI 10.1109/IS61756.2024.10705276

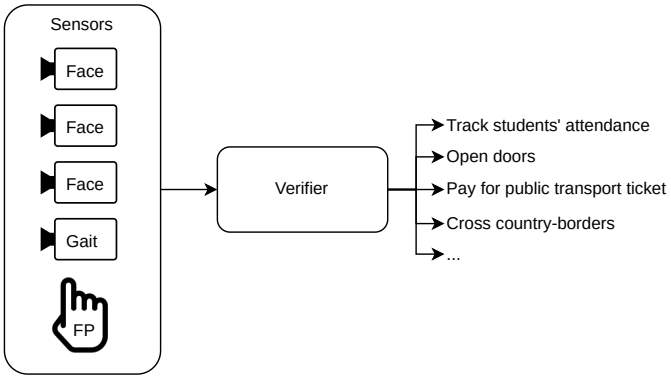

Fig. 1. This figure shows the architecture overview of biometric systems, with examples of different sensors (*face*, *gait*, and *f*inger*pr*int-recognition). The sensors capture biometric data from people and send that representation (most commonly in form of a high-dimensional vector) to a verifier. The verifier receives this information from one or more sensors and can then decide to trust these sensings enough to perform an action.

challenges in the development, deployment, and maintenance of these systems.

B. Complexity and rigidity of current systems

As biometric identification systems have become more pervasive, their complexity has escalated, primarily due to the integration of a variety of sensors [10], [11] and modalities [12], [13], all intended to minimize error rates and enhance system reliability. Each of these sensors and modalities comes with its own specifications, requirements, and compatibility issues, which increases the intricacy of these systems.

While hard-coded instructions were suitable for initial generations of biometric systems with a limited set of sensors and modalities, it is inflexible and challenging for more sophisticated systems. This rigidity is especially problematic when it comes to deploying new sensors or modifying system parameters to adapt to evolving threat landscapes or security requirements.

Further compounding the issue is the lack of a standardized, easy-to-use framework for integrating new sensors or adjusting system parameters. This lack makes it difficult for system developers and administrators to maintain, scale, and adapt their systems, leading to increased costs, longer deployment times, and potential vulnerabilities.

C. Proposed solution: BioDSSL

Given the growing complexity and rigidity of current biometric identification systems, there is a clear need for a more dynamic, adaptable, and scalable solution. To this end, we propose BioDSSL. One of the key advantages of BioDSSL is its ability to handle diverse sensor readings from various modalities. This allows for a more unified and efficient operation of biometric identification systems, regardless of the range of sensors and modalities they incorporate. By abstracting away the complexities of sensor integration and system configuration (Section III-B1), BioDSSL reduces the time and effort required for system maintenance, while enhancing scalability and adaptability.

In the sections that follow, we focus on the concept and design principles of BioDSSL, explore its unique features and advantages, and discuss how it fosters decentralization in biometric identification systems.

D. Scope and goals

The primary objective of this paper is to introduce BioDSSL and examine its potential role in enhancing the flexibility and security of biometric identification systems. The scope of our study includes an exploration of the design and features of BioDSSL, as well as an examination of how it addresses some of the current challenges faced by these systems.

We focus on the details of BioDSSL, discussing its concept, design principles, and approach towards decentralization of biometric identification systems. We further describe the unique features that make BioDSSL a valuable tool in the biometric identification landscape, underlining its ability to simplify the integration of new sensors and dynamic adjustments of security levels (Section III).

Furthermore, we focus on the practical implementation of BioDSSL (see Section IV), while providing a detailed methodology, including steps for integrating new sensors and dynamically adjusting security levels using BioDSSL. This allows to balance usability and security, crucial elements for the efficient operation of biometric identification systems.

Moreover, we present case studies and experimental results demonstrating the efficacy of BioDSSL (Section V). These real-world scenarios and experimental setups provide valuable insights into the practical application and advantages of BioDSSL. Additionally, quantitative and qualitative analyses of the results are provided to substantiate the improvements BioDSSL brings to biometric identification systems.

Lastly, we consider BioDSSL's impact on privacy and security (Section VI). Through this paper, we aim to contribute to the ongoing dialogue about enhancing the flexibility, security, and efficiency of biometric identification systems.

