Biometrics Data Space: Ensuring Trustworthy and Secure Data Exchange for Suspect Identification.

Katerina Kyriakou[†,‡], Apostolos Apostolaras[†,‡], Polychronis Velentzas[†], Ilias Syrigos[†,‡]
Stavroula Maglavera[†,‡], Spyridon Evangelatos[*,§], Eleni Veroni[*,§] and Thanasis Korakis[†,‡]

[†]*Department of Electrical and Computer Engineering, University of Thessaly*, Volos, Greece
[‡]*CERTH, The Centre for Research & Technology, Hellas*, Volos, Greece
[*]*Research & Innovation Development, Netcompany-Intrasoft S.A.*, Luxembourg, Luxembourg
[§]*Dept. of Electronic Engineering, Hellenic Mediterranean University*, Crete, Greece

***Abstract*—Concerns about privacy protection, ethics, and the urgency to adhere to EU regulations for personal data protection are increasing as digital biometric technologies are widely being adopted in order to improve the accuracy of the identification and verification processes. This paper proposes the formation of a Biometrics Data Space, a trusted ecosystem that is based on the Data Spaces technology and offers secure sharing and exchange capabilities of biometric data in potential use cases, such as foreign Law Enforcement Agencies (LEAs) and forensic agencies, with an aim to facilitate the process of reliable identification of the suspects. The suggested identification framework incorporates Privacy Enhancing Technologies (PETs), such as homomorphic encryption, to address data protection concerns. Moreover, Large-Scale Data Indexing is applied to the biometric data to provide a fast and efficient comparison of a given facial image with ones stored in owners' local premises and without disclosing any personal information during the search and match process. Furthermore, automated access rights control is implemented by Blockchain Smart Contracts that are integrated into the Biometrics Data Space framework. The main objective of the suggested framework is to offer a reliable and automated identification system that ensures trust, data sovereignty, interoperability, and robust data protection.**

***Index Terms*—Identification, International Data Spaces, Biometrics, Privacy Enhancing Technologies**

I. Introduction

In today's technology-oriented world, fast and reliable identification systems are crucial to verify an individual's identity in a range of use cases, such as border control, law enforcement or forensic investigations. The necessity for strongly accurate identification frameworks has led to the adoption of biometric technologies, which significantly benefit from the distinctiveness of a person's biological characteristics, such as the face, voice, gait, iris, etc., when compared to obsolete recognition approaches.

As biometric identification systems evolve and biometric data are transformed into digital data for this purpose, the amount of concerns regarding privacy protection and ethical issues increases accordingly. Such issues include potential risks of fraudulent use of personal data, privacy violations, ethical issues from Artificiall Intelligence (AI) driven actions and decisions, and social categorization and exclusion. Moreover, data-driven business opportunities for economic growth that could benefit from data originating from different sources within an organization's ecosystem severely lack interoperability caused by data heterogeneity.

To deal with such considerations, the concept of Data Spaces has been gaining attention over the past few years [1]. The specific approach aspires to the development and establishment of a secure, independent, and sovereign system for data sharing, where trust between the participating actors, usage control of data imposed by the data owners, and data interoperability are ensured.

Biometric identification systems necessitating high accuracy and robust data privacy safeguards could considerably profit from the integration of the International Data Spaces (IDS). To achieve such an aspiration, this paper focuses on the formation of a Biometrics Data Space, that relies on the International Data Space Reference Architecture Model (IDS-RAM) [2] and utilizes facial images for quick and precise verification of a person's identity. The suggested scheme constitutes a trustworthy and automated data sharing ecosystem for cross-organization suspect identification, which secures the elimination of privacy risks with the integration of data protection technologies.

II. Literature Review & State-of-the Art Analysis

A. Related Work in Biometric Identification

The concept of observing a person's characteristics, either physical or behavioral, has been used for thousands of years between individuals to recognize each other. One of the most common physical biometric features that was introduced in the late 19th century is the significant discovery of the uniqueness of human fingerprints, which has improved the process of identification with the formation of the Automated Fingerprint Identification System (AFIS) [3] in police authorities investigations. In real-world forensics, the described system becomes very complicated to use due to the potential distortion of files that can be either smudged, incorrect, or incomplete. Another well-known approach includes DNA-based identification, which is highly accurate in terms of distinctiveness, since the DNA is unique for each individual,

This work has received funding from the EU Horizon Europe research and innovation programme through TENSOR project under GA: 101073920.

except in the case of identical twins. However, this approach could become vulnerable to privacy issues, considering that sensitive information can be revealed, such as health issues related to DNA data. [4].

