Enabling Qualified Anonymity for Enhanced User Privacy in the Digital Era

Vaios Bolgouras*
vaiosbolgouras@ssl-unipi.com
University of Piraeus
Greece

Kostantinos Papadamou
kostantinos.papadamou@eecei.cut.ac.cy
Cyprus University of Technology
Cyprus

Ioana Stroinea
stroineaioana@gmail.com
certSIGN
Romania

Michail Papadakis
mpapadakis@lstech.io
LSTech ESPANA
Spain

George Gugulea
george.gugulea@certsign.ro
certSIGN
Romania

Michael Sirivianos
michael.sirivianos@eecei.cut.ac.cy
Cyprus University of Technology
Cyprus

Christos Xenakis
xenakis@unipi.gr
University of Piraeus
Greece

ABSTRACT

This paper presents a privacy-enhancing identity management platform designed to address the challenges associated with online identity verification and privacy protection. INCOGNITO offers a comprehensive solution by leveraging concepts such as Qualified Anonymity and cryptographic credentials, along with technologies including blockchain, Tor Network, and software stacks like Idemix. By employing these mechanisms, INCOGNITO aims to enable users to securely acquire and manage their identity attributes, while preserving their privacy and ensuring compliance with both regulatory bodies and Service Providers' requirements. The platform facilitates the issuance and verification of cryptographic credentials, granting users access to online services based on fine-grained subsets of their identity attributes. Furthermore, the effectiveness and feasibility of the platform are demonstrated through two pilot projects focused on online multimedia content sharing and identifying bots or fake users in online social networks. These pilots showcase the practical applicability of INCOGNITO in solving identity-related challenges while safeguarding user privacy and security.

KEYWORDS

Privacy, Qualified Anonymity, Identity Management, Cryptographic credentials, Artificial Intelligence

1 INTRODUCTION

In today's digital age, the importance of user privacy has become increasingly significant. With the widespread adoption of online services and the digitization of personal information, the need to safeguard sensitive data from unauthorized access has emerged as a critical concern. Instances of identity theft, privacy violations, and data breaches have raised alarming questions about the vulnerability of user information and its potential for exploitation [1] [2]. Such incidents have severe repercussions, not only impacting individuals' financial security and personal well-being but also eroding trust in online platforms [3]. Identity theft, wherein malicious actors acquire personal information to impersonate individuals, have become a prevalent threat. Unscrupulous activities like fraudulent financial transactions, unauthorized access to personal accounts, and manipulation of sensitive data have caused substantial harm to unsuspecting users [4]. Moreover, privacy violations, such as the unauthorized collection and sharing of personal data by Service Providers (SPs), further compound the risks users face. These infringements can result in targeted advertising, unwarranted profiling, and compromised confidentiality, thereby undermining individuals' autonomy and control over their own information [5]. While various solutions have been proposed to address these privacy concerns, they often fall short in terms of accessibility and ease of use for the average user. Existing mechanisms, such as complex encryption methods or consent management systems, often require specialized technical knowledge and are not readily understandable or usable by layman users. Consequently, users face a significant barrier when attempting to protect their privacy effectively [6].

To bridge this gap, we introduce the INCOGNITO platform as a user-friendly solution designed to enhance user privacy. By combining cutting-edge technologies such as anonymous credentials [7], User-Managed Access (UMA) [8] and blockchain technology [9], INCOGNITO offers a comprehensive privacy protection framework that empowers users to take control of their personal information.

Leveraging the power of artificial intelligence, INCOGNITO incorporates an intelligent assistant to guide users through the process of managing their privacy settings, making it accessible to individuals with varying levels of technical expertise. The anonymous credentials integrated into the INCOGNITO platform enable users to assert their identity without disclosing sensitive personal information, preserving their privacy in online interactions. Additionally, the adoption of UMA provides users with fine-grained control over how their personal data is accessed and shared by online SPs, ensuring transparency and informed consent.

In this paper, we present an in-depth exploration of the INCOGNITO platform, highlighting its core features and illustrating its user-friendly approach to privacy protection. We provide insights into the integration of anonymous credentials and UMA, showcasing their effectiveness in safeguarding user privacy. Furthermore, we discuss the role of the AI-based assistant within the INCOGNITO platform, elucidating how it simplifies the complex process of managing privacy settings for users of all backgrounds. Through the INCOGNITO platform, we aim to revolutionize the way individuals approach privacy protection in the digital realm. By combining cutting-edge technologies with user-friendly design principles, INCOGNITO can empower users to regain control over their personal information, mitigating the risks associated with identity thefts, privacy violations, and data breaches.