II. Background and related work

In this section, we focus on the historical context, evolution, and complexities surrounding the field of biometric identification systems (Section II-A). We explore the role of diverse sensors and modalities in enhancing the robustness and accuracy of these systems (Section II-B). We then address the challenges inherent in the present systems, detailing how their complexity and rigid structure makes system maintenance, scalability, and adaptability burdensome (Section II-C). This section also critically reviews previous attempts at resolving these issues, drawing attention to their limitations and the gaps they leave unaddressed (Section II-D). The collective understanding from this background study sets the stage for the introduction of our proposed solution to these challenges.

A. Evolution of biometric identification systems

Biometric identification systems have come a long way since their inception, evolving from basic systems with limited capabilities to sophisticated networks capable of handling multiple modalities and sensors. The earliest biometric systems were simple, employing single modality biometrics such as fingerprints or facial features for identification. As the technology advanced, these systems saw improvements in their speed, accuracy, and reliability. However, they remained largely static and rigid in their design, with fixed security levels and little flexibility to integrate new sensors or adjust to evolving threat landscapes.

In the last decade, the focus has shifted towards multi-modal biometric systems that integrate multiple biometric traits for more accurate and reliable identification [12], [13], [14], [15], [16], [17]. This shift has been driven by advances in sensor technology and computing power, along with the increasing need for robust and secure identification systems.

While these advancements have significantly enhanced the capabilities of biometric systems, they have also introduced new challenges. The integration of diverse sensors and modalities has made these systems more complex. Additionally, the increasing concentration of sensitive biometric data has raised privacy and security concerns.

B. Diverse sensors and modalities in biometrics

As discussed in the previous section, biometric identification systems have evolved to incorporate multiple sensors and modalities, enhancing their accuracy and reliability. This section focuses on the diversity of sensors and modalities currently employed in these systems.

Biometric sensors can be broadly classified into two categories: physiological and behavioral [18]. On the one hand, physiological sensors capture biometric traits such as fingerprints [19], face [20], iris [21], and palm prints [22], which are inherent to an individual and remain relatively stable over time. On the other hand, behavioral sensors capture traits such as voice [23], gait [24], and typing rhythm [25], which are unique to an individual but can vary based on factors like mood or health.

As for modalities, single-modal biometric systems use one sensor type to capture one biometric trait, while multi-modal systems use multiple sensor types to capture multiple biometric traits. Multi-modal systems offer several advantages over single-modal systems, including increased robustness to noise, greater resistance to spoofing, and improved identification accuracy [26].

However, the integration of diverse sensors and modalities in biometric systems is not without its challenges. Each sensor and modality has its own specific requirements and complexities, including different data formats, varying levels of sensitivity, and distinct comparison protocols. Furthermore, the dynamic nature of behavioral biometrics introduces additional layers of complexity, requiring systems to be adaptable and flexible.

Combining data from different modalities or sensors can be handled on different levels of fusion:

- Sensor-level fusion: This is the earliest stage at which fusion can occur. It involves integrating data from multiple sensors before any processing takes place. This approach can provide a rich dataset for identification but can also introduce significant complexity due to the need to manage raw data from diverse sensors.
- Feature-level fusion: Features are extracted from the sensor data, and the feature sets from different sensors are combined. This method has the potential for high identification accuracy because it uses detailed feature information. However, it requires a high degree of compatibility between feature sets, which can be challenging to achieve with diverse sensors and modalities.
- Score-level fusion: At this stage, each sensor or modality independently processes its data and outputs a score representing the confidence of a match. These scores are then combined to make a final decision. Score-level fusion is a popular choice because it offers a good balance between the amount of information used and the generalizability of the approach.
- Rank-level fusion: This method also involves independent processing by each sensor or modality, but instead of outputting scores, they output ranked lists of potential matches. These ranks are then combined to make a final decision. This method can be efficient and relatively simple to implement but may not utilize the available information as effectively as score-level fusion.
- Decision-level fusion: This is the final stage at which fusion can occur. Each sensor or modality independently processes its data and makes a yes/no identification decision. These decisions are then combined to make a final decision. This method is the simplest to implement but uses the least amount of information, potentially resulting in lower identification accuracy.

C. Challenges in current systems

With an understanding of the diversity and complexity of sensors and modalities in biometric identification systems, as well as the different fusion levels, we can now focus on the challenges that these systems currently face.

