Available online at website: https://jurnal.iaii.or.id/index.php/RESTI

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 10 No. 2 (2026) 537 - 547 e-ISSN: 2580-0760

On-Device Hybrid Access Control for Personal Data Sharing using Sensitivity and Trust Parameters

Geocey Shejy[1*], Pallavi Mangrulkar[2]
[1]Department of Computer Engineering, Ramrao Adik Institute of Technology D. Y. Patil University, Nerul, India
[2]Department of Computer Engineering, Mukesh Patel School of Technology, NMIMS University, Mumbai, India
geocey@gmail.com

Abstract

Protection of Personally Identifiable Information (PII) is challenging for organisations. Access to sensitive resources, ie, databases and files, can be controlled and restricted by the Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC) and other access control models defined at the organisational level. This work proposes a lightweight on-device PII access control model based on the principle of preserving privacy at the source of data generation. The set of data shared by the user is converted into objects, and the object is treated as a resource to which RBAC, ABAC and Hybrid access controls are applied. Coarse-level access to a set of PII information, in the form of PII objects, on a user device is implemented using RBAC, while fine-grained access is defined and performed using ABAC. Hybrid access, which supports object and attribute-level access control using sensitivity, trust, and Time to Live (TTL) environment, was evaluated. The RBAC, ABAC, and Hybrid models are lightweight, highly reliable, scalable, and efficient to implement on user devices. Three models were tested for scalability up to 1000 objects and a corresponding number of attributes. This model mitigates the risk of PII exposure posed by the data-collecting organisation and enhances user consent for PII sharing.

Keywords: ABAC; personally identifiable information; PII; RBAC; sensitivity; trust

How to Cite: [Geocey Shejy and Pallavi Mangrulkar, "On-Device Hybrid Access Control for Personal Data Sharing using Sensitivity and Trust Parameters ", *J. RESTI (Rekayasa Sist. Teknol. Inf.)* , vol. 10, no. 2, pp. 537 - 547, May 2026.
Permalink/DOI: https://doi.org/10.29207/resti.v10i2.7522

Received: January 24, 2026
Accepted: April 12, 2026
Available Online: May 2, 2026

This is an open-access article under the CC BY 4.0 License
Published by Ikatan Ahli Informatika Indonesia

1. Introduction

On-device mechanisms for protecting personal data are more favourable from the data owner's perspective, as they ensure that the individual retains sole authority and control over their data. In this article, an individual who discloses and can be identified through personal attributes is referred to as the Data Owner, and the entities or organisations that gather such personal information are referred to as Data Collectors. When sharing data, the data owner is concerned with whom the data is being released to, the purpose of the release, the amount of personally sensitive information disclosed, and the duration for which the data will be available. The sharing of personal data creates mutual benefits for both data owners and data collectors. Since data sharing fuels online services that have become integral to daily life, this scenario necessitates trustworthy interactions between the two parties, reinforced by personal data protection regulations. Regulations such as the GDPR in Europe, the Australian Privacy Principles, the Digital Personal Data Protection (DPDP) Act, India, and other personal data protection laws worldwide safeguard the rights of data owners over their information throughout its collection, processing, and storage[1-3]. In this work, the sensitivity of personal information is determined solely at the discretion of the data owner. Accordingly, common categories of personal information are explicitly classified into different sensitivity levels, namely: General Information (GI), Quasi-Identifiers (QI), Personally Identifiable Information (PII), and Personal Sensitive Information (PSI). The argument is that even though a single piece of information is not directly PII or PSI, a set of GI or QI will also lead to identification. When a data collector collects a specific amount of data from an individual based on the sensitivity category of information as above, the sum of each attribute's sensitivity is calculated, and sensitivity levels of the set of data are assigned. Each piece of information contributes a fraction to the total sensitivity of the set. 10 personal attributes, such as name (1), age (1), address (2), phone (4), email (4), occupation (1), gender (1), nationality (1), marital status (1), birthdate (3), with varying sensitivity, are considered here for the demonstration and calculation. The number in the

bracket near the attribute is the individual attribute sensitivity considered in this work.

The work examines three access control mechanisms: Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and hybrid access control. For RBAC PII access, the user is the data owner. Roles to collect PII are determined by the trust the data owner places in the data collector. Based on this trust, access is permitted or denied. For the ABAC PII access, online services or organisations request PII in attribute level. Decisions on access to specific attributes are based on the sensitivity of the attribute. Roles are based on the trust of the service provider or organisation. The hybrid model combines RBAC and ABAC to provide multi-granular access to PII. An object-level is a collection of PII and has a higher level of abstraction, whereas at the attribute level, the abstraction becomes more detailed and lower-level. A hybrid access control model can fine-tune PII access depending on the consent of the data owner, the sensitivity of the shared PII, the trust in the data collector, and the required duration for which the sharing of a specific PII needs to continue.

The models were implemented and tested for scaling and efficiency in terms of CPU and memory utilisation. RBAC, ABAC, and hybrid models are found to be successful lightweight on-device mechanisms for PII access. The hybrid model provides multi-granular access control. When an organisation collect data, if multiple personal information items are required, object-level granularity is used. If the access is aimed at a single piece of information, attribute-level granularity is the option. Apart from the user, role, and permissions of access, the duration of data sharing also applies in the hybrid model. The sensitivity of shared data has an inverse relationship to the Time to Live (TTL) of that sharing, either at the object level or attribute level. If the data owner shares a highly sensitive set of data or a single attribute, the TTL of sharing is less in comparison to the sharing of a less sensitive one. For this purpose, TTL is kept as an attribute environment in the hybrid model.

Protecting data at the source itself reduces the risk of legal complications. Access to data illegally questions the rights and freedom of expression [4-5]. Securing data at the source exists in many algorithms. This idea is rooted in the foundational work of Rivest et al. on digital signatures and public-key cryptosystems [6]. End-to-end encryption techniques help secure the data at its source, transmission, and at the receiver end [7], [8]. This work entrusts individuals with full rights over their data, ensuring that any access by data collectors remains transparent to the data owner. Furthermore, the shared personal data is recognised as having varying levels of sensitivity. Some attributes of the shared data reveal the identity of the data owner, which is Personally Identifiable Information (PII). PII carries various levels of sensitivity. The PII becomes sensitive depending on how accurate inferences one can draw about a person from the available personal data. Many customers are concerned about sharing their data online with firms or organisations to use online services [9], [10]. On the other hand, data from consumers is essential for the organisation. This scenario requires a mutually beneficial outcome for both the consumer, as the data owner, and the service providers, as the data collectors. The trust between the data owner and the data collector is the pivot for successful and legitimate relations between these parties. While data privacy laws seek to regulate these relationships effectively, significant technical challenges persist. PII may be transmitted to data collectors either with or without the awareness of the data owner. For example, mobile Android applications lead to PII exposure, which is unknown to the data owner[11] . Another set of data sharing is legitimately obeying personal data protection laws [12]. When personal data is collected with the explicit consent of the data owner, the trade of the data to avail of a service is included. For instance, in the banking sector, such exchanges are intended not only to generate profit but also to foster trust between the bank and its customers [13-14]. Since online banking services manage highly sensitive data, the risks associated with handling such information are considerably high. While the sharing and collection of personal data are essential for enabling transactions across services, these exchanges necessitate the growth of trust between financial institutions and their customers.

