Security and Privacy Requirements for Electronic Consent: A Systematic Literature Review

STEF VERREYDT, KOEN YSKOUT, and WOUTER JOOSEN, KU Leuven

Electronic consent (e-consent) has the potential to solve many paper-based consent approaches. Existing approaches, however, face challenges regarding privacy and security. This literature review aims to provide an overview of privacy and security challenges and requirements proposed by papers discussing e-consent implementations, as well as the manner in which state-of-the-art solutions address them. We conducted a systematic literature search using ACM Digital Library, IEEE Xplore, and PubMed Central. We included papers providing comprehensive discussions of one or more technical aspects of e-consent systems. Thirty-one papers met our inclusion criteria. Two distinct topics were identified, the first being discussions of e-consent representations and the second being implementations of e-consent in data sharing systems. The main challenge for e-consent representations is gathering the requirements for a "valid" consent. For the implementation papers, many provided some requirements but none provided a comprehensive overview. Blockchain is identified as a solution to transparency and trust issues in traditional client-server systems, but several challenges hinder it from being applied in practice. E-consent has the potential to grant data subjects control over their data. However, there is no agreed-upon set of security and privacy requirements that must be addressed by an e-consent platform. Therefore, security- and privacy-by-design techniques should be an essential part of the development lifecycle for such a platform.

CCS Concepts: • **Software and its engineering** → **Requirements analysis**; *Software design engineering*; • **Security and privacy** → *Security services*;

Additional Key Words and Phrases: Systematic literature review, e-consent, electronic consent, security-by-design, privacy-by-design

ACM Reference format:
Stef Verreydt, Koen Yskout, and Wouter Joosen. 2021. Security and Privacy Requirements for Electronic Consent: A Systematic Literature Review. *ACM Trans. Comput. Healthcare* 20, 2, Article 16 (March 2021), 24 pages.
https://doi.org/10.1145/3433995

1 INTRODUCTION

Currently, consent in a medical context is predominantly organized in a paper-based manner. Such consent approaches often offer "take it or leave it" terms that do not allow personalization and impede long-term interaction with the participants [2, 13, 18, 28, 45]. Electronic consent or e-consent has the potential to solve many consent-related challenges, in both medical and non-medical contexts [7, 15, 22, 30]. A recent survey [22] shows that 85%

This research was partially funded by the KU Leuven C2-ePIC project.
Authors' address: S. Verreydt, K. Yskout, and W. Joosen, KU Leuven, imec-DistriNet, Belgium; emails: {stef.verreydt, koen.yskout, wouter.joosen}@kuleuven.be.

2637-8051/2021/03-ART16 $15.00
https://doi.org/10.1145/3433995

of pharmaceutical companies plan to adopt e-consent for some studies in the near future. Furthermore, 71% of the survey's respondents indicated that the majority of their studies will adopt e-consent in the coming years.

A number of e-consent solutions already exist today, but there are some open issues regarding privacy and security. For example, in a survey published in 2015, Rezaeibagha et al. [51] investigated which security and privacy enhancing techniques are frequently used in current Electronic Health Record (EHR) systems. They conclude that there is a demand for standards to emphasize security and privacy protection when dealing with data sharing and that "there needs to be greater emphasis on the application of security operations." In another survey published in 2019, Zazaza et al. [63] note that around 60% of the papers they analyzed "highlighted the importance of using security approaches that value and ensure the privacy of patients' health information." The authors do not, however, discuss what these security approaches are specifically.

Privacy and security issues have become even more relevant with the recent introduction of the General Data Protection Regulation (GDPR) [1]. This work therefore aims to provide an overview of the security and privacy challenges, requirements, and solutions proposed by recent research discussing e-consent. Our literature review differs from the one published by Rezaeibagha et al. [51] in two ways. First of all, we aim to provide an overview of e-consent applications in general rather than focusing solely on a medical context. Second, we not only discuss the used security and privacy enhancing techniques but also which challenges the analyzed papers identify with existing approaches, and which requirements they pose for new ones. Compared to the survey by Zazaza et al. [63], we aim to provide a more elaborate overview of recent e-consent solutions by discussing all information security principles (confidentiality, integrity, availability, and non-repudiation) rather than just confidentiality.

2 METHODS

The structure of this literature review is based on the procedure proposed by Kitchenham [32]. It is reported based on the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) statement [44].

2.1 Search Strategy

E-consent relates to both the computer science and life science domains. We opted to examine ACM Digital Library and IEEE Xplore Digital Library, as they provide content related specifically to computer science. Similarly, PubMed Central was examined for its focus on life sciences. Other digital libraries were not examined, since most of their content related to computer science or life sciences is accessible through the preceding digital libraries [24]. The databases were searched for eligible studies on March 18, 2020. Our search strategy required the word "consent" to be present in the abstract of the paper. Furthermore, the full text should include the word "software" and any of the words "design," "model," or "architecture." Only papers published between 2010 and 2019 were considered. The specific search strategies are shown in Figures 1, 2, and 3. The search protocol was reviewed by a supervisor.

2.2 Study Selection and Eligibility Criteria

Relevant papers were selected from the search results in two stages. First, papers unrelated to e-consent were excluded by examining the title, abstract, introduction, and conclusion of the articles. Then, inclusion and exclusion criteria were applied to the full text of the remaining papers. Our inclusion criteria were full, English papers providing a comprehensive discussion of one or more technical aspects of e-consent systems, published between 2010 and 2019. Our exclusion criteria were surveys, papers not discussing technical aspects of e-consent systems, papers discussing solely the user interface of e-consent systems, and papers discussing solely e-consent forms and the questions asked therein. To verify the correct application of the criteria, they were also applied to a random subset of all papers by a supervisor. Disagreements about inclusion decisions were discussed to resolve any ambiguity in the criteria. These were mostly related to whether or not papers were sufficiently technical and comprehensive to be included.

```
[Abstract: "consent"] AND [Full Text: "software"] AND
[[Full Text: "design"] OR [Full Text: "model"] OR
[Full Text: "architecture"]] AND
[Publication Date: (01/01/2010 TO 12/31/2019)]
```

Fig. 1. ACM Digital Library search strategy.

```
((("Abstract":"consent") AND ("Full Text Only":"software") AND
("Full Text Only":"design" OR "Full Text Only":"model" OR
"Full Text Only":"architecture")))
```

Fig. 2. IEEE Xplore Digital Library search strategy.

```
"consent"[Title/Abstract] AND "software"[Text] AND ("design"[Text] OR
"model"[Text] OR "architecture"[Text]) AND
("2010/01/01"[PDAT] : "2019/12/31"[PDAT]) AND "loattrfull text"[sb]
```

Fig. 3. PubMed search strategy.

2.3 Data Items and Synthesis of Results

A template of high-level questions was prepared prior to the data collection. These comprised (i) what challenges are identified for existing e-consent solutions, (ii) what requirements are listed for a more optimal solution, and (iii) how the these challenges and requirements are tackled by the solution(s) proposed in the papers. During the data collection, two distinct yet relevant topics were identified in the included papers: some are concerned with representing consent preferences electronically, whereas others are concerned with implementing electronic consent in data sharing systems. The high-level questions described earlier were specified further for both topics. The complete question templates can be found in Appendix A. We elaborate on the most frequently mentioned security and privacy requirements, challenges, and solutions in Section 3.