As biometric identification advances into becoming commonplace in the AI era, many concerns regarding human rights and ethical principles arise. To address potential threats to fundamental rights, the European Commission focused on the legislation of high-risk AI systems. In 2020, the Assessment List for Trustworthy Artificial Intelligence (ALTAI) [5] was proposed as a tool that includes guides for special categories of data processing in accordance with privacy and data governance rules. In 2021, the European Commission introduced a plan for the first legal framework on AI, proposed as AI-Act [6], that denotes rules for three categories of biometric identification systems. These categories include remote biometric identification systems, such as live face recognition, biometric categorization systems, for the assignment of individuals based on their age, origin, etc. and emotion recognition systems, for the purpose of emotion or intention identification. AI-Act aims to absolve high-risk systems from potential threats to human fundamental rights and democracy and plans on obligating specific actions to such systems before they can be put on the market.

B. State-of-the-Art Analysis for Data Spaces

Recent technological advancements, including smartphones, 4G/5G networks, social media platforms, cloud computing, edge computing, and the Internet of Things (IoT), have led to a significant increase in data generation and storage. This surge in digital data is driven by the ongoing digital transformation in various sectors, such as business, governance, and industry. Additionally, the adoption of data analytics, machine learning, and artificial intelligence for data-driven decision making has further intensified the demand and consumption of data.

The proliferation of digital data has not only created opportunities but also challenges: On the one hand, digital data are an important asset and can be used as a tool to improve technological advancements, business competitiveness, economic growth, job creation, and social progress. Therefore, data-driven marketing empowers users with sufficient knowledge to improve their lives by gaining insight and making informed decisions. On the other hand, the unregulated use or misuse of digital data raises at the same time serious concerns that affect privacy and security. Therefore, effective and efficient management, analysis, and protection of digital data are of critical importance to foster economic and social growth.

In response to these challenges, the European Union (EU) has developed a digital data strategy [7] that puts citizens at the center of digital technological progress. The strategy aims to ensure that users preserve full control over their data, determining how it is used or shared by others. Therefore, safeguarding common European values and rights also requires prioritizing data privacy and security by using those technological enablers that can ensure data sovereignty, data usage control, and data governance. These enablers provide secure and privacy-preserving IT infrastructure to store, access, share and process data. One such technological solution that aligns with these requirements is the Data Spaces.

To support various aspects of data security, transparency, trust, interoperability, and sharing, the IDS [8] introduced the IDS-RAM, which is an open reference model that allows users to define and enforce their rules for accessing, processing, sharing, and using their data, while adhering to common regulations such as General Data Protection Regulation (GDPR) [9] and principles like Findable, Accessible, Interoperable, and Reusable (FAIR) [10].

The key technology for managing data access, usage, and control as well as to enable data sharing within IDS is the Connector, which was launched in 2015 by Fraunhofer research project funded by the German Federal Ministry for Education and Research [2]. A connector is composed of multiple containers, each serving a specific functionality by implementing any specific technology. The container management technology forms the basis for organizing and managing these containers within a connector. Importantly, the containers are designed to be independent of each other, allowing for the use of alternative technologies to minimize reliance on specific implementations or frameworks. Communication between connectors is established through an encrypted tunnel, ensuring secure and protected data exchange.

A notable initiative closely collaborating with IDS is Gaia-X [11]. It is a project aimed at achieving European strategic autonomy in the digital domain. Its primary focus is on developing and providing a Reference Architecture Model that federates data infrastructures and data service providers within the EU. The goal is to ensure and secure data sovereignty, empowering individuals, and organizations to have control over digital data.

Another implementation of the IDS that supports and complies with Gaia-X protocols and requirements is the Eclipse Data Space Connector (EDC) [12], which is designed to enable interoperable and sovereign data sharing and exchange based on the IDS-RAM. It consists of different entities or modules that work together to build Data Spaces, facilitating functions such as data query, data exchange, policy enforcement, monitoring, and auditing. More recent open-source implementations of Connectors compliant with the IDS include the FIWARE Data Space Connector [13], the FIWARE TRUE (TRUsted Engineering) Connector [14] by Engineering. Further information about Connector implementations and updates are periodically disseminated through International Data Spaces Association Connector Report [15].