Despite the legal safeguards provided by various data protection acts, widespread incidents of PII leakage worldwide have led to a decline in data owners' trust in data collectors [15]. For banking and financial institutions, such leakages act as a double-edged sword, posing risks not only to data owners but also to data collectors. Such leaks result in financial loss and psychological distress for data owners, while financial institutions face economic repercussions and the challenge of restoring the lost trust. Data owners face constant insecurity, often compelled to compromise their PII to access services, while data collectors struggle to retain their customer base through disproportionate efforts. In light of online resources on consumer safety in financial services, we observe that many governmental bodies promote data owners' control over their data [16]. Most businesses are willing to prioritise privacy to improve customer trust and loyalty. On the other hand, consumers feel the risk of sharing personal data outweighs the benefits they receive, and also, the data sharing is not transparent [17]. These discussions highlight the need for a system that enables customers and financial institutions to operate in an environment of mutual trust. The literature provides multiple definitions of trust between digital entities [18]. The definitions change depending on the application and technology. In any transaction, the entities involved rely on mutual trust, with the expectation that each party will act in alignment with the other's expectations, mutually. This work proposes

a mutually trusted environment designed to uphold these expectations.

The work in the proposal uses RBAC-based access control policies on the user device for object-level access to PII, and for attribute-level PII, it uses ABAC access control and also proposes a Hybrid access model for varying access possibilities. Many access control models available in the literature suffer from the drawback of requiring third-party involvement in the encryption and decryption process, leading to a strong reliance on the trustworthiness of the administering third party [19]. Attribute-Based Access Control (ABAC), a logical access control mechanism, helps in data sharing by controlling the shared information [20]. An object or resource in an ABAC is an entity that is protected from unauthorised access. The subject or requester is the entity requesting to operate on the object. ABAC helps security policy enforcement in a flexible, granular, and dynamic way. An update in policy is possible only after evaluating several policies [21]. This makes the administration of this model complex. Role-based access control (RBAC) is widely implemented because it is easily manageable, but lacks granular access control and flexibility like ABAC [22]. Integrating multiple access control models allows the strengths of different approaches to be combined into a single unified framework. Meta-policy is an approach that helps to combine policies from many access models. ABAC is applicable in scenarios where fine-grained and dynamic control over access rights is needed. It's often used in collaborative environments, cloud computing, and scenarios with complex authorization requirements.

Attribute-based encryption (ABE)is another security model that uses attributes to control resource access [23]. ABE is used in scenarios where data confidentiality is a primary concern. ABE enables more flexible, dynamic attribute-based access control. It allows data owners to encrypt data by attribute, so only users with matching attributes can decrypt and access it. ABE provides flexibility through a level of selective disclosure. It enables data owners to specify conditions under which encrypted data can be decrypted, based on the attributes of the requesting entity. ABE helps secure data sharing by allowing data owners to control who can access their data based on specific attributes, providing a more granular approach to data protection. Identity-Based Encryption (IBE) uses the recipient's identity as a key to encrypt a message, and the decryption key is derived from the recipient's identity [24]. The identities are properties or attributes of the recipient, like name, address, and social security number, which help to identify the recipient and permit or deny access to any sensitive resource of the organization.

Fuzzy Identity-Based encryption (Fuzzy IBE) views identity as a set of descriptive attributes instead of viewing it as a string of characters [25]. Fuzzy IBE helps to apply Attribute-Based Encryption, ABE. In ABE, the accessibility of a resource can be restricted to users who satisfy a certain set of attributes, and if 'k' attributes overlap, that recipient can access the resource. ABE-based encryption with more fine-grained access control is introduced in Key Policy Attribute-Based Encryption (KP-ABE) [26]. The decryption capability of users is controlled with private keys and labelled attributes of the ciphertext. It uses a tree access structure for each private key. This tree access structure keeps attributes as leaf nodes. It specifies the type of ciphertext the key can decrypt, where the ciphertext is labelled with a set of descriptive attributes. A user can decrypt a ciphertext if the attributes associated with a ciphertext satisfy the key's access structure. IBE, Fuzzy IBE, and ABE systems offer encryption based on attributes. Access control is not a major focus of these systems. In Fuzzy IBE, the data provider decides the way of sharing and is expressed with a predicate. The user of the data can use the data if and only if they satisfy the predicates by the data provider through the attributes of identity. In CP-ABE, data is encrypted with attributes, and access policies are defined in terms of these attributes. Users are given secret keys that correspond to their attributes, and they can decrypt data if their set of attributes satisfies the access policy associated with that data.

CP-ABE is an extension of Attribute-Based Encryption (ABE). CP-ABE allows data encryption with access policies specified in the ciphertext. In a typical CP-ABE system, the access policy defines attributes a user must have to decrypt a particular ciphertext. The dynamic aspect comes into play when attributes change over time or new users with different attribute sets need access. CP-ABE allow updates and modifications to the access policies without re-encrypting the data.

The access control model discussed above works as server-side controls. User-defined access control for on-device personal data is not present in the explained models. The work in this article uses RBAC and ABAC access control models for the access of personal data from the user device.

2. Methods

Access control models help control access to data resources based on the assigned roles of users. Traditionally, it is used at the organisational level, as shown in Figure 1. A user can be anyone working in the organisation. For example, in a banking context, a user can be any individual within the organisation assigned a specific role, such as Manager, Accountant, Auditor, or similar positions. The data resources, such as files and databases, are accessible based on permission levels.

In the proposed work, the users are organisations and the resources are users' personal information. Personal information is treated as a collection of many attributes related to a person who owns the data, and it refers to a person object. When one organisation collects data, it

can collect the data as an object or an attribute using RBAC or ABAC models, respectively.