2.4 Limitations

Some general topics are closely related but not specific to consent. For example, a consent statement could be seen as an access control policy, so general access control techniques may have been worth examining in this literature review. The search strategy described in Section 2.1, however, specifically requires the keyword “consent” to be present in the abstract, which results in such articles not being identified if they do not specifically mention consent in the abstract.

2.5 Search Results

Applying the search strategy resulted in a total of 530 papers being identified (Figure 4). A total of 503 of the identified papers were excluded by removing duplicates and applying the study selection process described in Section 2.2. Four additional records were added through examining the sources referenced in the included papers and the related literature reviews by Rezaeibagha et al. [51] and Zazaza et al. [63].

3 RESULTS

Two distinct topics have been identified in the collected set of papers. Ten of the 31 included papers are concerned with how to represent consent electronically. These papers describe the syntax and semantics of electronic consent policies and how these are translated to access control decisions. Twenty-three of the included papers concern the implementation of these policies and access control methods in data sharing

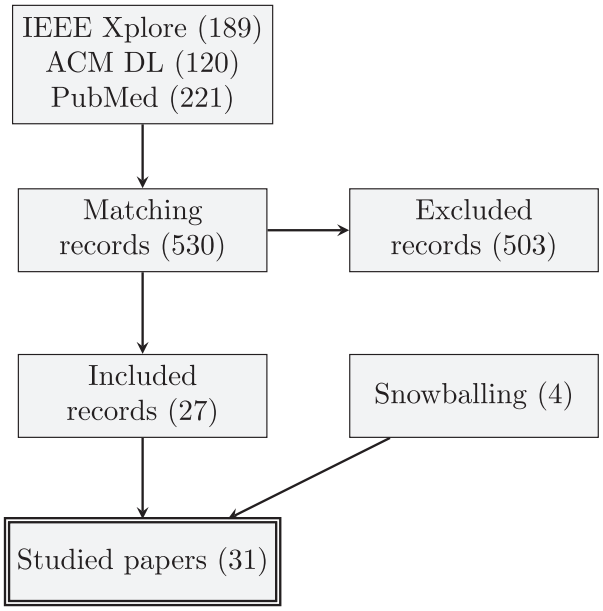

Fig. 4. PRISMA flowchart of the systematic literature review.

systems. More specifically, they describe how to grant data subjects control over their consent policies and how organizations can prove that the consent policies have been enforced correctly. Two of the included papers discuss both representation and implementation of e-consent. Frequently mentioned subjects will be discussed separately for both of the categories. The extracted data is included the tables presented in Appendix B.

3.1 Representation

The papers discussing e-consent representations mention several requirements for adequate representations, mainly related to which concepts should be represented in a consent policy (Table 1). Furthermore, they highlight challenges and propose solutions for both policy modeling and access control (Table 2).

We have identified six main themes, namely how the required concepts are gathered, the granularity of these concepts, additional context information that needs to be included, adherence to regulations, ontologies for consent, and access control models. In what follows, we provide an overview of these themes and their related challenges as described by the identified papers. A discussion will follow in Section 4.

3.1.1 Concept Discovery Method. Before choosing a representation language and access control model, the exact concepts that should be represented should be known. These mainly depend on the context and relevant regulations. Some papers [8, 49, 52] provide arbitrary sets of requirements without mentioning how they were gathered. Other papers [4, 6, 43] do not list any required concepts at all. Their goal is showing how a certain language can be used to represent some kind of consent rather than providing a complete representation. Three papers [10, 31, 62] use an ontology as the starting point for their representation (see Section 3.1.5). Finally, one paper [26] examines both context-specific and Canadian regulatory requirements to discover which concepts should be present in their proposed consent representation, without discussing an ontology. Frequently discussed concepts to be modeled are the subject, the actions for which consent is given, the involved data, and the purpose of the consent policy.

3.1.2 Concept Granularity. The level of precision with which consent concepts are expressed is an important decision to be made. This level of precision is referred to as granularity. The granularity of the basic consent aspects (subject, actions, data, purpose) are discussed briefly in this section.

We refer to the *subject* of a consent policy as the person who is granted or denied access to certain information. This is not to be confused with the data subject (i.e., the one to whom that information belongs). Two frequently required granularity levels for subjects are role-based consent [42] and fine-grained consent [25, 49]. In role-based consent models, users are assigned a role (e.g. "researcher" or "admin"), and access control policies grant or deny access to users based on their role. Fine-grained consent models allow access control policies to grant or deny access to specific users (e.g., "Bob").

The granularity of possible *actions* to be performed on data ranges from course-grained, all-or-nothing approaches [26] to very specific actions such as collect, record, store, and adapt [10, 25].

The *data* to which a consent policy allows or denies access also needs to be scoped. For example, in the context of EHRs, policies could target all records belonging to a patient, a single record, a section in a record, a specific data type (e.g., "address" or "blood pressure"), and so on [25, 49, 52].

Finally, a *purpose* for using the data may also be required in a consent policy, and granularity is again an important decision for this parameter. Examples of purposes include "personalized advertisements" or "cancer-related research." Purposes can be given as free text or chosen from a list of purpose categories [10]. Allowing any textual description may increase the ability to express the exact purpose required, but natural language may be ambiguous. However, offering static purpose categories removes ambiguity but introduces a lack of expressiveness when implementing consent policies.

3.1.3 Context-Dependent Requirements. Besides the basic consent policy concepts mentioned earlier, some additional features may be required, depending on the context.

The *validity period* [10, 49] of the consent is one of these features. Data subjects may want the option to set a time constraint on the usage of their data, or legislation may require a retention period to be present in consent policies.

A specific action that several papers [4, 49, 62] require to be supported is the *delegation* of management rights. In some cases (e.g., mental capacity, immaturity), laws can even force data subjects to delegate their consent management rights to caregivers or guardians [49, 62].

Another possible requirement is support for *multiple ownership*. A "friend" relationship on social media, for example, should be manageable by both parties in that relationship [43]. In a medical context, patients in a hospital are not the only authority controlling access to their personal medical record, with the hospital itself also being a controlling authority [31].

A final frequently discussed requirement is related to *policy conflict resolution* [26, 31]. Conflicting access control decisions may be made by multiple policies that concern the same data. For example, there could be a default policy that allows all doctors to access a person's health record, as well as a custom policy that denies access to the health record for one specific doctor. Such a situation could arise if the specific doctor is a (close) relative of the data subject and the data subject does not want that person to see certain sensitive information. These policies would provide conflicting answers when that specific doctor would request access to the health record. A possible solution to this problem would be to let policies concerning specific (groups of) subjects precede over policies concerning more general subject categories. The results of this would be that the doctor from the preceding example would be denied access to the health record. Another possibility would be to assign priorities to policies. If regulations require health information to always be available to emergency doctors, then the policy enforcing this could be given the highest priority to ensure that it always precedes over others. Implementing the preceding solutions may still lead to conflicting access decisions if the rules in question concern equally specific subject groups and have equal priorities. A default access decision could be implemented for these cases (e.g., a "deny" decision precedes over an "allow" one) [25].