The paper is organized as follows. Section 2 presents privacy challenges and threats, including the problem statement and threat model. Section 3 focuses on the architecture, detailing the components and processes of the INCOGNITO framework. Section 4 explores two use cases: online multimedia content sharing and fake news dissemination. Section 5 provides insights regarding related works in the field. Finally, Section 6 provides a conclusion summarizing the key findings and contributions of the paper.

2 PRIVACY CHALLENGES AND THREATS

In this section the problem statement is outlined, identifying the key issues and concerns associated with existing identity management systems. Subsequently, we define the threat model, analyzing the potential risks and adversaries that pose a threat to user privacy and data security. By understanding the problem landscape and the threat landscape, we lay the foundation for the design and implementation of our proposed framework.

2.1 Problem Statement

Identity fraud has emerged as a significant cybersecurity issue, reaching alarming levels in recent years. To mitigate this growing threat, commercial online services require users to disclose and validate their complete identities using various personal data and documents. Simultaneously, these online services must adhere to the General Data Protection Regulation (GDPR) [10] to safeguard privacy. However, existing online identification schemes lack the capability for fine-grained treatment of identity attributes, known as Attribute-Based Access Control (ABAC) [11]. Consequently, users are compelled to disclose their entire identities, even when a SP only requires specific attributes, such as age or nationality. Moreover, the absence of an integrated infrastructure for providing Qualified Anonymity (QA) exacerbates the problem. QA refers to the ability to access SPs using proofs of identity attributes without the need to disclose one's complete identity. Although users possess multiple proofs of identity, such as physical documents and online accounts, the current identity landscape lacks a comprehensive solution that ensures QA. Additionally, the issue of identity fragmentation further complicates the matter. Users maintain accounts and identity attributes across multiple online services, leading to challenges in proving ownership of accounts, transferring reputation scores between identity realms, and other related issues.

The combination of these challenges highlights the pressing need for an innovative solution that addresses the shortcomings of existing identity verification mechanisms. Such a solution should enable fine-grained attribute-based access control, ensuring that users only disclose necessary identity attributes to SPs. Moreover, it should provide a robust infrastructure for QA, allowing users to access services without compromising their complete identities. Additionally, addressing the issue of identity fragmentation is essential to facilitate seamless user experiences across multiple online SPs. By overcoming these challenges, individuals can regain control over their privacy while maintaining compliance with data protection regulations.

2.2 Threat Model

The threat model for the INCOGNITO platform encompasses potential risks associated with identity theft, unauthorized access, and privacy violations. INCOGNITO employs specific measures to mitigate these threats effectively. Firstly, to counter identity theft, the platform adopts a proactive approach by refraining from sharing users' complete identities. Instead, INCOGNITO focuses on providing proof of ownership for specific identity attributes, ensuring that only necessary information is disclosed, minimizing the risk of identity theft. Secondly, unauthorized access is mitigated through the implementation of FIDO2.0 [1] for secure and robust authorization. This advanced authentication mechanism enhances the platform's resistance to unauthorized access attempts, reducing the likelihood of data breaches and maintaining the integrity of user privacy. Lastly, INCOGNITO addresses privacy violations by empowering users to have full control over their personal data. Through the platform's user-centric design, individuals can make informed decisions about what information to share, thereby minimizing the potential for privacy breaches. Moreover, INCOGNITO operates on top of the Tor network [2], which provides an additional layer of privacy and anonymity, further safeguarding user data from unauthorized access and privacy violations. By incorporating these measures, INCOGNITO establishes a resilient framework that mitigates the risks of identity theft, unauthorized access, and privacy violations, ensuring a secure and privacy-preserving environment for users.