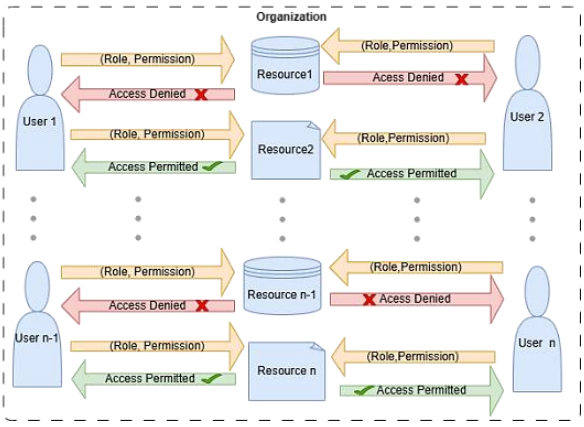


Figure 1. Working of access control models

The proposed model assumes that both the data owner and the data collectors are law-abiding, and both work together in mutual trust. The framework serves as a supporting system for such entities, ensuring they are not at risk of violating privacy laws. Personally Identifiable Information (PII) is formally defined as: "Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Single information or a collection of it leads to identifying a person; this quantifies the sensitivity related to that data or data collection. If *PII_1* is a set of data related to a user and is collected by an organization (Equation 1), then,

$$PII_1 = \{a_1 s_1, a_2 s_2, \ldots\ldots a_n s_n\} \quad (1)$$

Here, a_1, a_2, and a_n are attribute values released by the user with sensitivity s_1, s_2, s_n, respectively.

Then, the sensitivity associated with the release of PII_1 is as shown in Equation 2.

$$s_{PII1} = s_1 + s_2 + \cdots + s_n \quad (2)$$
$$= \sum_{i=1}^{n} s_i$$

Sensitivity associated with the release of PII_1,s_{PII1} the sum of individual sensitivity.

Here, s_{PII1} sensitivity associated with PII_1, which is the sum of individual attribute sensitivities.

Figure 2 explains the working of the access control models in varying level of granularity. There can be multiple data releases like this by one person for multiple organisations. A person's attributes and attribute values are tied together as an object, and access control policies are set for each object. In other words, for each release to a data collector, the data owner can impose access rules.

All sets of attributes form an object, and access to the object is controlled by Role-Based Access (RBAC). Access to the attribute level is controlled by Attribute-Based Access Control (ABAC). The following section discusses the working of RBAC and ABAC.

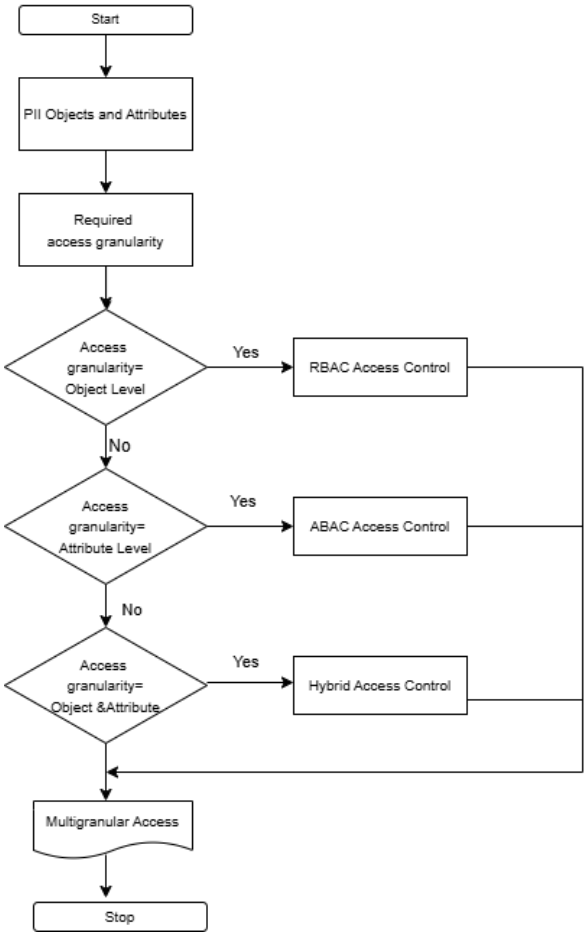


Figure 2. Varied granularity access-controlled sharing of PII

To test the scalability of the proposed model synthetic data set is generated using python script. For the RBAC access model, 1000 objects were tested, and for the ABAC model, up to 1000 attributes were tested. The Hybrid model is tested for 1000 objects, and each object has 10 attributes

2.1 RBAC model for PII object access from user the device

Role-based access models are simple and less granular. It is used here to access multiple PIIs from the data owners as a collection. The RBAC model for PII access defines rules of access to objects. Sensitivity of the object and trust of the organisation are the decision-making parameters of access. Objects that are a collection of many attributes use the collective sensitivity of all attributes. The data-collecting organisations are given some predefined trust values. Figure 3 explains the use of RBAC in object-level access, based on sensitivity and trust. This model of access is simple and lightweight.

Users release personal information with varying levels of sensitivity; in this work, each piece of personal information is considered PII because a combination of

information can lead to a person's identification. All information collected at the object management layer as attributes is converted into a collection, an object. Three PII releases done by the user are shown in Figure 1. Rel_1, Rel_2, and Rel3 have a different set of attribute releases, and due to the number and the individual sensitivity of the attributes in the collection, Object-1 is considered with high sensitivity. Object-2 has medium sensitivity, and Object-3, with only two attributes, has low sensitivity.