3.1.4 Regulations. Regulations like HIPAA (USA), PIPEDA and PHIPA (Canada), and GDPR (Europe) impose requirements on consent. The level of granularity at which information should be included in a consent policy is heavily dependent on the applicable regulations, as non-compliance may lead to severe sanctions [52]. Non-compliance with the GDPR, for example, could lead to administrative fines of more than 20 million euro [1]. Several papers [6, 10, 26, 31, 49, 52, 62] therefore mention their impact on the representation format. The GDPR, for example, requires consent to include a *specific* purpose, so designing a GDPR-compliant consent representation includes defining the required level of specificity. Since laws and regulations are complex, ambiguous, and prone to changes, achieving compliance is challenging [62].

3.1.5 Ontologies. Some papers [10, 31, 62] provide an ontology of consent when discussing their proposed solution. An ontology describes a domain through a combination of a structured vocabulary, a set of relationships between the concepts of that vocabulary, and a formal language [31, 54]. The vocabulary defines the relevant domain concepts. For example "consent," "subject," and "activity," with the latter being further specified to "create," "read," "update," or "delete," could be specified for a consent ontology. A possible relationship could be that "a consent must include an activity and a period of validity." Describing the identified concepts and relationships in a formal language removes any potential ambiguity. Examples of such languages include description languages like Web Ontology Language (OWL), formal specification languages like Z, or mathematical notations based on set theory and/or graphs.

3.1.6 Access Control Models. Several standards for access control policy languages exist. The type of access control model to use mainly depends on the required level of granularity. Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are two widely used models. They evaluate access requests based on a user's role (e.g., doctor) or specific attributes (e.g., name, role, IP address), respectively. ABAC is used more frequently in a medical context, as it is more flexible [53]. Note that RBAC is essentially a specialization of ABAC. eXtensible Access Control Markup Language (XACML) is an ABAC standard that not only defines the access control language but also a reference architecture and a method for evaluating access requests. Access control policies in XACML are sets of rules that are verified for incoming access requests (e.g., "grant access if role=doctor").

Although XACML has been used and implemented extensively, some authors list challenges regarding its applicability in practice, including the difficulty of expressing rules, a lack of native subject and resource hierarchies, and no support for multiple ownership [25, 31]. Furthermore, its reference architecture does not consider the GDPR data privacy regulations [10].

Another option for access control, which 8 of 10 included papers prefer, is to write policies in a formal language and evaluate access requests through logic reasoning [4, 8, 31, 49, 62] or model checking [6, 25, 43]. Logic reasoning entails discovering new knowledge from existing axioms (facts) through inference. If "Alice allows doctors to access her health records" and "Bob is a doctor" are two known axioms, a logic reasoner may infer that "Alice allows Bob to access her health records" by combining these axioms. If Bob then were to request access to Alice's health records, the reasoner would allow this based on the existence of the newly discovered axiom.

Model checkers, however, model consent policies as graphs and evaluate access requests by analyzing these graphs. An example graph is shown in Figure 5. Subjects and data types are represented by a node, and the connections between them represent the access control. For example, "doctor" and "Bob" could both be subject nodes, and if Bob is a doctor, they are connected through a "specification" relationship, meaning that Bob is a doctor. Alice's health data and her blood pressure could both be data type nodes, with blood pressure being a specification of health data. Consent policies are modeled as connections between these nodes—for example, an "allow access" relationship between Bob and blood pressure [25].

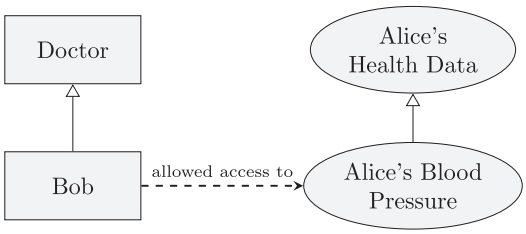

Fig. 5. Example consent policy graph as used by model checkers. Bob, a Doctor, is allowed access to Alice's blood pressure data.

3.2 Implementation

Of the 23 papers discussing e-consent implementation, 11 focus on eHealth systems, whereas the other 12 concern web or Internet of Things (IoT) applications, or generally applicable e-consent solutions. We observe that all included papers concerning the latter category were published only after 2015. Nine [9, 10, 19, 29, 33, 35, 46, 47, 59] of those 12 papers were, in fact, published after April 2016, which is when the GDPR was adopted. We therefore hypothesize that this increase in research for generally applicable e-consent implementations is caused by the introduction of the GDPR, which introduced stricter regulations for such applications. The publication dates for the papers concerning eHealth systems are more or less evenly distributed between 2010 and 2020, which could be explained by the existence of strict regulations for such systems prior to the introduction of the GDPR.

Most of the implementation challenges identified by the included papers are related to privacy and security, but some also mention interoperability and usability issues (Tables 3 and 4). We have categorized the requirements mentioned by the papers according to the main information security principles, namely confidentiality, integrity, availability, and non-repudiation. Additionally, requirements related to the control that data subjects have over their data ("data subject control") were also frequently listed. These include requirements on which concepts the consent should include and how granular these concepts should be, as discussed previously in Section 3.1, as well as requirements on how data subjects should be able to manage their data or consent preferences. An overview of the requirements is shown in Tables 5 and 6. Availability requirements were not encountered and thus are not included in these tables.

Besides mentioning requirements, the papers also propose solutions to these requirements. An overview of the proposed solutions is provided in Tables 7 and 8. They were analyzed in terms of how consent is enforced, if consent enforcement can be verified ("non-repudiation"), if any other information security measures are implemented, whether performance and scalability of the solution are discussed, which existing technologies are used, and which future challenges are listed. The remainder of this section discusses the frequently identified challenges and requirements, and how they are tackled by the proposed solutions.

3.2.1 Non-Repudiation. Transparency, verifiability, and auditing capabilities are recurring challenges and/or requirements listed by the analyzed papers. Data subjects and legal authorities expect a way to verify that data has not been processed without a valid consent. Many of the proposed solutions [5, 14, 16, 19, 21, 23, 33, 34, 39, 41, 60, 62] require a centralized authority to manage all accesses to sensitive data. Having such authority to maintain a log of all consents and processing activities does not necessarily lead to non-repudiation, as then the log itself needs to be verifiable. It is therefore imperative that every stakeholder trusts the centralized authority not to tamper with the logs, and thus not to allow unlawful access to data. In situations where trust is lacking (which is often the case in online environments), including a third party may not be an option. Several of the proposed solutions [10, 35, 37, 47, 50, 59] therefore rely on a blockchain to provide transparent and verifiable audit logs.

A blockchain is a ledger where transactions, grouped together in blocks, are appended to the ledger together with a cryptographic hash of the previous block. This makes the ledger resistant to tampering, as changing the contents of a block would invalidate the hashes of the subsequent blocks. The ledger is managed in a peer-to-peer fashion: every node in the blockchain network maintains a copy of the ledger, and adding new blocks requires validation through a process of consensus. Maintaining an audit trail in a blockchain thus removes the need for a trusted third party to validate the audit trail.