3 ARCHITECTURE

In this section, we provide an in-depth exploration of the architectural processes and components that constitute the INCOGNITO platform, as shown in Figure 1. By delving into the intricacies of the

[1] https://fidoalliance.org/specs/fido-v2.0-rd-20170927/fido-overview-v2.0-rd-20170927.html
[2] https://www.torproject.org/

platform's design, we aim to offer a comprehensive understanding of how INCOGNITO addresses privacy challenges and mitigates associated threats. The presented architectural framework encompasses a set of interconnected components and processes, working in harmony to ensure the secure and privacy-preserving acquisition and management of identity attributes. These components and processes incorporate various cutting-edge technologies, including cryptographic credentials, the Tor network, and blockchain, which collectively enhance the security and anonymity of user interactions with online service providers.

3.1 INCOGNITO Components

User Device: Within the INCOGNITO framework, the user's mobile device plays a vital role as the focal point for device-centric authentication. To facilitate the authentication process between the user and remote services, the FIDO2.0 protocol is employed. This module encompasses the FIDO2.0 Client and the FIDO2.0 Protocol stack, both operating on the user's device and establishing communication with the Relying Party. Additionally, INCOGNITO incorporates ABAC cryptographic credentials for Identity Providers (IdPs). The cryptographic credentials obtained from the Identity Consolidator (IdC) and various IdPs are securely saved in the designated cryptographic credentials storage on the user's device. Furthermore, the cryptographic credentials storage leverages the Trusted Execution Environment (TEE) capabilities of the user device to enhance credential security. The user's device comes with a cryptographic interface that engages with the Idemix protocol stack present on the device. This facilitates the retrieval of Idemix credentials stored in the Cryptographic Credential Storage. To improve the user device's TEE functionalities, the project utilizes Open-TEE [3], an open-source initiative for developing critical functionalities related to anonymous credential protocols such as Idemix for INCOGNITO. Federated login protocol OpenID Connect (OIDC) is employed to facilitate authentication and authorization between the IdP and SPs. Additionally, FIDO2.0 integration supersedes the conventional password approach for verifying the identity of the user device and the IdP. The user maintains authority over their personal identity details using the application for managing identity and access control. This application is installed on the user's device and establishes communication with the IdC. This software enables users to control the sharing of their identity information with individual SPs. The user can also generate cryptographic credentials directly from their identity attributes on the device, utilizing them for ABAC. The application includes consent management features and ID privacy functionality, empowering users to possess awareness and authority over the disclosure of particular elements of their identity to specific SPs.

The user device is equipped with an AI-powered Assistant that interacts with the IdC to provide information and assistance to the user in efficiently handling their identity. The AI Assistant alerts the user regarding the essential identity attributes that need to be shared with SPs in order to gain access to resources. Additionally, it alerts the user to the risks associated with revealing certain identity attributes, which may allow SPs to infer the user's complete identity. The device also incorporates an identity acquisition module that securely and swiftly acquires identity attributes from online identities (e.g., Facebook account) and physical ID documents (e-Passports, eIDs) using the Near-Field Communication (NFC) protocol. The user can choose to save the gathered and validated identity characteristics in the IdC. The QR client module is included on the user device for efficient credential transfer. By scanning a QR code, the user can access services from their browser without requiring re-authentication. The IdP utilizes the QR code to verify the user's authentication status, granting them access to create a new session.

Identity Provider: INCOGNITO prioritizes user security and privacy, and in this context, IdPs play a crucial role in authentication. An Identity Provider (IdP) functions as a reliable entity that verifies the identities of individuals on behalf of online assets, like SPs. Federated authentication forms the basis of the authentication procedure, which involves multiple organizations consenting to utilize identical identification information for accessing various applications or services. In this scenario, the IdP functions as the party responsible for authentication where users possess their login credentials. A third party, such as a SP in INCOGNITO, trusts the authenticating party.Hence, when a user seeks to utilize services offered by a SP, they verify their identity to an IdP, who subsequently generates a token enabling the user to authenticate themselves with the third party. Given the instances of password leaks and the exposure of sensitive user information resulting from data breaches and security attacks on SPs' user credential databases in recent years, employing an IdP introduces multiple layers of security, including features like multi-factor authentication and strong encryption.