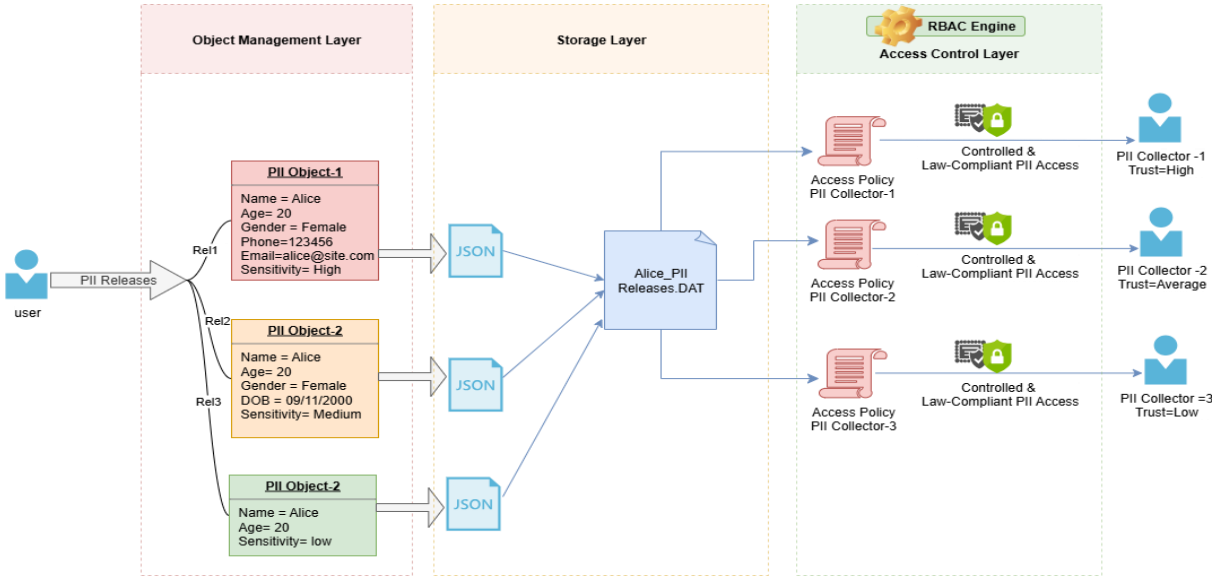


Figure 3. The Role-Based Access Control model gives Object-level granularity

The storage layer converts objects into a file after they are serialised into JSON format. This storage is lightweight in terms of memory usage. Role-based access rules are defined and implemented at ACL. The parameters that decide access are the sensitivity of the object and the trust of the data-collecting organisation. Three levels of trust are used here. Collectors 1, 2, and 3 have high, average, and low trust, respectively. RBAC access rules are listed.

RBAC rules for PII Access:

1. ***U:*** *Data collector Set (Users of PII): {Org1, Org2, Org3}*
2. ***P:*** *Accessibility Permission PII Object: {Access, Deny}*
3. ***R:*** *Role-Based on Trust: {Highly Trusted, Average Trusted, Least Trusted}*
4. ***UA:*** *User Assignments: {(Org1, Highly Trusted), (Org2,Average Trusted), (Org3, Least Trusted)}*
5. ***PA:*** *Permission Assignments: {Org1(Access All PII Objects), Org2(Access PII Object with < threshold of sensitivity), Org3(Access PII Object with low Sensitivity)}*

Table 1 shows the User, Role, Permissions, and Resources utilised in the RBAC model for PII access. The users are organisations, and their trust is the role defined. Resources are objects with varying levels of sensitivity, viz, highly sensitive, medium sensitive, and very low sensitive. The access permission matrix for RBAC is shown in Table 2. If the user Organisation is highly trusted, then the user is permitted to access all objects or highly sensitive records. Average trust organisations access objects with a sensitivity lower than a threshold sensitivity, i.e., medium-sensitive records. The least trusted organisations have access only to records or objects of very low sensitivity.

Table 1. Role-Based Access Control for PII access: User, Role, Permission and Resource

User	Role	Permissions	Resources
Organization 1	Highly Trusted	All Object access	PII records: Highly Sensitive
Organization 2	Average Trust	Access to Objects < threshold sensitivity	PII-Records: medium Sensitive
Organization 3	Least Trust	Access to very low sensitive Objects	PII-Records are very low sensitive

Table 2. Role-Based Access Control- Access Permission Matrix

User/Role	Object sensitivity greater than Threshold Sensitivity	Object sensitivity lesser than Threshold Sensitivity	Object with Lowest Sensitivity
Organisation1/ Highly Trusted	Full access	Full access	Full access
Organization2/ Average Trust	No access	No access	Can access
Organization3/ Least Trust	No access	No access	Can access

The object-level access using the RBAC access control model in PII on-device is applicable if the user and the organisation have already entered into a consent for data sharing and collection, which is a legitimate process. For example, in the scenario of a sanctioned loan from the bank, the PII shared remains the same as long as there is a change in requirements. If there is a

requirement for additional PII by the organisation or if a user is interested in sharing a single PII, increased granularity on access to information is mandatory. The RBAC model for PII access is unable to address this situation. The ABAC model for PII access is proposed in the following session to address scenarios that demand attribute-level PII access.

2.2 ABAC Model for PII access from the user device

The ABAC Model for PII access is illustrated in Figure 4. This model addresses the PII at the attribute level. Ten attributes with varying sensitivities are considered in the work. The variable *s* and the associated values show attribute sensitivity. Each attribute in this model is a resource. To make it possible, individual attributes are treated as objects and are serialised for storage purposes. These attribute objects can be accessed by the organisation based on ABAC access control rules. ABAC access sets comprise subjects, objects, permissions and attribute values. These definitions and sample ABAC rules for ABAC access are:

*1. **S:** Subject- Entities Requesting Access to PII attributes: {Org1, Org2, Org3}*

*2. **O:** Object-Resources being accessed with associated sensitivity value:*

{Obj1.Name, Obj1.Age, Obj1.Address, Obj1.Phone, Obj1.Email, Obj1.Occupation,

Obj1.Gender, Obj2.Nationality, Obj1.Married, Obj1.DOB}

*3. **A:** Action: {Permit access, Deny Access}*

*4. **R:** Trust Attribute value: {Highly Trusted, Average Trusted, Least Trusted}*Sample rules

Here, Attribute 1 is considered highly sensitive.