3.2.2 Consent Management. Another frequently mentioned requirement is to give data subjects control over who accesses their data. In centralized systems, a single authority usually stores the consent policies and offers some kind of dashboard for patients to manage their preferences. OAuth and User Managed Access (UMA) are specific implementations of such centralized data control systems used when a data subject's resources may be distributed across multiple locations [19]. Such an approach suffers from the same centralization and trust issues as mentioned in Section 3.2.1, and blockchain could again be a solution for them. In a blockchain system, entities manage their resources through a "wallet," which is usually a public/private key pair. Sending valid transactions from a wallet is only possible for the entity controlling the private key of that wallet. The proposed blockchain solutions for e-consent leverage this property by having users store their consent preferences on a blockchain. A transaction in an e-consent context is a consent policy—for example, "I allow Bob to access my health record." Since blockchain only allows adding new transactions, updating a consent policy involves adding a new policy to the blockchain that overrides the previous ones. Blockchain thus grants data subjects full control over their consent (and thus data) in a distributed and tamper-resistant manner.

3.2.3 Confidentiality. Data is confidential if it can be accessed only by entities authorized to do so. Enforcing the consent policies is therefore a crucial requirement for the confidentiality of e-consent systems. Blockchain-based solutions face additional threats to confidentiality, as all data on the chain is visible to all participants. Both of these topics are discussed briefly in this section.

Consent enforcement. Many of the analyzed papers list consent enforcement as a requirement [10, 19, 20, 29, 34, 41, 50, 59, 60]. An overview of different access control models was provided in Section 3.1.6. Enforcing access control models in a centralized environment is fairly straightforward: an entity sends an access request to the central authority, which evaluates it and grants or denies access to the resources based on the evaluation. Centralized eHealth systems are mainly based on IHE [55] integration profiles, using either Basic Patient Privacy Consent (BPPC) [58] or Advanced Patient Privacy Consent (APPC) [56] to record and enforce consent preferences. The decentralized solutions utilizing blockchain to store consent policies use smart contracts to enforce these policies. A smart contract is in essence a piece of code that enforces the conditions listed in a contract. Blockchain solutions such as Ethereum and Hyperledger allow smart contracts to be coded in a transaction. Requests to execute a smart contract are forwarded to all nodes on the network, which then agree on the correct output through consensus. Users are thus certain that their contract cannot be tampered with, because it is stored on a blockchain, and that it is executed correctly, because the nodes need to agree on the correct outcome. Furthermore, smart contract executions are recorded on the blockchain, which ensures that they are verifiable. These properties make smart contracts ideal mechanisms to store and enforce consent policies in a distributed environment.

Blockchain confidentiality. Access control is just one aspect of confidentiality. When compared to centralized systems, blockchain introduces other major confidentiality challenges, as every transaction in a blockchain system is visible to all participating nodes. For this reason, none of the distributed solutions proposed in the analyzed papers store any sensitive data (e.g., blood pressure values) directly on the blockchain. Instead, smart contracts return the location of the sensitive data and an access token if all conditions are met. The sensitive data could be located in a central database, some data silo belonging to a single stakeholder or a distributed database (e.g., IPFS).

3.2.4 Integrity. Protecting data from unauthorized modifications is an essential requirement for any system dealing with sensitive information. The majority of the analyzed papers [10, 14, 17, 33–35, 37, 47, 50, 59] therefore mention some kind of integrity requirement. Few of these papers, however, describe specific solutions. Communication-level encryption (e.g., TLS [34]) and the tamper resistance of blockchain were identified as integrity measures by some papers.

3.2.5 Other Non-Functional Requirements. Solutions for e-consent need to be secure and privacy preserving but need to address additional non-functional requirements as well. For example, a platform used for managing consent will also have to interoperate with other systems, be user-friendly, and sufficiently performant.

Interoperability. Interoperability may be an important requirement for e-consent systems, such as when multiple hospitals work together for research projects. Centralized solutions therefore incorporate standardized architectures and data formats like the ones provided by IHE [55] and HL7 [11] to integrate all stakeholders. Furthermore, some of the centralized solutions [9, 23, 39] utilize XACML as a standardized access control model, leading to easier interoperability.

Most of the blockchain solutions are based on either Ethereum [35, 47] or Hyperledger Fabric [10, 33, 50, 59]. Both of these platforms describe protocols for integration and define programming languages in which smart contracts should be written. None of the blockchain-based solutions, however, refer to a standard representation of consent policies in smart contracts. There is thus also no standardized method of enforcing consent policies in a blockchain, which may hinder interoperability.

Usability. Several of the identified papers [10, 47, 50, 59, 62] mention usability challenges. Although not the main focus of this article, as we did not consider UI-related papers, new usability challenges are arising for blockchain-based solutions, as they require a major shift in user behavior [47]. For example, writing a confidential and secure smart contract demands knowledge about programming languages and blockchain itself. Luu et al. [38] discovered that 8,833 out of 19,366 existing Ethereum contracts are vulnerable, which demonstrates that most users do not have this required knowledge. Frequent Security flaws in Ethereum contracts are related to their dependence on transaction ordering or mishandled exceptions [38]. The learning curve associated with blockchain thus may deter people from using the system, or introduce vulnerabilities that could lead to privacy breaches.

Performance and scalability. E-consent systems need to be performant and scalable for them to be useful in practice. These requirements were, however, not frequently mentioned. Furthermore, few of the papers provide a performance evaluation of their proposed solution. Performance and scalability are mostly mentioned as future work, indicating that they are usually an afterthought rather than a requirement. Two papers [14, 59] mention a trade-off between performance and scale. For blockchain specifically, the consensus mechanism is identified as a possible bottleneck. The "proof-of-work" consensus mechanism of Ethereum, for example, requires solving computationally hard puzzles to verify new transactions on the blockchain, which restricts its scalability [47].

4 DISCUSSION

This section provides a further discussion of our findings reported in the previous section.

4.1 Representation

Gathering all requirements for a valid consent and choosing suitable policy languages and access control methods were identified as important aspects for the design of a consent representations in e-consent systems.

4.1.1 Consent Requirements. Requirements for consent are usually ambiguous and complex (e.g., regulations) and depend heavily on the context. For example, Robol et al. [52] and Davari and Bertino [10], who refer to European regulations, identify *purpose* as a key aspect of consent, whereas Huynh et al. [25], who refer to

Canadian regulations, do not. Seven of the 10 papers discussing e-consent representations [4, 6, 8, 31, 43, 49, 52], however, provide a consent policy language and access control method without discussing what "consent" entails. A sensible first step in selecting a consent representation could be to formalize the requirements by composing a comprehensive ontology of consent [10]. Doing so should reveal the required concepts and their relationships, as well as the necessary level of granularity.

4.1.2 Access Control Models. Recent literature seems to prefer formal access control models like logic reasoning and model checking (as described in Section 3.1.6) over RBAC and ABAC approaches like XACML. Furthermore, consent standardization efforts such as IHE's BPPC [58] and APPC [56], GA4GH's Automatable Discovery and Access Matrix (ADA-M) [61], and ISO standards (e.g., ISO 22600-1:2014 [27]) were not discussed in the identified papers. This could be due to two reasons: either standardized approaches are sufficient as they are now, so there is no additional research needed, or the exact opposite, being that they are deemed inappropriate and are not considered an option anymore. The challenges listed by the identified papers do not reveal any major issues with standardized access control methods, so we can assume the former reason is true. Despite traditional approaches seeming sufficient for most use cases, formal ones may have several advantages depending on the exact implementation, a first of which is performance. Research shows that they could evaluate requests significantly faster than XACML when there is a large number of rules [25]. A possible second advantage is ease of policy definition, as custom approaches may offer simpler syntax and semantics when compared to traditional approaches. Third, formal approaches allow to target a specific use case instead of having to extend or modify existing approaches. Despite these advantages, it may not be worth implementing custom approaches for several reasons. First of all, existing standards like XACML have been used and reviewed by a large community. In contrast, there are no standards for formal consent models and reasoners. Second, although formal approaches may allow for a solution that is more fit for the use case at hand, integration with other systems may be hindered because of this [6]. In contrast, XACML is generic but can be extended to fit specific requirements. Furthermore, smart contracts lend themselves to traditional access control methods where "if..., then..., else..." statements are executed rather than formal methods. It remains to be seen whether the formal methods can be incorporated in a distributed context. Choosing an access control model will largely depend on the context and requires a thorough analysis of both functional and non-functional requirements.