III. Biometrics Data Space Architecture

A. Biometrics Data Space Components

The foundation of the Biometrics Data Space architecture proposed in this paper is the IDS-RAM [2], which is considered the de facto standard for creating and operating data ecosystems that aim at exchange of sensitive information in a trustworthy and sovereign manner. The core concept is the linkage of biometric data along with the enforcement of

conditions regarding access and usage strictly determined by the data owner, for the purpose of suspect identification. The data sharing scheme does not require a central data storage and management unit for the exchange of biometric data between different trusted organizations or countries. Instead, the data providers are able to share their data and services when requested while maintaining them at their local premises. The proposed scheme leverages the following components:

Connector: It is the core component for data exchange in a Data Space. Its role is to enable trusted and secure data sharing, as well as to provide mechanisms that establish data flows across different users, organizations, systems, and devices. The Connector component forms a gateway that is able to seamlessly connect trusted systems and their data to a Data Space, while ensuring data integrity and confidentiality. To enable the aforementioned functionalities, the Connector allows data owners to specify the rules and the policies that regulate the accessibility on the data and the way that it can be used, processed or shared. Unauthorized access, usage or disclosure is governed by the data usage control mechanism that ensures that data is used only according to the rules that have been imposed by the data owner and comply with international standards and rules for personal data protection. To ensure the principles of trust, data sovereignty and interoperability, the connector hosts a collection of containers as depicted in Figure 1, such as the execution core container for data exchange, the data application container that acts as a message router for data requesting and offering, as well as the usage control application container for the enforcement of control policies.

Identity Provider: It is the component responsible for creating, maintaining, managing, monitoring, and validating the identity certificates and information of the users exchanging data in a Data Space and their respective Connectors. To ensure trust among participating actors, it is compulsory to provide authorization and prohibit unauthorized access to the published data. The Identity Provider issues the Connector's self-description, as well as the static certificates that are used for its authentication. For the purpose of the data exchange, the Connector obtains dynamic tokens from an attribute server.

Metadata Broker: It is the entity that manipulates artifacts offerings by providers in the Data Space. Based on the IDS-RAM [2], there are multiple options for offering artifacts, including the Metadata Broker, the Federated Catalog, or their combination. The Metadata Broker constitutes a central component where artifacts' self-descriptions are registered, while the Federated Catalog provides the option for periodically crawling self-descriptions from participating Connectors with the Federated Cache Crawler component (FCC) and caching their self-descriptions inside the Connector's Federated Cache Node (FCN). In this paper, data offering is conducted with the usage of Metadata Broker which acts as a registry of offered artifacts and provides the functionalities for data offering for providers and data requesting for consumers.

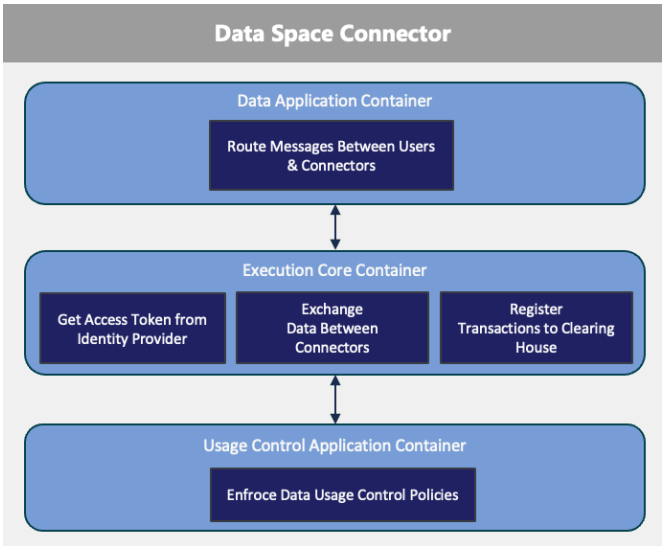

Fig. 1: Internal reference architecture for the Data Space Connector containers and corresponding functionalities that ensure trustworthy data exchange while maintaining data sovereignty, (based on the FIWARE TRUE Connector Architecture) [14].