1. Access (org1, Attribute1) is permitted if {org1.trust = Highly Trusted}

2. Access (org2, Attribute1) is denied if {org2.Average Trusted}

3. Access (org3, Attribute1) is denied if {org2.Least Trusted}

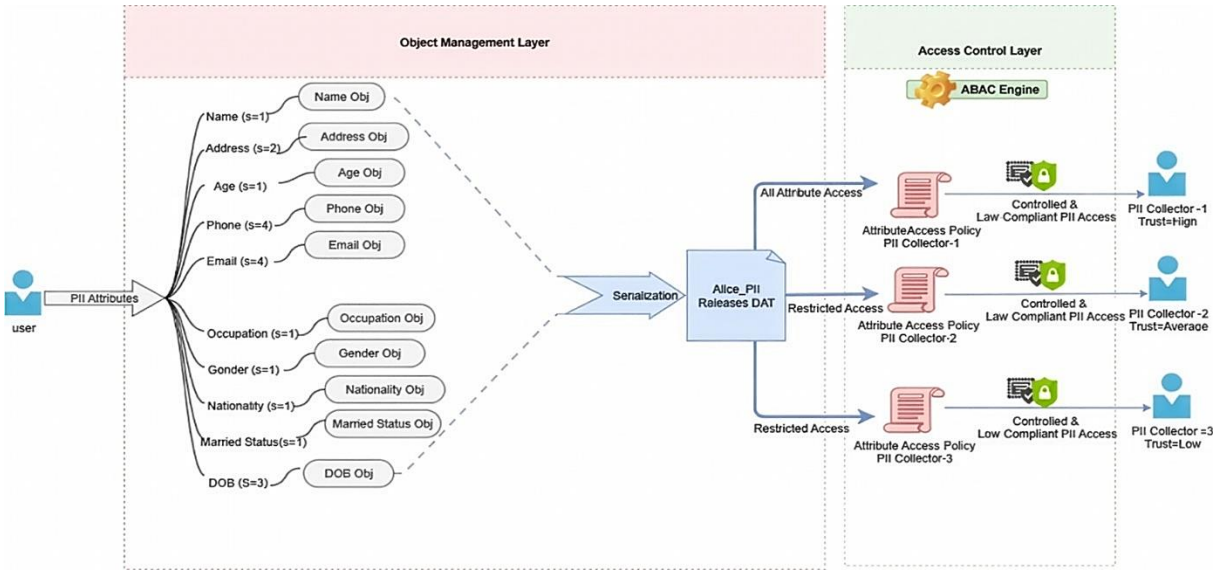


Figure 4. Attribute-Based Access Control model with Attribute-level granularity

Table 3 is the ABAC PII Attribute Access permission matrix. It shows the access possibilities of a specific attribute by the user and their roles. In the ABAC, PII access, the users are organisations that access the attribute, and the individual PII of the data owner is the resource. Sensitivity of the attribute and trust of the organisation are the key parameters for the decision on attribute access. Threshold sensitivities are set to control access.

Table 3. PII Attribute Access Permission matrix for Attribute-Based Access Control

User/ Role	Name (s=1)	Age (s=1)	Address (s=2)	Phone (s=4)	Email (s=4)	Occupation (s=1)	Gender (s=1)	Nationality (s=1)	Married (s=1)	DOB (s=3)
Org1/ Highly Trusted	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Org2/ Average Trusted	yes	yes	yes	no	no	yes	yes	yes	yes	no
Org2/ Least Trusted	yes	yes	no	no	no	yes	yes	yes	yes	no

The attributes, with *s=5* or *s=4*, are highly sensitive and are accessible only to *Highly Trusted* organisations, and not accessible to *Average and Least Trusted* ones. *A highly trusted* organisation has access to all attributes. When *s=4 or s=3, Highly Trusted and Average Trusted* organisations are permitted to access, but *Least Trusted* organisations are denied access. *The Least Trusted* organisation can access only attributes with *s=1* sensitivity. The sample ABAC rules given are based on a highly sensitive single attribute, with access possibilities for different user roles.

2.3 On-Device Hybrid PII Access Control Model

The two models, the RBAC model for PII object-level access and the ABAC model for PII attribute-level access, provide PII access in two different levels of granularity. These models do not handle the Time To Live (TTL) of attributes or objects, and lack flexibility in granularity. TTL is an environmental parameter that decides the duration of the sharing time existing between the data owner and the data collector. TTL is applicable for both the object and attribute levels and is dynamic in nature. The reason for introducing TTL is that a highly sensitive shared PII (Object or attribute) is not required to continue in an accessible state, even though the organisation is highly trusted. The sharing must terminate or undergo an update once the need for the existing sharing is satisfied. To enhance the access control with improved granular behaviour and TTL, a hybrid access control model is proposed in the work. Figure 5 explains the working of the hybrid access model for PII access on-device.

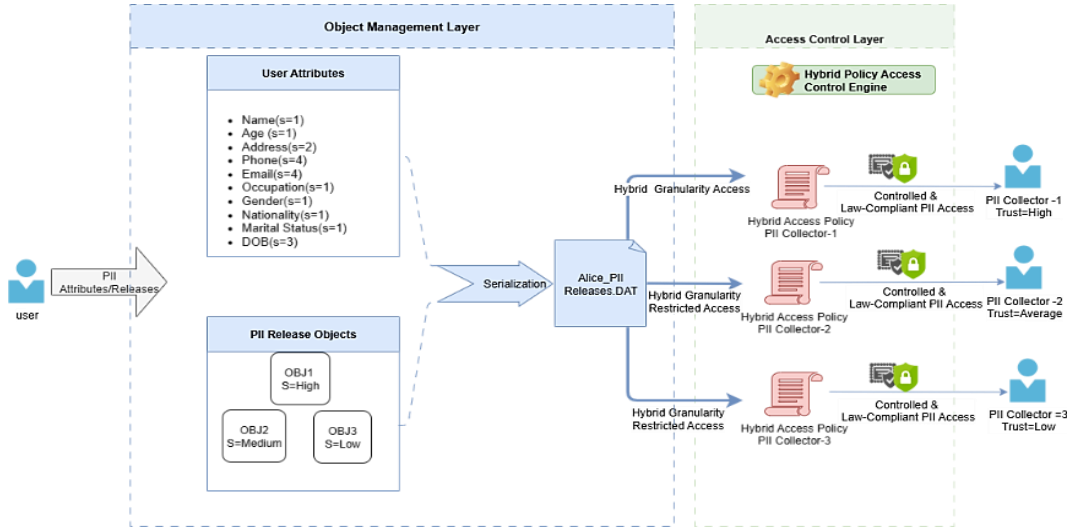


Figure 5. Hybrid Access control model with Object-level and Attribute-level granularity

Object Management Layer manages objects of two different granularities. Objects exist as a collection of multiple attributes, and also as attributes with a single value. As the work in the RBAC and ABAC models, objects are serialised and stored in the hybrid model. ACL engine defines hybrid policy access rules. Hybrid Access Control and sample access rules are given in the next session.

RBAC and ABAC access control models combined to create a Hybrid access model. The hybrid access model defines sets for users, roles, resources, and attributes, and uses set operations to express access rules. For example, an organisation can access a resource if they are in a specific role AND their location attribute matches the resource's location attribute. The Hybrid Access Control model rules offer varied granularity in access, as detailed in the following rules.