One challenge in current biometric systems is the integration of new sensors. As we have seen, each sensor and modality comes with its own specific requirements and complexities. Integrating a new sensor into an existing system can be a daunting task, often requiring substantial effort and modifications to the system.

Further, adjusting security levels in response to evolving threat models is another challenge. Given the static nature of many existing biometric systems, making such adjustments can be complex and time-consuming. The inability to quickly and dynamically adjust security levels can potentially leave systems vulnerable to emerging threats.

In addition, balancing usability and security presents a persistent challenge. On the one hand, systems must be secure and robust against spoofing attempts and noise. On the other hand, they must also be user-friendly, minimizing the time and effort required by users during identification. Striking the right balance is a delicate task that many current systems struggle with.

These challenges highlight the need for a solution that simplifies sensor integration, enables dynamic security adjustments and makes it easy to balance usability and security. In the following sections, we will see how BioDSSL is designed to address these challenges, improving the overall efficiency, adaptability, and resilience of biometric identification systems.

D. Previous attempts at solutions and their limitations

While there has been extensive research on various aspects of biometric systems, a structured way of specifying components in a biometric system has not been addressed in academic literature. Most studies have primarily focused on the intricacies of different fusion levels and detailed exploration of single modality systems. Consequently, these investigations do not provide comprehensive solutions for integrating diverse sensors seamlessly into an existing system nor updating the pipeline.

III. BioDSSL: A Domain Specific Sensor Language

Given the challenges and limitations identified in current biometric identification systems, we propose a novel solution, BioDSSL. We describe its underlying concept, design principles (Section III-A) and unique features (Section III-B) to simplify and enhance the resilience of biometric identification systems.

A. Concept and Design Principles of BioDSSL

BioDSSL has been developed with the aim to alleviate challenges related to complexity and scalability inherent in biometric identification systems. It accommodates the fact that different verifiers or operators of biometric systems can have vastly different requirements based on the context and purpose of the system (cf. Fig. 2).

For instance, in high-security environments such as border control checkpoints, the verifiers may wish to rely on a single, highly trusted biometric device that has been extensively validated for accuracy and reliability. This might include sophisticated devices such as iris scanners or high-resolution fingerprint readers, and the associated high level of assurance is necessary given the potential risks involved. On the other hand, in less critical contexts where the primary focus might be convenience or throughput, the requirements for the biometric system can be significantly less stringent. For example, in an educational institution tracking student attendance, less accurate but more expedient methods may be perfectly sufficient. In such a scenario, a simple facial recognition system or a fingerprint reader on a smartphone might be deemed adequate.

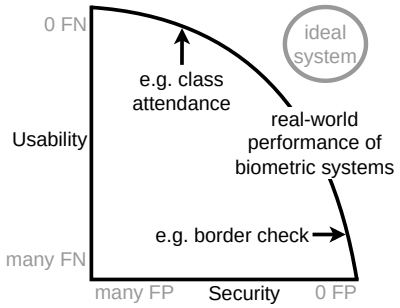

Fig. 2. Different scenarios require a different trade-off between security and usability. In some cases (e.g. border control) false positives should be drastically reduced. In exchange, some false negatives might be acceptable, as additional (better) sensings could take care of these. On the other hand, in a different scenario (e.g. attendance tracking) the focus could be reducing false negatives, as the consequences are less severe than a false positive.

The fundamental concept behind BioDSSL is to provide a structured yet flexible language that can manage the configuration, integration, and operation of a wide variety of applications. Through this, BioDSSL aims to simplify the process of integrating new sensor modalities into existing systems, as well as provide mechanisms for dynamically adjusting the system's security settings as per situational requirements.

B. Unique Features and Advantages

1) Level of fusion: BioDSSL wants to use as much biometric data as possible for fusion without overly complicating the system or creating undue burdens when changes are implemented. To this end, BioDSSL adopts score-level fusion as a fundamental part of its design. This level of fusion is chosen because it retains a high level of information, but does not necessitate the re-training of complex models when changes, such as adding a new modality, are introduced. This is in contrast to sensor-level and feature-level fusion, which, while heavily researched in recent years [27], [28], typically require retraining of the network whenever changes are implemented. Given the dynamic nature of biometric systems, it is not feasible to retrain networks each time a change is made. Score-level fusion, therefore, represents a practical and efficient choice. It allows BioDSSL to accommodate changes in the system, such as the addition of new modalities or updates in security levels, without needing to undergo time-consuming and resource-intensive retraining processes.