4.2 Implementation

Gathering a comprehensive set of requirements is again identified as an important step in the design of an e-consent implementation, similar to the design of an e-consent representation. Although standards exist for centralized architectures, especially in the context of eHealth, blockchain may offer solutions for the centralization issues faced in these systems.

4.2.1 Requirements. Most papers mention some information security requirements, but none provide a complete overview. As expected, consent management and enforcement, and access control in general, are identified as essential confidentiality requirements for e-consent systems. Integrity requirements such as secure communication and tamper resistance are also prevalent. Non-repudiation, however, was rarely considered as a requirement before the introduction of the GDPR, which exposed transparency issues with traditional client-server architectures. Although IHE offers integration profiles for auditing [57], these rely on a security officer to detect non-compliant behavior, which introduces centralization and trust issues. Distributed solutions, however, target these non-repudiation issues but do not consider confidentiality challenges introduced by blockchain. The complete absence of availability requirements is especially interesting, as it is a key aspect of information security.

As for other non-functional requirements, interoperability and usability are mentioned as challenges with current approaches, but are only sporadically listed as actual requirements. Performance requirements are also lacking in the identified papers. These are, however, essential properties for any usable system.

In general, although most of the identified records covered the main requirements of consent management and enforcement, none of them provide a complete overview of all relevant requirements.

4.2.2 Blockchain. Blockchain provides many advantages for e-consent systems compared to traditional, client-server architectures, including the following:

- It is fully *distributed*, allowing multiple stakeholders to collaborate without the need for a trusted third party.
- It provides a generally *immutable and transparent audit trail.*
- Data owners have *full control* over their own data through the use of smart contracts.
- It is *robust* and provides *high availability* because each node has a full copy of the ledger.
- It provides inherent *pseudonimity*, as data owners are represented by a (random) public key rather than, for example, an email address [36].

Nonetheless, the proposed blockchain-based solutions are in relatively early stages of development [37]. A recent report by the European Commission [3] describes multiple challenges for blockchain that have not been tackled by the papers identified in this SLR. Some relevant ones are the following.

First, although entities in a blockchain network are pseudonymous, they are not anonymous: *reidentification* may still be possible, and countermeasures (e.g., stealth addresses) are needed to prevent this. Second, *key management* is crucial in blockchain environments. Entities lose control over their data if they lose their private key. Something as simple as losing your phone could lead to major difficulties in a blockchain environment. Some papers (e.g., [37]) propose a secure key backup, but this reintroduces centralization issues. A third challenge lies with *encryption*, as it is the basis of all blockchain security and confidentiality. Although state-of-the-art encryption protocols are practically unbreakable for now, this might change with quantum computing. Fourth, existing blockchains currently face *performance and scalability* issues, which may hinder their applicability in practical use cases. A fifth challenge lies with the GDPR's *right to erasure*, also known as the "right to be forgotten," and is therefore specific to applications hosted in European member states. As the name suggests, the right to erasure states that individuals have the right to have their personal data erased. Erasing information from a blockchain requires that a majority of the cooperating nodes agree to do so, which may not be feasible in practice. Finally, blockchains are only tamper resistant to a certain extent. Techniques like a 51% attack, where attackers attempt to control over half of the nodes in a blockchain network to manipulate the consensus mechanism, hypothetically allow entities to change the transaction history. Countermeasures are needed to protect blockchains from such attacks.

These challenges hinder the use of blockchain when sensitive data is involved, as is the case in e-consent systems. Despite this, several sensitive applications currently *do* use blockchain in practice [37]. Estonia, for example, recently moved all of their healthcare information to a blockchain [12]. There is a general trade-off between the transparency of distributed solutions and the confidentiality of traditional, centralized solutions. A comprehensive analysis of the context, regulations, and other requirements is necessary to decide which of these properties is most important.

5 CONCLUSION

We performed a systematic literature review to provide an overview of the privacy and security challenges and requirements for e-consent implementations, and how recent literature addresses these. Two categories of papers were identified: some are concerned with representing consent preferences electronically and how to enforce them, whereas others are concerned with implementing electronic consent in data sharing systems.

In summary, for electronic consent representations, traditional access control standards like XACML seem to be sufficient in most cases, as the identified papers did not reveal any major issues with them. Nonetheless,

formal approaches may be beneficial depending on the context. There is, however, no consensus on what consent entails.

For e-consent implementations in data sharing systems, none of the identified papers describes a comprehensive set of requirements. As for solutions, centralized architectures lack transparency, whereas distributed solutions like blockchain lack confidentiality. None of the papers therefore describe a solution that takes into account all information security principles, which may be caused by the lack of a comprehensive set of requirements. Context analyses should reveal which approach is favorable for the use case at hand.

Because of a lack of consensus on the requirements for both e-consent representations and implementations, it is crucial to design e-consent system with security and privacy in mind from the start. This includes carefully eliciting the context-specific security and privacy requirements for the designed system, and addressing these requirements during the design of the system.

APPENDICES

A QUESTION TEMPLATE

- What is the current state of the-art of e-consent representations?
  - What are the requirements for e-consent representations?
    - How are the requirements gathered?
    - Are any regulations considered?
  - What are the current challenges for existing e-consent representations?
  - What are state-of-the-art e-consent representations?
    - What policy languages are used?
    - What access control methods are used?
- What is the current state of the art of e-consent implementations in data sharing systems?
  - What are the current challenges for existing e-consent implementations?
  - What are the requirements for e-consent implementations?
    - What are the Confidentiality requirements?
    - What are the Integrity requirements?
    - What are the Availability requirements?
    - What are the Non-Repudiation requirements?
  - How is e-consent implemented in state-of-the-art data sharing systems?
    - Are the solutions aimed at a specific domain? (General data sharing, eHealth, IoT, Web, ...)
    - How are consent preferences enforced?
    - How is confidentiality guaranteed?
    - How is integrity guaranteed?
    - How is availability guaranteed?
    - How is non-repudiation guaranteed?
    - How do the systems perform and scale?
    - What existing technologies are used?
  - What are future challenges for e-consent implementations?