Adopting an IdP also relieves users from the burden of creating and remembering multiple passwords, while simultaneously sparing SPs from the responsibility of storing and safeguarding user information. The SP relies on the authentication data stored by the IdP to prevent the need for local storage of user information. The IdP preserves the identity characteristics of its users and assists in generating cryptographic credentials on the user's device via the credential management component. This module adheres to the FiWARE specification [4] and utilizes the Idemix cryptographic credential stack for generating credentials. The credential management module also handles credential verification, resulting in trusted identity attributes that are transferred to SPs using the OpenID specification and to the IdC for storage and backup in the event of an IdP failure. The IdPs rely on two key servers. The first one is the FIDO2.0 server, which facilitates user registration and authentication at the IdPs. The second one is the QR authentication server, designed to enable users to access services from other devices or browsers while they are already authenticated on their user device. The user can utilize a QR Client installed on their device to scan a QR code and transmit it to the QR Authentication server for validation. This procedure allows the IdP to verify the user's identity and provide authorization for accessing resources from a device distinct from the one employed for QR Code scanning.

Identity Consolidator: The IdC serves as the central node in the INCOGNITO platform, integrating various. Primarily, it functions as the repository of a user's online identity. The IdC collects real-world and online information about the user and consolidates

[3] https://open-tee.github.io/

[4] https://github.com/FIWARE/specifications

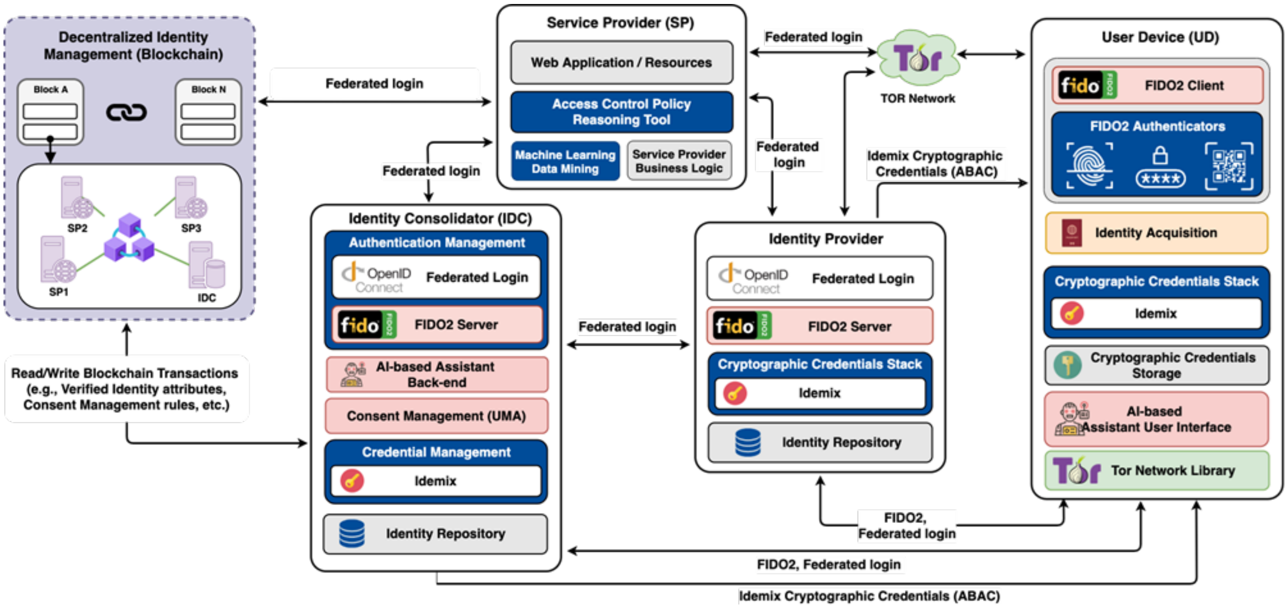
Decentralized Identity Management (Blockchain)
Block A
Block N
SP2
SP3
SP1
IDC
Read/Write Blockchain Transactions (e.g., Verified Identity attributes, Consent Management rules, etc.)
Federated login
Service Provider (SP)
Web Application / Resources
Access Control Policy Reasoning Tool
Machine Learning Data Mining
Service Provider Business Logic
Federated login
Federated login
TOR Network
Federated login
Idemix Cryptographic Credentials (ABAC)
User Device (UD)
fido
FIDO2 Client
FIDO2 Authenticators
Identity Acquisition
Cryptographic Credentials Stack
Idemix
Cryptographic Credentials Storage
AI-based Assistant User Interface
Tor Network Library
Identity Consolidator (IDC)
Authentication Management
OpenID Connect
Federated Login
fido
FIDO2 Server
AI-based Assistant Back-end
Consent Management (UMA)
Credential Management
Idemix
Identity Repository
Federated login
Identity Provider
OpenID Connect
Federated Login
fido
FIDO2 Server
Cryptographic Credentials Stack
Idemix
Identity Repository
FIDO2, Federated login
FIDO2, Federated login
Idemix Cryptographic Credentials (ABAC)