2) Sensor tags: BioDSSL incorporates a tag system for sensors to increase flexibility and adaptability, allowing the system to respond effectively to a wide array of circumstances, whether anticipated or not. The tags can be as generic or as specific as required by the context. For our running examples, a tag could be *soft biometric* for a system tracking student attendance, or it could refer to a specific device model used at a border control checkpoint. By allowing the tags to be mutable and not fixed, BioDSSL can adapt to evolving circumstances and changing system requirements.

In more detail, useful tags for a sensor could include a universally unique identifier (UUID) for unambiguous identification, the modality (fingerprint, iris, face, etc.), the operator (who uses or manages the sensor), the modality class (soft or hard biometric), the certified by tag (indicating the certifying authority), and the location of the sensor. These tags enable a granular level of control and customizability.

IV. Implementation

BioDSSL adopts a straightforward and easily comprehensible language syntax. The core elements of the language include tags (*TAG*), which are alphanumeric strings that can include hyphens, and values (*VALUE*), which can either be strings without quotes (*VALUE-NO-QUOTES*) or strings enclosed in quotes (*VALUE-WITH-QUOTES*). These elements are combined to create tag-value pairs (*TV*), which are semicolon-separated tag-value sequences (*TVS*). Each sensor has the mandatory *SECS* tag, denoting a floating-point value that defines the permissible duration, in seconds, for utilizing a reading. Additionally, it supports an arbitrary number of tag-value sequences using a comparison operator (“>” or “<”), along with a threshold level (*THRESHOLD*) associated with that sensor. A complete set of sensors (*AUTH*) is then defined as a comma-separated sequence of sensor definitions.

The language structure can be represented in augmented Backus-Naur form:

```
TAG = ALPHA *("-" / ALPHA) ;
VALUE-NO-QUOTES = 1*(ALPHA / DIGIT) ;
VALUE-WITH-QUOTES = DQUOTE 1*(VALUE-NO-QUOTES
    / SP) DQUOTE ;
VALUE = VALUE-WITH-QUOTES / VALUE-NO-QUOTES ;
TV = TAG "=" VALUE ;
TVS = TV *(";" TV) ;
THRESHOLD = FLOAT ;
SENSOR = "SECS = " INTEGER ";" TVS ("<" / ">")
    THRESHOLD ;
JOIN = "AND" / "OR" ;
AUTH = ["("] SENSOR *(["("] JOIN SENSOR [")"])
    [")"] ;
```

This language design, while simple, enables the representation of complex sensor configurations, allows dynamic adjustments of security levels and is able to accommodate a wide array of sensors and modalities.

The ability to adjust the confidence level and comparison operator directly addresses the need for dynamic security adjustments, catering to varying needs across different contexts. In the following section, we will explore how this implementation of BioDSSL is tested and validated through case studies and experimental results. This will provide a practical demonstration of BioDSSL's efficacy in addressing the challenges in the current paradigm of biometric identification systems.

V. Case studies and experimental results

To evaluate the effectiveness and efficiency of BioDSSL, we conducted a series of case studies and experiments. These exercises were designed to test the adaptability, scalability, and resilience of biometric identification systems managed using BioDSSL, in two scenarios.

A. Experimental setup

Our experimental setup involved describing the application of BioDSSL in different biometric identification system contexts, ranging from high-security applications such as border control, to more routine scenarios like student attendance tracking. The chosen scenarios differed significantly in their security requirements, the diversity of sensors used, and the volume of biometric data handled. This diverse selection was intended to test the adaptability and versatility of BioDSSL.

We used a variety of modalities in our experiments, including both hard and soft biometrics. The tag system of BioDSSL allowed to manage this diversity and helped in the seamless integration of new sensors.

B. Case studies demonstrating the efficacy of BioDSSL

The case studies conducted show the flexibility of BioDSSL in accommodating a variety of system requirements and sensor configurations.

1) Student attendance tracking: The first case study focused on student attendance tracking for a lecture. In this setting, a single soft biometric could be sufficient to meet the system's requirements, leading to this BioDSSL config:

```
AUTH =  secs=60;operator=dept-a;
        modality="soft biometric" < 1.0
```

This example demonstrates how BioDSSL can be efficiently used to manage a lower-security requirement setting, accommodating a soft biometric sensor and enabling easy adjustment of security settings based on the context. The tag system streamlined the integration of the soft biometric sensor. Moreover, the inherent adaptability of BioDSSL provides the department with flexibility for future expansions or changes. For instance, if the department decides to deploy a new sensor, even of a different modality, the system will continue to operate seamlessly, as long as the new sensor is also tagged as a *soft biometric* modality.