B. Biometrics Data Space Design Principles

The design of the Biometrics Data Space involves the following fundamental principles for the accomplishment of the data exchange framework where security, privacy preservation, effectiveness, and ethical use of data are ensured.

Trust: Data sharing, data governance and manipulation are essential for Biometrics Identification systems to create a trustworthy environment for data exchange. "Trust" includes aspects regarding the management of roles, identities and user certificates, which are complemented by governance aspects. Each Connector that participates in the Data Space must be characterized by a unique identifier and possess a valid certificate. Moreover, every connector must be capable of verifying other Connectors' IDs. Each user that wants to access the Data Space through a connector must be certified in order to establish trust among all participants.

Data sovereignty: Usage policies definition and enforcement is an important aspect for a Data Space, to ensure data protection imposed by owners' own rules. Sovereignty rules form a powerful part of IDS by providing the ability for self-determination of access and usage conditions by the data providers, before even sharing the data with interested data consumers. Potential usage control policies include who has the rights to access the data, under what restrictions (e.g. location, time, duration) or which actions (process, share) are available.

Standardized Interoperability: Data exchange between users is conducted in a standardized manner, by leveraging the IDS Connector component. Each user shall be able to deploy and execute the Connector in its premises, or mobile/embedded devices or in the cloud.

Transparency: Every transaction that is related to any action, data access, data transmission or incident is recorded and logged by the IDS Clearing House component. Statistical assessment on data usage is derived from the analysis of those records and automated reporting and recommendations are generated and sent to the actual users.

IV. Biometric Data Spaces for Trustworthy Identity Verification

In this section, a trustworthy person recognition scheme will be proposed, leveraging the power of IDS with the use of biometric data. Existing biometric identification systems fall behind in terms of privacy compromisation issues as well as the lack of data exchange due heterogeneity of data sources and bureaucracy. The participating roles, processes and technologies described will be used cooperatively to achieve efficient cross-sector data sharing in a trustworthy, sovereign and interoperable manner.

A. Biometric Data

This identification scheme focuses on the exploitation of strong biometric features that are highly distinctive for each human being, such as face images. As mentioned in [16], recognition based on images of a person's face consist one of the most commonly used application for a variety of use case scenarios, since it includes features that are unique to individuals and cannot be easily changed or replaced. The scheme can also be extended to incorporate different types of physiological biometric features, such as fingerprints.

B. Privacy Enhancing Technologies

Data Spaces offer a data exchange ecosystem between participating stakeholders based on the European standards for data sovereignty and trust. On the contrary, PETs [17] propose a set of technologies for data protection and secrecy, in order to prohibit the original data sharing as it can be considered as a privacy compromisation threat. Data Spaces already include a number of PETs techniques such as access and usage control defined from data owners or anonymization of data owners when offering their data in the IDS Metadata Broker. In order to enhance protection of facial features revealed from images in the Biometrics Data Space for privacy and ethical concerns, the proposed recognition framework encompasses Homomorphic Encryption and Large-Scale Indexing.

1) Homomorphic Encryption: Homomorphic Encryption [18] is an encryption type that supports the computations to be performed on encrypted data without the requirement for previous decryption. The specific encryption type is very significant for the enrichment of privacy protection and law regulations enforcement, since it allows the identification process to take place without risking the revealing of any content. In the focused use case scenario, Homomorphic Encryption enables the secure person identification while maintaining confidentiality of personal data and prohibiting the access to unauthorized parties. Specifically, a biometric key-based Homomorphic Encryption will be used, where the data itself represents the protection key for the encryption process.

2) Large-Scale Data Indexing: The identification process heavily relies on the comparison of a provided facial image with other facial images stored in the local premises of the data owners. For fast and efficient retrieval and comparison of facial images, Large-Scale Data Indexing is suggested. Indexing improves the speed and cost of locating and retrieving specific data when needed by integrating deep hashing techniques along with artificial intelligence, and specifically Approximate Nearest Neighbor Search (ANN) algorithms. The specific combination addresses the problems of applications with large amounts of data, while maintaining low computational cost during the search process. Moreover, deep hashing techniques allow comparison of produced hashes based on facial images, in order to provide a similarity measure between the biometric data, which denotes the similarity between them.

The combination of the two technologies improves the trustworthiness of the identification process through the Biometrics Data Space. However, the proposed scheme should carefully consider the tradeoff between security and performance, since such PETs may increase resource and computational requirements.