Figure 1: INCOGNITO Reference Architecture

it into a single trusted identity. Once the user's information is transformed into identity attributes within the IdC, it acts as the intermediary between the user and Identity or SPs. It enables and guarantees the establishment of secure communication between the user and service providers (SPs), creating cryptographic credentials to authenticate the user at different SPs and hosting servers like FIDO2.0 for secure authentication or UMA for user-based consent management.

The IdC provides users with the ability to oversee their personal identity using modules like the Account Management Module or Identity Management Module. This grants users the opportunity to strengthen the security of their accounts and exert authority over the IdC's administration of their identity, which includes the utilization of the UMA server. Users have the ability to establish policies that hold greater importance than the assurance level determined by the IdC when integrating information acquired from different IdPs. Additionally, the IdC provides users access to an AI-based assistant, which assists users in identity management and disclosure. The AI-based assistant possesses the necessary expertise to alert users about potential risks and enable them to take appropriate actions to protect their privacy and security. Moreover, the IdC employs two layers of security: the Tor Network facilitates communication between users and SPs, enhancing anonymity, while blockchain technology logs user interactions with online services such as the IdC or SPs.

Service Provider: To achieve widespread adoption of the INCOGNITO platform by multiple SPs, our focus is on making essential changes that can be easily adopted with minimal modifications. SPs, which are already available in the market and utilized by consumers, often have specific requirements that users must meet to access their services. Users do not directly share their identity information with SPs. Instead, the OIDC protocol combined with a cryptographic credentials stack like Idemix is employed to deliver the necessary attribute(s) to the SPs, granting users access to their services. Furthermore, INCOGNITO incorporates a blockchain solution to enhance privacy and security. SPs are integral components of the blockchain network as they operate an endpoint and actively engage in submitting transactions onto the blockchain. This integration ensures that SPs are accountable for their actions within the network's lifecycle.

Decentralized Identity Management (DIM): The blockchain infrastructure of the INCOGNITO platform exhibits specific architectural characteristics. Every participant, including the IdC and SPs, maintains a local instance of the distributed ledger. Notably, the IdC serves as both a central node and a participant within the blockchain network. Concurrently, the SPs function as network constituents by running endpoints and actively engaging in transaction submission. The logged information within the blockchain encompasses several key elements. Firstly, the user's policies, as submitted by the UMA residing on the IdC, are recorded. Additionally, the actions undertaken by the IdPs and the IdC pertaining to the disclosure of users' identity attributes to SPs are documented.

The IdC facilitates this process by relaying pertinent identity attributes to the SPs using access tokens, thereby ensuring privacy preservation. It is important to note that the SPs receive access tokens directly from the user's mobile device, thereby maintaining a communication barrier between the IdC and SPs. The corresponding message, signed by both the sender (IdC) and the receiver (SP), is subsequently recorded in the distributed ledger. Furthermore, the blockchain logs encompass encrypted values of identity attributes, thereby decentralizing the role of IdPs and ensuring the confidentiality of user identities. Only authorized IdPs possess the necessary privileges to write and decrypt data from the blockchain, thus guaranteeing secure access to encrypted attribute information. The established blockchain infrastructure facilitates transparent and secure logging of user interactions, policy management, and the sharing of identity attributes between the IdC, IdPs, and SPs within the INCOGNITO platform.

Tor-enabled: The INCOGNITO platform incorporates the implementation of the Tor Network within the User's Device, utilizing a Tor Network library to introduce an additional layer of security to the Idemix protocol. By employing Tor, the platform mitigates the risks associated with both basic and advanced traffic analysis techniques. This is achieved through the dispersion of user transactions across multiple locations on the Internet, preventing any single point from establishing a connection between the user and their destination. Rather than following a direct route from source to destination, data packets within the Tor network traverse a randomized pathway, passing through various relays that effectively conceal the user's digital footprint. Consequently, no observer at any given point can ascertain the origin or intended recipient of the data.