The adaptability of BioDSSL proves to be a valuable feature, providing flexibility for future expansions or changes. For instance, the department could decide to introduce a second authentication modality using a fingerprint scanner. By tagging the fingerprint scanner as a new modality, students who use the scanner would also be marked as present.

```
AUTH =  secs=60;operator=dept-a;
        modality="soft biometric" < 1.0 OR

        secs=300;operator=dept-a;
        modality="fingerprint" < 0.04
```

An additional benefit of BioDSSL are decentralized deployments. If another department, physically located in the same hallway also want to use biometric attendance tracking, the same sensors can be used, provided that the sensor's operator grants permission for this shared use. Without BioDSSL, each

verifier would need to be individually configured and updated whenever there are changes in sensor usage or security protocols. This task becomes cumbersome and prone to errors with an increasing number of verifiers. However, with BioDSSL, changes can be implemented universally by merely updating the shared BioDSSL specification, significantly reducing the effort and potential for errors. For instance, if the department decides to introduce gait recognition sensors in multiple locations, the BioDSSL configuration can be effortlessly updated to accommodate the new modality, as shown below:

```
AUTH =  secs=60;operator=dept-a;
        modality="soft biometric" < 1.0 OR

        secs=300;operator=dept-a;
        modality="fingerprint" < 0.04 OR

        secs=30;operator=dept-b;
        modality="gait" < 1.0
```

2) Border control: On the other end of the spectrum, in the context of a high-security scenario such as border control, the system requirements differ significantly. The border control authority could rely on a specific, trusted device to ensure stringent security measures are met.

To integrate the trusted device into the BioDSSL system, the following configuration could be used:

```
AUTH =  secs=15;uuid=655f60a4 < 0.3
```

This implementation showcases the ability of BioDSSL to seamlessly incorporate specific, trusted devices within high-security applications. By specifying the device's unique identifier (*UUID*) and defining the appropriate security threshold, the system can effectively utilize the trusted device to enhance security measures at border control checkpoints.

However, in order to further enhance the border control system's capabilities, the integration of, for example, radar distance sensing can be considered. Radar distance sensing technology can provide valuable information about the physical proximity of individuals, which can be useful in identifying potential threats or unauthorized access attempts. To incorporate radar distance sensing into the existing BioDSSL system, the sensor configuration can be extended as follows:

```
AUTH =  secs=15;uuid=655f60a4 < 0.3 AND
        secs=15;modality="radar distance" < 0.5
```

By including the additional modality of radar distance and assigning an appropriate threshold, the system can leverage radar distance sensing to complement the existing trusted device. This combination of sensors enables a multi-modal approach to security, incorporating both the trusted device and radar distance sensing to enhance threat detection and to ensure a robust border control system.

The use of parentheses and the logical operators "and" and "or" (*JOIN*) in BioDSSL enables the creation of more complex scenarios and enhances the system's flexibility. By enclosing sensor configurations within parentheses, it becomes possible to group conditions and establish precedence when evaluating them. This allows for the specification of intricate requirements and the logical relationships between different sensor modalities or thresholds.

VI. Attacks

While BioDSSL significantly enhances the flexibility of biometric identification systems, it is essential to assess its impact on privacy and security. This includes understanding potential vulnerabilities and considering potential attack vectors.

One potential threat scenario involves a rogue sensor that could deceive the system by falsifying specific tags. In this scenario, an attacker could manipulate a sensor to replicate the tags associated with a trusted sensor, leading the system to accept fraudulent biometric data. This type of attack is similar to a cybersecurity technique known as "spoofing", where an unauthorized entity assumes the identity of a trusted entity to exploit the system's vulnerabilities.