B DATA EXTRACTION

Table 1. Representation Requirements

Paper	Concept Discovery Method	Concept Granularity				Context-Dependent Requirements				Compliance
		Subject	Actions	What Data	Purpose	Period of Validity	Delegation	Multiple Ownership	Rule Consistency	
Pruski [49]	Arbitrary	Fine-grained	x	Health data grouped into well-defined sets	x	x	x			x
Brucker et al. [6]										x
Can [8]	Arbitrary	Role and organization	x	x	x					
Khan and McKillop [31]	Proof-of-concept ontology provided, but their approach allows any ontology							x	x	HIPAA1, PIPEDA2, PHIPA3, EU-DPD
Yu et al. [62]	Consent ontology						x			US federal, state, and local laws
Bhatia and Singh [4]										
Huynh et al. [25]	Derived from hospital and regulatory requirements	Fine-grained	Grant or deny	Single record or group of records					Priorities	Canadian laws
Mehregan and Fong [43]								x		
Robol et al. [52]	Arbitrary			Fine-grained data types	x					GDPR
Davari and Bertino [10]	Consent ontology derived from GDPR	x	Multiple subcategories (Collect, record, store, ...)	x	Multiple subcategories (Statistics, research, ...)	x				GDPR

Note: An "x" signifies that the paper identified the requirement in general, without describing what is expected specifically.

Table 2. Representation Challenges and Solutions

Paper	Challenges	Solutions	
		Policy Modeling Language	Access Control Method
Pruski [49]	Lack of formal approaches, delegation of rights	BNF syntax, first-order logic, set theory	Inference
Brucker et al. [6]	RBAC insufficiently expressive for complex relationship	Higher-order logic	Model-based testing
Can [8]		Description language (ALCQ)	Inference
Khan and McKillop [31]	Multiple ownership, consent transference, Pruski [49] expects all cooperating systems to use eCRL, traditional AC models unsatisfactory	OWL (N3)	Semantic reasoner
Yu et al. [62]		OWL	Inference
Bhatia and Singh [4]		Z specification language	Theorem prover (Z/EVES)
Huynh et al. [25]	RBAC not granular enough; XACML lacks native subject and resource hierarchies, and rule expression is difficult	Set theory, directed graphs	First-order logic model checkers (Alloy, ProB)
Mehregan and Fong [43]		Graph patterns	Model based, relationship based
Robol et al. [52]	DLs have limited expressivity	Unspecified Description Language	
Davari and Bertino [10]	Existing XACML extensions do not consider GDPR	XACML	Attribute based

Table 3. Challenges for Electronic Consent Implementations in eHealth Systems

Paper	Target Domain	Information Security	Interoperability	Usability
Heinze et al. [23]	eHealth	BPPC has privacy issues and lacks granularity		
Koster et al. [34]	eHealth/IoT	Need for end-to-end security		
Ma and Sartipi [40]	eHealth	Security flaws in existing PACSs (Picturing Archiving and Communication Systems)	DICOM does not transfer user information between parties, making it hard to enforce access control and extract audit trails; difficult to integrate systems with separate databases	
Yu et al. [62]	eHealth			Existing approaches not fit for procedure-oriented treatment regimes
Grunwell and Sahama [16]	eHealth	Logs contain sensitive information, how to store them while maintaining privacy and security	How to perform big data analytics on shared, heterogeneous electronic health records; difficult to integrate systems with separate databases and varying data formats	
Gjerdrum et al. [14]	eHealth	Data subject has little control over data; existing encryption, firewalls, and authentication mechanisms are often inflexible and statically defined		
Brandner et al. [5]	eHealth		Lack of standardized interfaces for personal health records leads to difficult integration	
Haarbrandt et al. [17]	eHealth		Hospitals often employ disparate and proprietary software without standardized interfaces, which hinders efficient data sharing	
Rajput et al. [50]	eHealth	Consent granularity, lack of auditing capabilities for patients		Obtaining consent in emergency situations is often slow
Leeming et al. [37], Prokosch et al. [48]	eHealth			

Table 4. Challenges for Electronic Consent Implementations in Web, IoT, and Other Systems

Paper	Target Domain	Information Security	Interoperability	Usability
Maler [41]	Web	ToS and OAuth force users into acquiscence		
Hashi et al. [20]	IoT			
Ulbricht and Pallas [60]	General	Sticky policies need trusted third party	It is costly to implement distributed usage control on all participating systems	
Joy et al. [29]	IoT	Permission managers lack fine-grained granularity	Lack of cross-platform approaches	
Kiyomoto et al. [33]	General	How to provide verifiable transaction logs of anonymized dataset trading for data owners; difficult to trace anonymized data		
Kouzinopoulos et al. [35]	IoT			
Norta et al. [47]	Web	Existing data brokerage systems generally lack privacy and security		Blockchain-based approaches require major shift in user behavior
Coroller et al. [9]	IoT	Access control without usage control is not sufficient to protect privacy in distributed systems		
Truong et al. [59]	General	Client-server architectures lack transparency and trust; existing approaches depend on the trustworthiness of certificate authority; difficult for service providers to prove GDPR compliance		IPFS: owners are responsible for tasks like key generation, file encryption, and establishing secure channels for communication
Morel et al. [46]	IoT	Individuals do not have simple means to express and communicate it to the entities collecting data; devices used to collect data in IoT environments have scarce resources		
Davari and Bertino [10]	General	It is challenging for the data controller to show that personal data has been processed securely and legally as required; data subjects cannot verify the data controller's compliance in a centralized architecture; few approaches have been proposed for managing access control by using blockchain	Data deletion is challenging, as most corporations store information across multiple business lines without a unified architecture; the data processor processes data on behalf of the data controller and is not aware of consents associated with the requested data and where the data is stored	Usability issues with blockchain
Hardjono [19]	General			

Table 5. Requirements for Electronic Consent Implementations in eHealth Systems

Paper	Target Domain	Data Subject Control		Integrity	Confidentiality	Non-Repudiation	Regulations
		Consent Requirements	Consent Management				
Heinze et al. [23]	eHealth						German legislation
Koster et al. [34]	eHealth/ IoT		User-friendly consent management, consent should propagate together with data	Authenticate data sources, prevent or detect unauthorized data modifications	Consent enforcement		EU Directive 95/46, HIPAA
Ma and Sartipi [40]	eHealth						
Yu et al. [62]	eHealth					A standard way to specify, update, and check compliance with regulations	US federal, state, and local laws, regulations and standards
Grunwell and Sahama [16]	eHealth		Patients should have control over who can access their information and how it is used				
Gjerdrum et al. [14]	eHealth	Fine-grained consent	Revocation of consent	Confidentiality and integrity			Declaration of Helsinki
Brandner et al. [5]	eHealth	Requirements elicited in separate, non-English paper					
Haarbrandt et al. [17]	eHealth	Fine-grained access control	Consent revocation	Data safety and privacy			GDPR
Prokosch et al. [48]	eHealth				Federated authentication system, anonymiza-tion/pseudonymization, privacy preserving record linkage		
Rajput et al. [50]	eHealth			Integrated, trustworthy, and complete data	Access control		
Leeming et al. [37]	eHealth	Fine-grained	Grant and revoke access permissions	Secure information communication, encryption	Pseudonomization	Logging, subjects must be able to view and verify interactions on their data	GDPR

Table 6. Requirements for Electronic Consent Implementations in Web, IoT, and Other Systems