The process of establishing a private network pathway with Tor involves the gradual construction of an encrypted connection circuit through the network's relays. This circuit is incrementally extended, with each relay solely aware of the previous relay that transmitted data to it and the subsequent relay to which it transmits data. No individual relay possesses knowledge of the complete data packet path. After a circuit is set up, various types of information can be shared, and a wide range of software programs can be utilized across the Tor network. Due to the restricted visibility of each relay to only one hop within the circuit, both eavesdroppers and compromised relays are unable to exploit traffic analysis methods to link the connection's source and destination.

3.2 INCOGNITO Processes

The initiation of the entire INCOGNITO platform, as it can be observed at Fig. 1, relies on the User-to-Device Authentication block. Every authentication process at Identity or SPs, any updates made by a user regarding their identity at an online service, and any transfer of identity attributes between entities are directly linked to the authentication of the user to their personal device. This mechanism ensures the secure execution of all interactions within the system. INCOGNITO leverages the capabilities offered by modern mobile phones, as outlined in this section. Users interact with their devices through robust and secure authentication mechanisms, such as biometrics (facial recognition, fingerprints), or a personal identification number (PIN). These distinctive user characteristics are transformed into cryptographic keys, which are securely stored on the user's device. To achieve the required security standards, the device incorporates a TEE, which integrates a Trusted Operating System with hardware components, working collaboratively to fulfill the necessary security prerequisites. The primary focus is placed on guaranteeing that the user's characteristics remain confined to their device, even in the event of an OS failure. Atop the TEE, a Cryptographic Credential Storage (CCS) operates, serving as the repository for the generated keys on the user's device. INCOGNITO facilitates user authentication to their device through roaming authenticators, utilizing the usability provided by the FIDO2.0 protocol. These authenticators can be connected to the user's device as needed, and the user interacts with them to verify their ownership. The fundamental security requirement for the User-to-Device Authentication in INCOGNITO revolves around ensuring that the user's characteristics never leave their device and that any subsequent information transfer is authorized through cryptographic protocols utilizing the cryptographic keys derived from the user's characteristics. By adhering to this approach, the security of the user's physical attributes is upheld, mitigating the risk of malicious exploitation of personal physical data.

We ensure the achievement of QA within the INCOGNITO platform, which guarantees that online services possess only a pseudonym rather than any personally identifiable information about the user. To accomplish this, we incorporate federated login solutions such as OIDC in conjunction with anonymous credential systems like Idemix. This integration enables online services to receive a limited subset of the user's identity attributes, ensuring that the user meets the qualifications necessary to access a particular resource. Cryptographic credentials are utilized by the user to demonstrate ownership of an identity attribute. These cryptographic credentials are then submitted to the IdP, which employs the corresponding cryptographic credential stack (Idemix). Ultimately, the identity attributes are conveyed to the SP using OIDC. Simultaneously, the user's anonymity is maintained, thus successfully realizing the concept of QA. Without this solution, users would be compelled to disclose their complete identity to SPs in order to utilize desired services. To enhance anonymity during the communication of identity attributes, the TOR network is employed. This utilization occurs when cryptographic protocol stacks like Idemix are employed to facilitate communication between users and the IdC.

User-based consent management forms a fundamental cornerstone of the INCOGNITO platform, as it aims to provide enhanced security and privacy to its users. INCOGNITO not only safeguards identity transfers and protects users' privacy but also empowers users to exercise greater control and flexibility over their shared identity attributes. The underlying protocol enabling user-based consent management in INCOGNITO is UMA. This protocol operates in conjunction with an authorization server, responsible for managing user preferences pertaining to their identity.

UMA allows users to define policies at the authorization server, which are subsequently utilized asynchronously, even in the absence of users' online presence, to grant access to specific identity attributes. These policies offer a broad spectrum of flexibility, enabling users to selectively share certain attributes with specific SPs or create diverse policies governing different identity attributes with varying levels of access. Through UMA, users reclaim control over their identities and can restrict the control of the IdC over their personal identity attributes. For instance, if the IdC possesses the capability to share a user's name, age, and address with a particular IdP based on a level of trust, the user can restrict the IdC to only disclose their age to that specific IdP. Additionally, the INCOGNITO project incorporates an AI-based assistant to guide users in managing their identities, providing relevant knowledge about information disclosure requirements to specific entities and associated risks. As a result, individuals have the ability to exert control over identity administration by providing permission for the release of desired identity characteristics. The interaction between users and the AI-powered assistant is made easy through an incredibly user-friendly User Interface, which can be accessed via a web interface or a mobile app. Furthermore, UMA is enriched by integration with ABAC, enabling fine-grained authorization capable of handling dynamic and complex access relationship scenarios.