To address this issue, several mitigations commonly employed against spoofing attacks can be applied in this instance as well. These include:

- Authenticating sensors: Implementing a robust authentication mechanism that verifies the identity and integrity of each sensor can prevent rogue sensors from infiltrating the system. This ensures that only trusted sensors are accepted, reducing the risk of fraudulent data.
- Digital signatures for tags: Utilizing digital signatures for the tags issued by trusted entities. These entities can range from a specific institution or organization to a more global or national authority. For instance, in a system designed for tracking student attendance, only those tags signed by the responsible educational institute could be trusted. Alternatively, certain applications may opt to trust tags signed by a more overarching issuer, such as a national regulatory body.

By implementing these mitigations, the system can reduce the risk of spoofing attacks and enhance its overall security posture in the face of rogue sensor threats.

The modular nature of BioDSSL allows for the integration of additional security measures as they become available or necessary. This could include cryptographic verification methods, dynamic tag assignment, or sophisticated anomaly detection algorithms to identify and isolate potential rogue sensors.

VII. Conclusion

In conclusion, this paper has presented BioDSSL as a solution to the escalating complexity of biometric identification systems. By addressing the challenges associated with system maintenance, scalability, and adaptability, BioDSSL offers a systematic and repeatable language for integrating new sensors and dynamically adjusting security levels based on specific use cases.

The decentralization of biometric identification systems is a key focus of privacy-conscious biometric identification. BioDSSL contributes to the dispersal of sensitive biometric

data across various nodes, enhancing privacy protection and reducing the potential damage from localized security breaches. This strategic step towards decentralized and resilient systems aligns with the progressive interconnectivity of our world.

The adoption of BioDSSL not only improves technical aspects but also holds the promise of indirect benefits. It enables the efficient operation of biometric identification systems by handling diverse sensor readings from multiple modalities. Moreover, it enhances reliability and adaptability in the face of evolving threat landscapes and technological advancements.

As biometric identification systems continue to become ubiquitous, BioDSSL offers stakeholders a powerful tool for striking an optimal balance between usability and security. By simplifying the integration of new sensors and facilitating dynamic adjustments of security levels, BioDSSL significantly improves the overall maintainability and resilience of these systems.

Moreover, BioDSSL's adaptable design allows for future improvements and advancements, providing opportunities to enhance the overall architecture and further reinforce security measures in the years to come. For example, in the future BioDSSL could be enhanced by offering encryption mechanisms, access control policies, and anonymization techniques to ensure the protection of biometric data during transmission or storage.

In summary, BioDSSL is a strategic and comprehensive approach to overcome the challenges faced by global, distributed, biometric identification systems. Its potential to indirectly improve privacy, enhance reliability, and enable adaptability positions it as a valuable solution in the ever-evolving landscape of biometric technology.

ACKNOWLEDGMENT

This work has been carried out within the scope of Digidow, the Christian Doppler Laboratory for Private Digital Authentication in the Physical World. We gratefully acknowledge financial support by the Austrian Federal Ministry of Labour and Economy, the National Foundation for Research, Technology and Development, the Christian Doppler Research Association, 3 Banken IT GmbH, ekey biometric systems GmbH, Kepler Universitätsklinikum GmbH, NXP Semiconductors Austria GmbH & Co KG, and Österreichische Staatsdruckerei GmbH.

REFERENCES

[1] uidai.gov.in, "Unique Identification Authority of India," 2023, accessed February 2, 2023. https://uidai.gov.in/en/.

[2] C. Liu, "Multiple social credit systems in China," *Economic Sociology: The European Electronic Newsletter*, vol. 21, no. 1, pp. 22–32, 2019.

[3] mos.ru, "The Face Pay system for fare payment was launched at all metro stations," 2023, accessed February 2, 2023. https://www.mos.ru/news/item/97579073/.

[4] europa.eu, "Entry/exit system (ees)," 2023, accessed April 3, 2023. https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/smart-borders/entry-exit-system_en.

[5] S. C. Hoo and H. Ibrahim, "Biometric-based attendance tracking system for education sectors: A literature survey on hardware requirements," *Journal of Sensors*, vol. 2019, 2019.

[6] L. Mecke, K. Pfeuffer, S. Prange, and F. Alt, "Open sesame! user perception of physical, biometric, and behavioural authentication concepts to open doors," in *Proceedings of the 17th international conference on mobile and ubiquitous multimedia*, 2018, pp. 153–159.

[7] P. Chatterjee and A. Nath, "Biometric authentication for uid-based smart and ubiquitous services in india," in *2015 Fifth International Conference on Communication Systems and Network Technologies*. IEEE, 2015, pp. 662–667.