Paper	Target Domain	Data Subject Control		Integrity	Confidentiality	Non-Repudiation	Regulations
		Consent Requirements	Consent Management				
Maler [41]	Web				Consent enforcement		
Hashi et al. [20]	IoT	Fine-grained concepts			Consent enforcement		
Ulbricht and Pallas [60]	General	Utilizer (subject), specific data and purpose			Consent enforcement		European Data Protection Directive, GDPR
Joy et al. [29]	IoT	The data owner should be able to specify how accurately and frequently location information should be disclosed	User control for granularity		Consent enforcement, third-party apps only have access to privatized data		
Kiyomoto et al. [33]	General			Secure transactions		Verifiability of data transactions	Act on the Protection of Personal Information (Japan)
Kouzinopoulos et al. [35]	IoT			Certainty on the authenticity of data independently on the originating device or the medium through which they were communicated			GDPR
Norta et al. [47]	Web		Data providers require an easy, secure, and transparent method of creating and managing data, and to explore data requests	Secure data exchange		Logging	
Coroller et al. [9]	IoT	Fine-grained consent	Consent revocation		End-to-end data confidentiality	Data processing transparency	GDPR
Truong et al. [59]	General	Fine-grained consent	Data subject controls data	Tamper-resistance and data integrity checking	Authentication, authorization, consent enforcement	Logging, transparency, traceability	GDPR
Morel et al. [46]	IoT				Consent enforcement	Demonstrate GDPR compliance by storing consent	GDPR
Davari and Bertino [10]	General	Purpose		Data authenticity (digital signatures)	"Identity mechanism," consent enforcement	Transparency, non-repudiation, data retention	GDPR
Hardjono [19]	General		Subject controls data, single point of access		Cross-domain identity management and consent enforcement; if no consent is obtained, only aggregate data that does not permit reidentification should be released	Transparency, accountability	GDPR, CCPA

Table 7. Solutions for Electronic Consent Implementations in eHealth Systems

Paper	Target Domain	Consent Enforcement	Non-Repudiation	Other Information Security Measures	Performance/ Scalability	Existing Technologies	Future Challenges
Heinze et al. [23]	eHealth	Centralized architecture, based on IHE				BPPC, XDS.b, XACML, HL7 CDA, IHE	
Koster et al. [34]	eHealth / IoT	Centralized architecture, based on IHE XDS	Centralized (IHE ATNA)	Encryption		TLS 1.0, IHE XDM (S/MIME), WS-I BSP (TLS 1.0), Zigbee security, Bluetooth security, HL7 CDA R2	
Ma and Sartipi [40]	eHealth	Centralized architecture, PACS server stores and enforces policies (OpenID/OAuth)				(ClearCanvas) PACS, DICOM, authn/authz, Oauth, OpenID, Client Registry RI, FEM, HIAL, XACML	Incorporating cloud infrastructure
Yu et al. [62]	eHealth	Centralized architecture, based on OpenMRS (open source EHR system)	Centralized authority stores logs			OpenMRS, YAWL	
Grunwell and Sahama [16]	eHealth	Centralized architecture, no standards mentioned	Centralized audit ledger				Prototype, scalability and performance
Gjerdrum et al. [14]	eHealth	Centralized architecture, no standards mentioned	Distributed audit ledger		Performance–scale trade-off, thrashing at large amounts of container instances		Prototype, scalability and performance
Brandner et al. [5]	eHealth	Centralized architecture, based on IHE	Centralized authority stores logs			Liferay, IHE	Two-factor authentication
Haarbrandt et al. [17]	eHealth	Sub-domains are responsible for access control, based on IHE	Each sub-domain has its own audit logs	Pseudonymization		IHE XDS, openEHR, HL7 FHIR	Adapting to the GDPR requirements
Prokosch et al. [48]	eHealth	Sub-domains are responsible for access control		Pseudonymization, anonymization		HL7 FHIR	Quality management, IT security, data protection, privacy-by-design
Rajput et al. [50]	eHealth	Blockchain/smart contracts (Hyperledger Fabric)	Smart contracts log all transactions to the blockchain	Blockchain	Evaluation of response times	Hyperledger Fabric, Hyperledger Composer	
Leeming et al. [37]	eHealth	Blockchain/smart contracts	Smart contracts log all interactions to the blockchain	Blockchain, interactions stored on the chain are encrypted such that only the data subjects can verify their validity			

Table 8. Solutions for Electronic Consent Implementations in Web, IoT, and Other Systems

Paper	Target Domain	Consent Enforcement	Non-Repudiation	Other Information Security Measures	Performance/ Scalability	Existing Technologies	Future Challenges
Maler [41]	Web	UMA	Future work		Scalability is claimed	OAuth/UMA	Formal auditability, claims gathering
Hashi et al. [20]	IoT	Centralized authority stores and enforces policies				RDF, CouchDB	Performance evaluation
Ulbricht and Pallas [60]	General	Centralized authority stores and enforces policies				Hippocratic database, sticky policies	Prototype, more detailed delineations on the legal dimension of technically mediated consent, distributed usage control
Joy et al. [29]	IoT	Consent policies enforced by the mobile device that collects the data		Anonymization		GPSd daemon	
Kiyomoto et al. [33]	General	Sub-domains are responsible for access control	Blockchain	Encryption (AES-CTR, SHA-256, ECDSA), *k*-anonymity	Transaction times evaluated, claims blockchain scalability	Hyperledger Fabric, Docker containers	
Kouzinopoulos et al. [35]	IoT	Blockchain, smart contracts	Blockchain			Ethereum, EVM	
Norta et al. [47]	Web	Blockchain, smart contracts	Blockchain	Encryption, key management	Ethereum proof-of-work consensus is bottleneck	Data Source: IPFS; Profile-Key Server: ZeroPass; Data-Profile manager: BigChainDB, Ethereum, Qtum; Search Agent: JADE; Smart-Contract Manager: BigChainDB, Ethereum, Qtum; Contract Evaluator: Embark, Populus; Escrow: BigChainDB, Ethereum, Qtum; Request Manager: BigChainDB, Ethereum, Qtum	

(Continued)

Table 8. Continued

Paper	Target Domain	Consent Enforcement	Non-Repudiation	Other Information Security Measures	Performance/ Scalability	Existing Technologies	Future Challenges
Coroller et al. [9]	IoT	Usage control data stored in a distributed hash table and enforced by gateways near the IoT devices	Unspecified external/ independent log storage	Future work	Overhead in computation potentially makes it unsuitable for monitoring real-time consumer applications, DHT provides scalability	UCONabc, XACML 3.0	Prototype and performance testing
Truong et al. [59]	General	Blockchain, smart contracts	Blockchain	ECSDA provides pseudo-anonymity but depends on trustworthiness of the Fabric CA, encryption, signatures	Latency vs throughput trade-off; can be partially solved by partitioning the BC network so fewer messages are exchanged, but this results in reduced decentralization and the system being more sensitive to 51% and selfish mining attacks	Hyperledger Fabric, Kafka	Prototype, more mechanisms to resolve lack of trusted centralized RS, fine-grained expressive data usage policies, pricing and incentive models, multi-party computation
Morel et al. [46]	IoT	IoT-device stores consent preferences and automatically sends them to tracking devices upon entering a monitored area; tracking is only allowed if the controller's privacy policy complies with the preferences					Usability
Davari and Bertino [10]	General	Blockchain, smart contracts	Blockchain	Blockchain, digital signatures		HLF, XACML, MongoDB	
Hardjono [19]	General	UMA				OAuth/UMA	

REFERENCES

[1] Intersoft Consulting. n.d. General Data Protection Regulation GDPR—Official Legal Text. Retrieved February 1, 2021 from https://gdpr-info.eu/.