1. ***U:*** *The set of all users: {Org1, Org2, Org3}*
2. ***UA:*** *User Attribute Org1: {Org1.trust}*
3. ***R:*** *Roles: {Highly Trusted, Average Trusted, Least Trusted}*
4. ***Res:*** *The set of all resources /Objects: {Obj1(Highly sensitive data set), Obj2(Medium Sensitive Data Set), Obj3(Low sensitive data set)}*
5. ***OAObj1:*** *The set of all attributes obj1 :{Obj1.Name, Obj1.Age, Obj1.Address, Obj1.Phone, Obj1.Email, Obj1.Occupation, Obj1.Gender, Obj2.Nationality, Obj1.Married, Obj1.DOB}*
6. ***Operations:*** *{Permit access of attribute, Deny access of attribute}*
7. ***Aenv:*** *Attribute Environment: {TTL of the object}*
8. ***RPA:*** *Role Permission Assignment: {(Highly Trusted, (access, Obj1)), (Highly Trusted, (access, Ob2)), (Highly Trusted, (access, Obj3)), ((Average Trusted, (access,Obj2)), ((Average Trusted, (access,Obj3)), ((Least Trusted,(access,Obj3)), (Highly Trusted,(Access, Phone)),(Least Trusted, (Deny, Phone)),(Least Trusted,(Access, Name))}*
9. ***URA:*** *User-Role Assignment: {(Org1, Highly Trusted), (Org2, Average Trusted), (Org3, Least Trusted)}*

Sample Hybrid Access Rule: Granularity - Object level

1. **Rule 1:** Permit access to all objects if the organisation is highly trusted and if the TTL =true

2. **Rule 2:** Permit access to only objects 2 and 3 if the organisation is of average trust and TTL=true 3.

3. **Rule 3:** Permit access to only object 3 if the organisation is the least trusted and TTL=true

4. **Rule 4:** Not to permit access to any object if TTL = 0

Sample Hybrid Access Rule: Granularity-Attribute level

1. **Rule 1:** Permit access to all attributes if the organisation is highly trusted, and if the TTL =true

2. **Rule 2:** Permit access to only attributes with sensitivity < 3 if the organisation is of average trust and TTL=true

3. **Rule 3:** Permit access only to the attribute with sensitivity =1 if the organisation is the least trusted and TTL=true

4. **Rule 4:** Not to permit access to any attribute if TTL = 0

Sample rules, both object-level and attribute-level, are controlled by three parameters. Sensitivity of the involved PII, trust of the data collector and TTL based on the sensitivity of the shared object. Including the environmental parameter TTL in the rule improves control over PII access.

All three models are implemented and tested for scalability, memory and CPU utility. Various components and effects of their changes on different parameters of the proposed system are analysed in the results section.

3. Results and Discussions

Figures 6 show the analysis of the RBAC model for PII access on the device. Three access organisations, Org1, Org2, and Org3, are accessing object-level data, and access is either denied or permitted based on two factors: trust in the organisation and the sensitivity of the data. Plot 1 in Figure 6 illustrates the access granted based on Object sensitivity and the organisation's trust. Also, the TTL is lower for objects with higher sensitivity. Org1, with the highest trust among the 3 organisations, is permitted to access all objects regardless of sensitivity. Org2 is permitted to access obj1 and obj3 but not obj2, which has higher sensitivity. Org3, with the least trust, is denied access to all objects. The plot depicts various aspects related to this model.

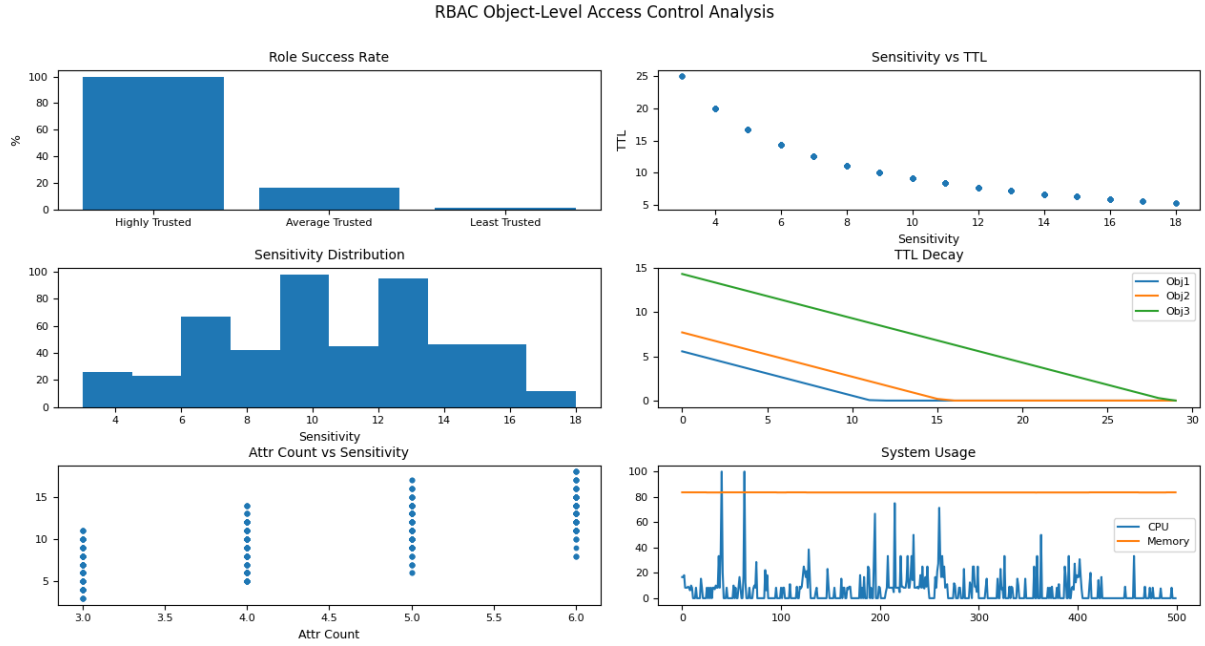


Figure 6. Analysis of Role-Based Access Control for PII access

The role success rate shows a higher number of permitted accesses for Org1, whereas Org2 and Org3 have success rates corresponding to their trust. The sensitivity vs TTL plot describes the inverse relation between these parameters. The TTL decay plot shows that the lifetime of objects is dynamic, and it decays over time. Randomly chosen multiple objects and their TTL decays are shown in the plot. Scalability up to 1000 objects shows that the model is lightweight in terms of storage and CPU utilisation.

ABAC for PII access and its results and analysis are shown in Figure 7. Attribute-level access to the organisation depends on the user's trust. Organisations with a high level of trust value have access to all attributes. Access to highly sensitive attributes for Org2 is denied.