C. Blockchain Smart Contracts

Providing a fully automated identification system that removes the need from intermediaries to execute and control the internal processes is established with the integration of Blockchain Smart Contracts in the Biometrics Data Space. Smart Contracts can be considered as self-executing contracts implemented by scripts that automatically execute specific actions when predefined conditions are met in a trusted way [19]. The proposed scheme leverages the Blockchain Smart Contracts technology by providing automated agreements that ensure data sovereignty. In this scheme, Smart Contracts will control the enforcement process by performing access and usage rights checking, and accordingly grant or prohibit the access to the homomorphically encrypted biometric data. The data provided to the blockchain will be stored in decentralized, self-controlled Data Pods based on the Solid framework [20], which are stored in the owners' local premises or cloud infrastructures. Another important aspect of Blockchain is the registration of the transactions performed between participants for auditing purposes. Blockchain guarantees traceability and transparency since its corresponding transactions are immutable.

D. Identification System

The Biometrics Data Space framework suggested in this paper relies on the combination of IDS with the technologies of Homomorphic Encryption, Large-Scale Data Indexing and Blockchain Smart Contracts, for accurate person identification in a privacy perserving way. This section provides a the main functionalities executed between two participant roles, one Data Consumer that requests access to sensitive biometric data and one Data Provider that offers the access or usage. The following processes are based on the IDS-RAM Process Layer

[2] and describe the main interactions between the components of the Biometrics Data Space:

Onboarding: The specific process is necessary for the identification of a stakeholder, the acquisition of a Connector component and its registration to the Data Space. It consists of a preparation phase and an instantiation phase. During the Preparation phase, the Provider and the Consumer both request registration and certification of their organization in the Data Space. After the certification is granted, the instantiation phase takes place where a Connector component is created and assigned to each corresponding user. The created Connector is assigned a unique identity by the Identity Provider and can be registered to the IDS Metadata Broker, in order to be discoverable by other participating trusted Connectors.

Data Offering: The existence of homomorphically encrypted and indexed facial images is required for comparison during the identification process. In most cases, Data Providers do not know in advance which consumers will be interested in their data. To tackle this challenge, each offered artifact is assigned a "Self-Description" document that includes necessary information as well as the usage conditions.

The "Data Offering" in the proposed scheme follows the Metadata Broker approach where a Data Provider registers data Self-Descriptions to the central broker component, to declare its availability to other trusted Connectors. A Connector is able to search through the broker's catalog to discover registered artifacts. At the same time, the homomorphically encrypted and indexed data should also be uploaded to the Provider's own Data Pod to enable Smart Contracts Execution.

Usage Contract Negotiation: Before the actual exchange of the biometric data, the usage control policies must be agreed upon between the participants. Control policies may vary from completely allowing or prohibiting the access to partial availability of information, time-restricted reachability or location-based approval of access. The access control happens with the use of Blockchain Smart Contract Execution Manager which receives access requests from Consumer Connector and performs access and access rights checking before authorizing the data and providing the decryption key. The usage control enforcement takes place through the Connector's functionalities.

As presented in Figure 2, the identification process workflow utilizing the Biometrics Data Space between two stakeholders can be summarized in the following steps:

1) Data Consumer initiates a request through the Consumer Connector and provides a previously homomorphically encrypted and indexed facial image.
2) The Consumer Connector searches to the Metadata Broker Catalog the self-descriptions of offered data from other Connectors. Then, it compares the provided indexed data with the Broker's indexed data and obtains a list of matches based on the acceptance of their similarity scores.
3) For the data whose similarity scores exceed the pre-defined acceptance threshold, the Consumer Connector submits a request to the Blockchain Smart Contract Execution Manager in order to check usage rights and determine access.
4) The Data Provider gets notified about the data access request and the Blockchain Smart Contract Execution Manager performs access rights checking for the homomorphically encrypted data stored in the Data Provider's Data Pod and responds either with grant or rejection of access.
5) If access is granted, the request is forwarded to the Provider Connector which retrieves the data from the Pod along with the decryption key returned from the Blockchain Component.
6) Usage control policies are enforced and the indexed data along with the decryption key are shared from the Provider Connector to the Consumer Connector. The Consumer Connector decrypts the homomorphically encrypted data based on the received key and returns the decrypted data to the Data Consumer.