4 USE CASES

In order to prove the efficiency and usefulness of the privacy and security preserving methods that the INCOGNITO platform offers, two use cases are designed to be deployed as pilots.

4.1 Online Multimedia Content Sharing

The primary objective of this use case is to devise and implement an infrastructure capable of issuing and validating cryptographic credentials at the behest of Online Services, regardless of whether they support such software stacks or not. This functionality empowers Online Services to receive a granular subset of the user's identity attributes, ensuring that the user possesses the necessary qualifications to access a specific resource. Moreover, the use case showcases the practicality and viability of the privacy-preserving QA approach. Additionally, it endeavors to facilitate users' utilization of the Identity Acquisition and Management platform, facilitating swift and secure acquisition of identity attributes from Physical ID documents and Online Identities. Notably, users are afforded the flexibility to store the acquired and verified identity attributes either within a centralized entity or a distributed system based on blockchain technology.

This use case entails several key steps. Firstly, the user registered an account on the INCOGNITO Online platform, providing essential information such as their name, surname, and email. Subsequently, the user went through an email verification process. To augment the user's identity attributes, two modules came into play: the Online Identity Acquisition Module and the Physical Identity Acquisition Module. Through the former, users retrieved identity attributes from an Online IdP, while the latter enabled data retrieval from NFC-enabled documents like National ID cards. In the context of this use case, attributes such as age and financial status become vital for accessing online multimedia content sharing services, while compliance with legal requirements necessitates the inclusion of a National ID number or equivalent identifier. The collected data encompasses a range of information, including first name, surname, email, birthday, gender, National ID number, phone number, address, postal code, city, country, and financial status. Leveraging cryptographic credentials facilitated by software stacks like Idemix, the online multimedia content sharing service can receive a fine-grained subset of the user's identity attributes, effectively ensuring their eligibility for resource access while preserving user anonymity, thus embodying the desired concept of QA.

4.2 Fake News Dissemination

The aim in this use case is to detect and identify bots or fraudulent users within Online Social Networks. Through the implementation of INCOGNITO, users have the means to substantiate their humanity when accessing online services. Furthermore, they can provide evidence of their credibility, such as by disclosing their profession, and showcase a positive reputation acquired through previous posts, all encapsulated as relevant attributes. By incorporating these mechanisms, the use case strives to enhance the trustworthiness and reliability of online interactions, particularly in combating the spread of misinformation.

More specifically, the user initiates registration on the INCOGNITO Online platform, providing their name, surname, and email, followed by email verification. Just as in the previous use case, the Online Identity Acquisition Module and Physical Identity Acquisition Module serve to enrich the user's identity attributes. Users can retrieve attributes from an Online IdP or NFC-enabled documents like National ID cards. In this case, attributes like profession assume significance to enhance the user's reputation. The collected data includes first name, surname, email, birthday, gender, National ID number, and phone number. Notably, specific identity attributes can accrue reputation based on evaluations by other users, with such transactions recorded in a blockchain stack. This mechanism empowers users to provide evidence supporting the veracity of particular identity attributes.

5 RELATED WORK

Several EU-funded research projects have focused on privacy, security, and identity management, addressing similar challenges to the INCOGNITO framework. PRISMACLOUD [5] (Privacy and Security Maintaining Services in the Cloud) was an EU-funded project that aimed to develop a comprehensive framework for privacy-enhancing cloud services. The project recognized the privacy concerns associated with cloud computing and focused on protecting users' data and ensuring their privacy in cloud-based environments. PRISMACLOUD introduced innovative techniques and cryptographic mechanisms to preserve privacy while allowing secure data processing and storage in the cloud. The project addressed challenges such as secure data sharing, data privacy preservation, and secure computation in the cloud, making significant contributions to the field of privacy-preserving cloud services.