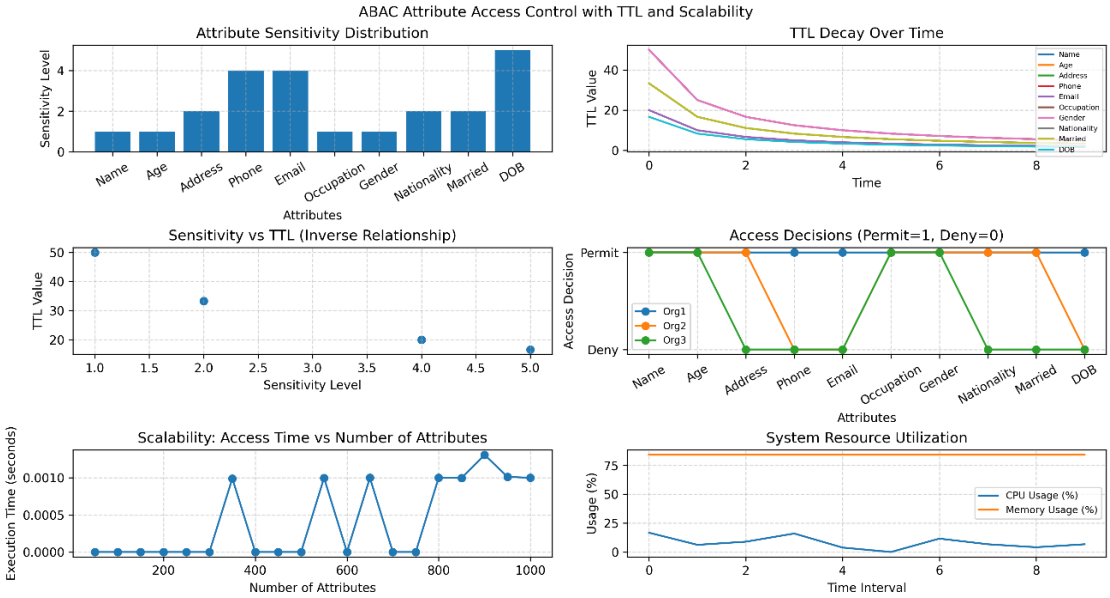


Figure 7. Analysis of Attribute-Based Access Control for PII Access

The analysis plots are showing parameters based on attributes. Individual attributes and sensitivity are plotted in the Attribute sensitivity plot. Scalability up to 1000 attributes belonging to a single person, showing a maximum of 0.0010 seconds of accessibility. Also, memory and CPU utilisation are minimal for the ABAC model for PII attribute-level access. Thus, the model also does not burden the device.

The access control obtained by the Hybrid access model is shown in Figure 8. The hybrid access permits two levels of access granularity: object-level access granularity for Org1, and attribute-level access granularity for the same organisation. These accesses are possible only if the Org1 is in the trust of the user,else access will be denied.First plot shows this scenario. Highly trusted organisations are in a high success rate of data access and least trusted is in a low success.

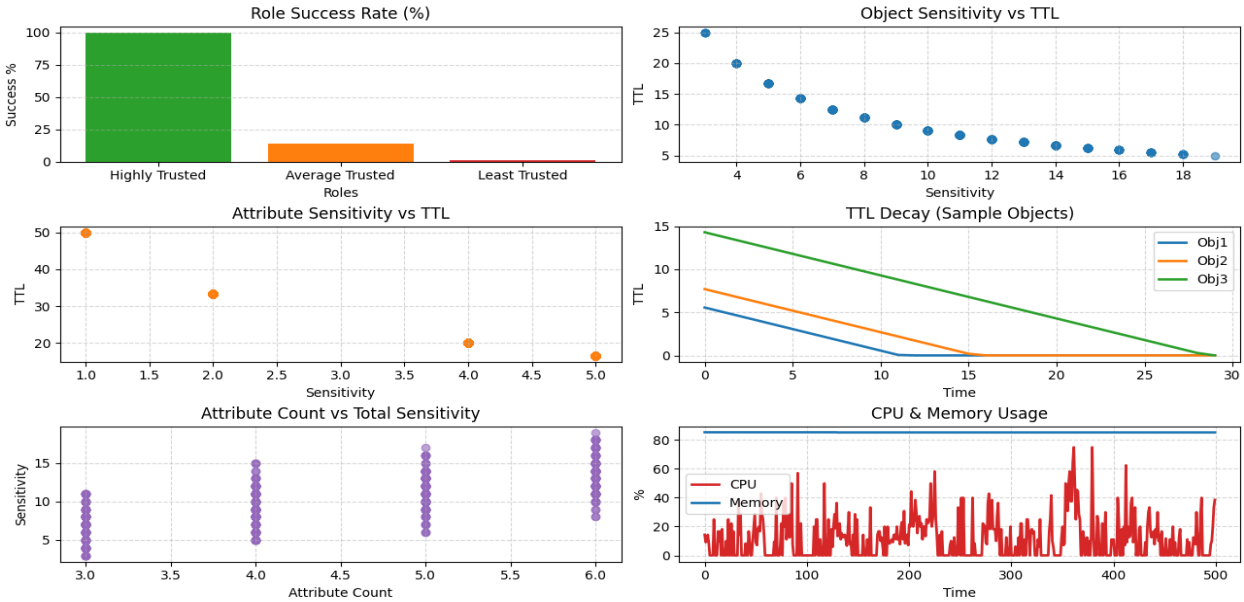


Figure 8. Analysis of Hybrid access control for PII access

Organisations 2 and 3 also can perform attribute and object-level access. But the permission of access depending on the sensitivity of the attribute or the object. Object sensitivity vs TTL and Attribute sensitivity vs TTL are also plotted. The total life time of a sharing is controlled by sensitivity of the objects and attributes. CPU and memory usage for the hybrid model were observed as lightweight.

Table 3 summarises the performance of the three models. RBAC models are less granular with object-level data abstraction for access. ABAC models are

more granular but lightweight. The hybrid model with object-level and attribute-level access and additional TTL state is complex but flexible. The on-device model efficiently avoids computationally expensive cryptographic operations, thereby achieving low latency and CPU usage. TTL dependency with the sensitivity of PII makes these models useful in scenarios where the user's consent to share their PII is highly time-bound. From a legal perspective, the user's data should not be used beyond the requirement of data sharing. PII access control that can work on a user device is designed and implemented in this work.

Table 3: Performance summary of the models

Model	Max. Latency (sec)	Avg. Latency (sec)	Max. CPU Usage	Avg. CPU Usage
RBAC	0.003	0.0018	55%	45%
ABAC	0.001	0.0003	22%	8%
Hybrid	0.001	0.00006	34%	8%

4. Conclusions

RBAC, ABAC, and Hybrid models were tested, and the results are analysed. Depending on the scenario of access control, these models help with varying levels of granularity. All models are observed to be efficient in terms of scalability, CPU, and memory utilisation. ABAC and RBAC models control access to PII based on sensitivity and trust. The hybrid model has more fine-tuned controls by introducing an environment variable, TTL. Both object- and attribute-level granularity offer more flexibility.