[8] G. Veerajay, S. Ramiah, and H. Vasudavan, "Biometric bus ticketing system in mauritius," *International Journal of Scientific and Technology Research*, vol. 8, no. 12, pp. 568–571, 2019.

[9] R. D. Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti, and G. Sforza, "Biometric recognition in automated border control: a survey," *ACM Computing Surveys (CSUR)*, vol. 49, no. 2, pp. 1–39, 2016.

[10] D. Prangchumpol, "Face recognition for attendance management system using multiple sensors," *Journal of Physics: Conference Series*, vol. 1335, no. 1, p. 012011, Oct 2019.

[11] E. G. Llano, M. S. García Vázquez, J. M. C. Vargas, L. M. Z. Fuentes, and A. A. Ramírez Acosta, "Optimized robust multi-sensor scheme for simultaneous video and image iris recognition," *Pattern Recognition Letters*, vol. 101, p. 44–51, Jan 2018.

[12] S. K. Choudhary and A. K. Naik, "Multimodal biometric authentication with secured templates — a review," in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, Apr 2019, p. 1062–1069.

[13] S. S. Sengar, U. Hariharan, and K. Rajkumar, "Multimodal biometric authentication system using deep learning method." Pune, India: IEEE, Mar 2020, p. 309–312.

[14] L. Wu, J. Yang, M. Zhou, Y. Chen, and Q. Wang, "Lvid: A multimodal biometrics authentication system on smartphones," *IEEE Transactions on Information Forensics and Security*, vol. 15, p. 1572–1585, 2020.

[15] N. D. Sarier, "Multimodal biometric authentication for mobile edge computing," *Information Sciences*, vol. 573, p. 82–99, Sep 2021.

[16] *Procedia Computer Science*, vol. 85, p. 109–116, Jan 2016.

[17] K. Kumar and M. Farik, "A review of multimodal biometric authentication systems," vol. 5, no. 12, 2016.

[18] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Systems with Applications*, vol. 143, p. 113114, Apr 2020.

[19] Z. Jin, M.-H. Lim, A. B. J. Teoh, B.-M. Goi, and Y. H. Tay, "Generating fixed-length representation from minutiae using kernel methods for fingerprint authentication," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 46, no. 10, pp. 1415–1428, 2016.

[20] K. Pranav and J. Manikandan, "Design and evaluation of a real-time face recognition system using convolutional neural networks," *Procedia Computer Science*, vol. 171, pp. 1651–1659, 2020.

[21] H. K. Rana, M. S. Azam, M. R. Akhtar, J. M. Quinn, and M. A. Moni, "A fast iris recognition system through optimum feature extraction," *PeerJ Computer Science*, vol. 5, p. e184, 2019.

[22] D. Zhong, X. Du, and K. Zhong, "Decade progress of palmprint recognition: A brief survey," *Neurocomputing*, vol. 328, pp. 16–28, 2019.

[23] A. T. Ali, H. S. Abdullah, and M. N. Fadhil, "Voice recognition system using machine learning techniques," *Materials Today: Proceedings*, pp. 1–7, 2021.

[24] C. Wan, L. Wang, and V. V. Phoha, "A survey on gait recognition," *ACM Computing Surveys (CSUR)*, vol. 51, no. 5, pp. 1–35, 2018.

[25] K. Ali, A. X. Liu, W. Wang, and M. Shahzad, "Keystroke recognition using wifi signals," in *Proceedings of the 21st annual international conference on mobile computing and networking*, 2015, pp. 90–102.

[26] M. O. Oloyede and G. P. Hancke, "Unimodal and multimodal biometric sensing systems: a review," *IEEE access*, vol. 4, pp. 7532–7555, 2016.

[27] H. F. Nweke, Y. W. Teh, G. Mujtaba, U. R. Alo, and M. A. Al-garadi, "Multi-sensor fusion based on multiple classifier systems for human activity identification," *Human-centric Computing and Information Sciences*, vol. 9, no. 1, pp. 1–44, 2019.

[28] S. Qiu, H. Zhao, N. Jiang, Z. Wang, L. Liu, Y. An, H. Zhao, X. Miao, R. Liu, and G. Fortino, "Multi-sensor information fusion based on machine learning for real applications in human activity recognition: State-of-the-art and research challenges," *Information Fusion*, vol. 80, pp. 241–265, 2022.