The ARIES [6] (reliAble euRopean Identity EcoSystem) project aimed to establish a comprehensive framework for a reliable e-identity ecosystem, focusing on enhancing identity-based services while ensuring the highest levels of security and privacy. The project leveraged strong eID documents and biometrics to prevent identity theft and associated crimes in both physical and virtual domains. By univocally linking derived virtual and mobile IDs to citizens' biometric features, ARIES increased the level of identity assurance during credential issuance and authentication processes. The project emphasized data protection standards to provide privacy-preserving features, addressing European-specific concerns and supporting law enforcement efforts. ARIES encompassed use case demonstrators, such as secure eCommerce and identity virtualization for secure travel, to showcase the practical application of the virtual ID ecosystem and its positive socio-economic impacts.

The PANORAMIX [7] (Privacy and Accountability in Networks via Optimized Randomized Mix-nets) project focused on the development of a multipurpose infrastructure for privacy-preserving communications based on mix-networks. Mix-nets ensured the confidentiality of communication content and obscured the identities of senders and receivers through cryptographic relays. The project's

[5] https://cordis.europa.eu/project/id/644962
[6] https://cordis.europa.eu/project/id/700085
[7] https://cordis.europa.eu/project/id/653497

objectives included building a European mix-net infrastructure, applying the infrastructure to private electronic voting protocols, privacy-aware cloud data-handling, and privacy-preserving messaging. PANORAMIX aimed to provide an open-source codebase and infrastructure tailored to European needs, enabling secure and privacy-respecting applications across various domains. By fostering collaboration between academia, civil society, and industry, the project brought together expertise in privacy technologies and industry partners with a focus on high-impact applications.

6 CONCLUSION

In conclusion, this paper presented the INCOGNITO framework, which addresses the challenges of privacy and security in online identity management. The proposed framework offers a solution by integrating various components and processes to ensure the privacy-preserving acquisition and management of identity attributes. The architecture of INCOGNITO, combined with technologies such as cryptographic credentials, Tor network, and blockchain, enhances the security and anonymity of user interactions with online SPs. The use cases of online multimedia content sharing and fake news dissemination demonstrated the practical applicability of the framework. Overall, INCOGNITO provides a promising approach to protect users' privacy while enabling secure and trusted digital interactions.

ACKNOWLEDGMENTS

- INCOGNITO (H2020-MSCA-RISE-2018, GA 824015)
- SECONDO (H2020-MSCA-RISE-2018, GA 823997)

REFERENCES

[1] X. Zhang, M. M. Yadollahi, S. Dadkhah, H. Isah, D.-P. Le, A. A. Ghorbani, Data breach: analysis, countermeasures and challenges, International Journal of Information and Computer Security 19 (3-4) (2022) 402–442.

[2] D. Chen, M. M. Chowdhury, S. Latif, Data breaches in corporate setting, in: 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), IEEE, 2021, pp. 01–06.

[3] L. I. Labrecque, E. Markos, K. Swani, P. Peña, When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach, Journal of Business Research 135 (2021) 559–571.

[4] Z. Alkhalil, C. Hewage, L. Nawaf, I. Khan, Phishing attacks: A recent comprehensive study and a new anatomy, Frontiers in Computer Science 3 (2021) 563060.

[5] A. Karale, The challenges of iot addressing security, ethics, privacy, and laws, Internet of Things 15 (2021) 100420.

[6] Z. Wu, G. Li, S. Shen, X. Lian, E. Chen, G. Xu, Constructing dummy query sequences to protect location privacy and query privacy in location-based services, World Wide Web 24 (2021) 25–49.

[7] L. Hanzlik, D. Slamanig, With a little help from my friends: Constructing practical anonymous credentials, in: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, 2021, pp. 2004–2023.

[8] M. P. Machulak, E. L. Maler, D. Catalano, A. Van Moorsel, User-managed access to web resources, in: Proceedings of the 6th ACM workshop on Digital identity management, 2010, pp. 35–44.

[9] M. Pilkington, Blockchain technology: principles and applications, in: Research handbook on digital transformations, Edward Elgar Publishing, 2016, pp. 225–253.

[10] H. Li, L. Yu, W. He, The impact of gdpr on global technology development (2019).

[11] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, J. Voas, Attribute-based access control, Computer 48 (2) (2015) 85–88.