E. Advances of Biometrics Data Space for Trustworthy identification

According to the new Prüm II Regulation [21] about automated data exchange frameworks for police cooperation, new rules are introduced for the improvement and acceleration of data sharing frameworks for investigation of criminal cases. The proposed model of this paper achieves to adhere to Prüm II rules by: (1) allowing automated data exchanges on facial images with the Biometrics Data Space Identification framework, (2) maintaining central components in the Data Space such as the Identity Provider, the IDS Metadata Broker, the IDS Clearing House or the Blockchain Smart Contract Execution Manager, (3) ensuring the matching and data exchange is conducted in much less than 48 hours due to the automated data exchange framework and the fast indexing and encryption/decryption techniques, and (4) the enhanced data protection with strong safeguards based on the Homomorphic Encryption that prohibits the exchange of sensitive raw biometric data between the participating stakeholders.

V. Conclusions

Existing biometric identification systems, although accurate and utilized in many use cases, threaten the privacy protection of personal data with compromisation risks aiming from economic exploitation to social categorization or exclusion, and lack in data sharing opportunities for cross-organization suspect identification. To address the above mentioned limitations, this paper proposes the formation of a Biometrics Data Space for trustworthy suspect recognition. The suggested identification framework relies on the IDS-RAM Components to ensure trust between participating stakeholders, data sovereignty imposed by data owners and interoperability between heterogeneous data sources. Enhanced data protection is guaranteed by the integration of PETs, focusing specifically on Homomorphic Encryption applied on data in order to avoid the exchange of raw biometric data. Fast and efficient data retrieval and comparison is ensured through the application of

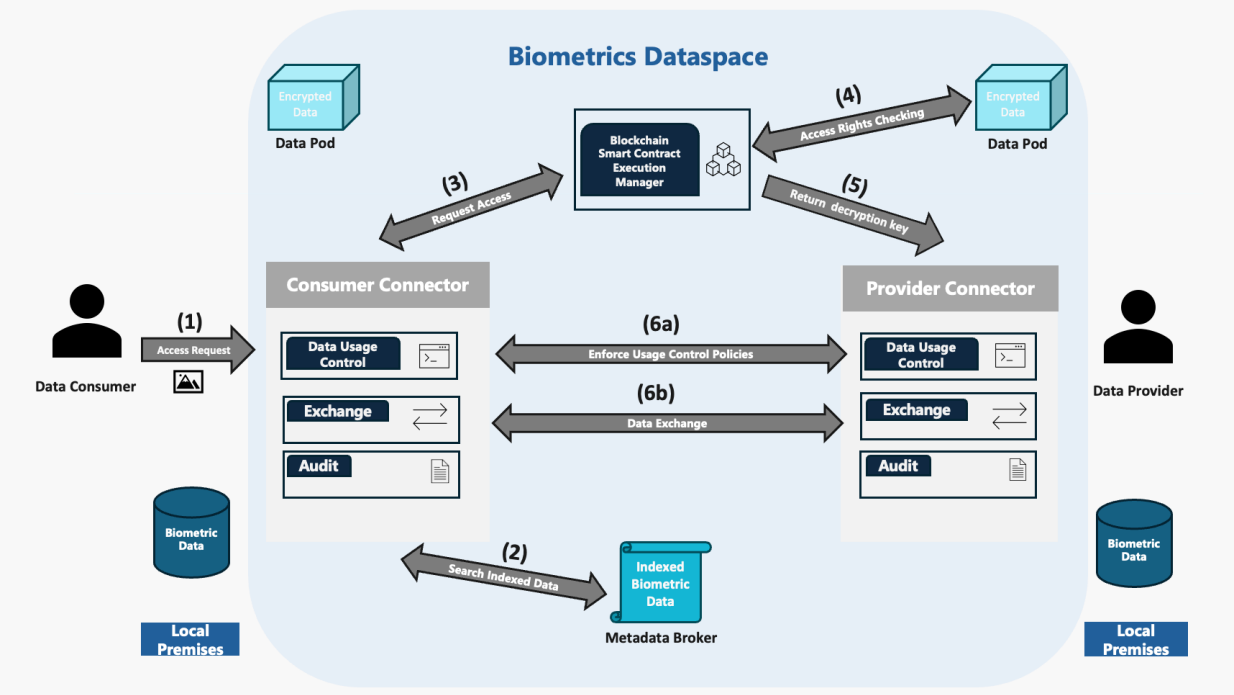

Fig. 2: Representation of person identification process with the use of Biometrics Data Space.