Three levels of sensitivity and trust are defined in the work. In a real-world scenario, there must be more levels for these. The proposed sensitivity model uses a simple sum with predefined weights. This can be replaced with learned weights and the probability of identification. The assumed trust levels can be fine-tuned with realistic data. This work is not intended to deal with the cryptographic security and anonymisation of data in transit. Integrating machine learning algorithms for sensitivity and trust identification and calculation will help data owners and data collectors to fetch more accurate values. NLP models can be included to automate rules.

References

[1] "Ministry of Law and Justice, Government of India. (2023). The Digital Personal Data Protection Act, 2023 (Chapters 2 \& 3). The Gazette of India. https://egazette.nic.in/WriteReadData/2023/248107.pdf Accessed April 8, 2025."

[2] "Office of the Australian Information Commissioner. (2019). Australian Privacy Principle 11 – Security of personal information (Chapter 11). In Australian Privacy Principles guidelines. https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information . Accessed April 8, 2025."

[3] "European Parliament and Council of the European Union. (2016). 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 (General Data Protection Regulation), Chapter 3: Rights of the data subject. Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 Accessed April 8, 2025."

[4] O. L. van Daalen, "The right to encryption: Privacy as preventing unlawful access," *Computer Law and Security Review*, vol. 49, Jul. 2023, https://doi.org/10.1016/j.clsr.2023.105804

[5] J. Shurson, "A European right to end-to-end encryption?," *Computer Law and Security Review*, vol. 55, Nov. 2024, https://doi.org/10.1016/j.clsr.2024.106063

[6] R. L. Rivest, A. Shamir, and L. Adleman. 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21, 2 (Feb. 1978), 120–126. https://doi.org/10.1145/359340.359342

[7] S. Lin, L. Cui, and N. Ke, "End-to-End Encrypted Message Distribution System for the Internet of Things Based on Conditional Proxy Re-Encryption," *Sensors*, vol. 24, no. 2, Jan. 2024, https://doi.org/10.3390/s24020438

[8] M. Nabeel, "The Many Faces of End-to-End Encryption and Their Security Analysis," in *Proceedings - 2017 IEEE 1st International Conference on Edge Computing, EDGE 2017*, Institute of Electrical and Electronics Engineers Inc., Sep. 2017, pp. 252–259. https://doi.org/10.1109/IEEE.EDGE.2017.47

[9] H. Liu and Y. Wang, "Social Media Use and Privacy Concerns: How do College Students view Internet Privacy and Information Protection," *European Journal of Humanities and Social Sciences*, vol. 3, no. 2, pp. 93–102, Apr. 2023, https://doi.org/10.24018/ejsocial.2023.3.2.429

[10] A. Sharma and M. Bantan, "Simulating data breaches: Synthetic datasets for depicting personally identifiable information through scenario-based breaches," *Data Brief*, vol. 58, Feb. 2025, https://doi.org/10.1016/j.dib.2024.111207

[11] N. Wongwiwatchai, P. Pongkham, and K. Sripanidkulchai, "Detecting personally identifiable information transmission in android applications using light-weight static analysis," *Comput. Secur.*, vol. 99, Dec. 2020, https://doi.org/10.1016/j.cose.2020.102011

[12] B. Custers and G. Malgieri, "Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data," *Computer Law and Security Review*, vol. 45, Jul. 2022, https://doi.org/10.1016/j.clsr.2022.105683

[13] A. Ammari, E. Allodi, D. Salerno, and G. P. Stella, "An asymmetrical approach to understanding consumer haracteristics in banking trust during the COVID-19 pandemic in Italy," *Res. Int. Bus. Finance*, vol. 64, Jan. 2023, https://doi.org/10.1016/j.ribaf.2023.101903

[14] S. Ahmed, K. Bangassa, and S. Akbar, "A study on trust restoration efforts in the UK retail banking industry," *British Accounting Review*, vol. 52, no. 1, Jan. 2020, https://doi.org/10.1016/j.bar.2019.100871

[15] "Consumer Financial Protection Bureau. (2017). Consumer protection principles: Consumer-authorized financial data sharing and aggregation. Consumer Financial Protection Bureau. https://www.consumerfinance.gov/data-research/research-reports/consumer-protection-principles-consumer-authorized-financial-data-sharing-and-aggregation Accessed on 23.3.2025."

[16] "Termly. Data privacy statistics: Understanding consumer concerns and business impact. Termly. https://termly.io/resources/articles/data-privacy-statistics Accessed on 23.3.2025."

[17] H. Tyagi, R. Kumar, and S. K. Pandey, "A detailed study on trust management techniques for security and privacy in IoT: challenges, trends, and research directions," *High-Confidence Computing*, vol. 3, no. 2, Jun. 2023, https://doi.org/10.1016/j.hcc.2023.100127

[18] H. Wang and Y. Song, "Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain," *J. Med. Syst.*, vol. 42, no. 8, Aug. 2018, https://doi.org/10.1007/s10916-018-0994-6

[19] V. C. Hu *et al.*, "NIST Special Publication 800-162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations", https://doi.org/10.6028/NIST.SP.800-162

[20] C. Daudén-Esmel, J. Castellà-Roca, and A. Viejo, "Blockchain-based access control system for efficient and GDPR-compliant personal data management," *Comput. Commun.*, vol. 214, pp. 67–87, Jan. 2024, https://doi.org/10.1016/j.comcom.2023.11.017

[21] Ravi Sandhu, David Ferraiolo, and Richard Kuhn. "The NIST model for role-based access control: towards a unified standard". In Proceedings of the fifth ACM workshop on Role-based access control (RBAC '00). Association for Computing Machinery, New York, NY, USA, 47–63. 2000, https://doi.org/10.1145/344287.344301

[22] H. Wang and Y. Song, " Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. ," *J. Med. Syst.*, vol. 42, no. 152, 2018 https://doi.org/10.1007/s10916-018-0994-6

[23] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," 2005, https://doi.org/10.1007/11426639_27

[24] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2006, pp. 89–98. https://doi.org/10.1145/1180405.1180418

[25] Waters, B. (2011). Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds) Public Key Cryptography – PKC 2011. PKC 2011. Lecture Notes in Computer Science, vol 6571. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-19379-8_4

[26] "U.S. Department of Labour. Guidance on the Protection of Personally Identifiable Information (PII). Available at: \url https://www.dol.gov/general/ppii Last updated: 10/1/2025. Accessed April 8, 2025."