Large-Scale Biometric Data Indexing, while automated access rights checking is performed by Blockchain Smart Contracts. Altogether, the proposed system ensures quick and accurate identification results, as well as transparency and traceability.

REFERENCES

[1] B. Otto, "The evolution of data spaces," in *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage*. Springer International Publishing Cham, 2022, pp. 3–15.

[2] B. Otto, S. Steinbuss, A. Teuscher, and S. Lohmann, "IDS Reference Architecture Model," Jul. 2021. [Online]. Available: https://doi.org/DOI:10.5281/zenodo.5105529

[3] K. R. Moses, P. Higgins, M. McCabe, S. Prabhakar, and S. Swann, "Automated fingerprint identification system (afis)," *The fingerprint sourcebook*, vol. 1, pp. 6–1, 2011.

[4] H. M. El-Bakry and N. Mastorakis, "Personal identification through biometric technology," in *9th WSEAS International Conference on Applied Informatics and Communications (AIC09), Moscow, Russia*, 2009, pp. 325–340.

[5] E. Commission, C. Directorate-General for Communications Networks, and Technology, *"The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self assessment"*. Publications Office, 2020.

[6] "EUR-Lex - 52021PC0206 - EN - EUR-Lex, "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts"." [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

[7] "Member States and Commission to work together to boost artificial intelligence "made in Europe"." [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6689

[8] H. Pettenpohl, M. Spiekermann, and J. R. Both, *International Data Spaces in a Nutshell*. Cham: Springer International Publishing, 2022, pp. 29–40. [Online]. Available: https://doi.org/DOI:10.1007/978-3-030-93975-5_3

[9] "EUR-Lex - 32016R0679 - EN - EUR-Lex, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)" ." [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

[10] M. Axton, A. Baak, N. Blomberg, J.-W. Boiten, L. B. da Silva Santos, P. E. Bourne, J. Bouwman, A. J. Brookes, T. Clark *et al.*, "The fair guiding principles for scientific data management and stewardship," *Scientific data*, vol. 3, p. 160018, 2016.

[11] Gaia-X Association, "Overview - Gaia-X Architecture Document - 22.10 Release," 2022. [Online]. Available: https://docs.gaia-x.eu/technical-committee/architecture-document/22.10/overview/

[12] "Eclipse dataspace connector — projects.eclipse.org." [Online]. Available: https://projects.eclipse.org/proposals/eclipse-dataspace-connector

[13] U. Ahle and J. J. Hierro, "Fiware for data spaces," *Designing Data Spaces*, p. 395, 2022.

[14] "FIWARE TRUE (TRUsted Engineering) Connector: easing data sharing in Gaia-X." [Online]. Available: https://www.eng.it/en/case-studies/true-connector-per-facilitare-la-condivisione-di-dati-in-gaiax

[15] M. H. G. Giussani, S. Steinbuss and N. Gras, "Data Connector Report," Jan. 2024. [Online]. Available: https://doi.org/DOI:10.5281/zenodo.10591027

[16] V. Dhir, A. Singh, R. Kumar, and G. Singh, "Biometric recognition: A modern era for security," *International Journal of Engineering Science and Technology*, vol. 2, no. 8, pp. 3364–3380, 2010.

[17] H. T. Tavani and J. H. Moor, "Privacy protection, control of information, and privacy-enhancing technologies," *ACM Sigcas Computers and Society*, vol. 31, no. 1, pp. 6–11, 2001.

[18] X. Yi, R. Paulet, E. Bertino, X. Yi, R. Paulet, and E. Bertino, *Homomorphic encryption*. Springer, 2014.

[19] M. Kolvart, M. Poola, and A. Rull, "Smart contracts," *The Future of Law and etechnologies*, pp. 133–147, 2016.

[20] C. Esposito, R. Horne, L. Robaldo, B. Buelens, and E. Goesaert, "Assessing the solid protocol in relation to security and privacy obligations," *Information*, vol. 14, no. 7, p. 411, 2023.

[21] "EUR-Lex - 52021PC0784 - EN - EUR-Lex, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council"." [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A784%3AFIN