[2] Andrea Akkad, Clare Jackson, Sara Kenyon, Mary Dixon-Woods, Nick Taub, and Marwan Habiba. 2006. Patients' perceptions of written consent: Questionnaire study. *BMJ* 333, 7567 (Sept. 2006), 528. DOI: https://doi.org/10.1136/bmj.38922.516204.55

[3] Amanda Anderberg, Elena Andonova, Mario Bellia, Ludovic Calès, Andreia Inamorato Dos Santos, Ioannis Kounelis, Igor Nai Fovino, et al. 2019. *Blockchain Now and Tomorrow*. Publications Office of the European Union, Luxembourg.

[4] Rekha Bhatia and Manpreet Singh. 2014. Formal specification of a privacy aware access control framework in web services paradigm using *z* notation. In *Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies (ICTCS '14)*. ACM, New York, NY, 1–5. DOI: https://doi.org/10.1145/2677855.2677929

[5] Antje Brandner, Bjorn Schreiweis, Lakshmi S. Aguduri, Tobias Bronsch, Aline Kunz, Peter Pensold, Katharina E. Stein, et al. 2016. The patient portal of the personal cross-enterprise electronic health record (PEHR) in the Rhine-Neckar-Region. *Studies in Health Technology and Informatics* 228 (2016), 157–161.

[6] Achim D. Brucker, Lukas Brügger, Paul Kearney, and Burkhart Wolff. 2011. An approach to modular and testable security models of real-world health-care applications. In *Proceedings of the 16th ACM Symposium on Access Control Models and Technologies (SACMAT'11)*. ACM, New York, NY, 133–142. DOI: https://doi.org/10.1145/1998441.1998461event-place: Innsbruck, Austria.

[7] Isabelle Budin-Ljosne, Harriet J. A. Teare, Jane Kaye, Stephan Beck, Heidi Beate Bentzen, Luciana Caenazzo, Clive Collett, et al. 2017. Dynamic consent: A potential solution to some of the challenges of modern biomedical research. *BMC Medical Ethics* 18, 1 (Jan. 2017), 4. DOI: https://doi.org/10.1186/s12910-016-0162-9

[8] Ozgu Can. 2013. A semantic model for personal consent management. In *Metadata and Semantics Research*. Communications in Computer and Information Science, Vol. 390. Springer, 146–151.

[9] Stevan Coroller, Sophie Chabridon, Maryline Laurent, Denis Conan, and Jean Leneutre. 2018. Position paper: Towards end-to-end privacy for publish/subscribe architectures in the Internet of Things. In *Proceedings of the 5th Workshop on Middleware and Applications for the Internet of Things (M4IoT'18)*. ACM, New York, NY, 35–40. DOI: https://doi.org/10.1145/3286719.3286727

[10] Maryam Davari and Elisa Bertino. 2019. Access control model extensions to support data privacy protection based on GDPR. In *Proceedings of the 2019 IEEE International Conference on Big Data (Big Data'19)*. 4017–4024. DOI: https://doi.org/10.1109/BigData47090.2019.9006455

[11] R. H. Dolin, L. Alschuler, C. Beebe, P. V. Biron, S. L. Boyer, D. Essin, E. Kimber, T. Lincoln, and J. E. Mattison. 2001. The HL7 clinical document architecture. *Journal of the American Medical Informatics Association* 8, 6 (Dec. 2001), 552–569.

[12] e-Estonia. 2018. Blockchain and Healthcare: The Estonian Experience. Retrieved February 1, 2021 from https://e-estonia.com/blockchain-healthcare-estonian-experience/.

[13] Matthew E. Falagas, Ioanna P. Korbila, Konstantina P. Giannopoulou, Barbara K. Kondilis, and George Peppas. 2009. Informed consent: How much and what do patients understand? *American Journal of Surgery* 198, 3 (Sept. 2009), 420–435. DOI: https://doi.org/10.1016/j.amjsurg.2009.02.010

[14] Anders T. Gjerdrum, Håvard D. Johansen, and Dag Johansen. 2016. Implementing informed consent as information-flow policies for secure analytics on ehealth data: Principles and practices. In *Proceedings of the 2016 IEEE 1st International Conference on Connected Health: Applications, Systems, and Engineering Technologies (CHASE'16)*. 107–112. DOI: https://doi.org/10.1109/CHASE.2016.39

[15] Christine Grady, Steven R. Cummings, Michael C. Rowbotham, Michael V. McConnell, Euan A. Ashley, and Gagandeep Kang. 2017. Informed consent. *New England Journal of Medicine* 376, 9 (2017), 856–867. DOI: https://doi.org/10.1056/NEJMra1603773

[16] D. Grunwell and T. Sahama. 2015. Information accountability and Health Big Data Analytics: A consent-based model. In *Proceedings of the 2015 17th International Conference on E-health Networking, Application, and Services (HealthCom'15)*. 195–199. DOI: https://doi.org/10.1109/HealthCom.2015.7454497

[17] Birger Haarbrandt, Bjorn Schreiweis, Sabine Rey, Ulrich Sax, Simone Scheithauer, Otto Rienhoff, Petra Knaup-Gregori, et al. 2018. HiGHmed—An open platform approach to enhance care and research across institutional boundaries. *Methods of Information in Medicine* 57, Suppl. 01 (July 2018), e66–e81. DOI: https://doi.org/10.3414/ME18-02-0002

[18] Bente Hamnes, Yvonne van Eijk-Hustings, and Jette Primdahl. 2016. Readability of patient information and consent documents in rheumatological studies. *BMC Medical Ethics* 17, 1 (2016), 42. DOI: https://doi.org/10.1186/s12910-016-0126-0

[19] Thomas Hardjono. 2019. Federated authorization over access to personal data for decentralized identity management. *IEEE Communications Standards Magazine* 3, 4 (Dec. 2019), 32–38. DOI: https://doi.org/10.1109/MCOMSTD.001.1900019

[20] Yuichi Hashi, Kazuyoshi Matsumoto, Yoshinori Seki, Masahiro Hiji, Toru Abe, and Takuo Suganuma. 2015. Data management scheme to enable efficient analysis of sensing data for smart community. In *Proceedings of the 2015 IEEE 39th Annual Computer Software and Applications Conference*, Vol. 3. 182–187. DOI: https://doi.org/10.1109/COMPSAC.2015.233

[21] Yuichi Hashi, Kazuyoshi Matsumoto, Yoshinori Seki, Masahiro Hiji, Toru Abe, and Takuo Suganuma. 2015. Design and implementation of data management scheme to enable efficient analysis of sensing data. In *Proceedings of the 2015 IEEE International Conference on Autonomic Computing*. 319–324. DOI: https://doi.org/10.1109/ICAC.2015.58

[22] Signant Health. 2020. State of eConsent Report 2020. Retrieved February 1, 2021 from https://discover.signanthealth.com/2020-eConsent-Survey.html.

[23] Oliver Heinze, Markus Birkle, Lennart Köster, and Björn Bergh. 2011. Architecture of a consent management suite and integration into IHE-based regional health information networks. *BMC Medical Informatics and Decision Making* 11, 1 (Oct. 2011), 58. DOI: https://doi.org/10.1186/1472-6947-11-58

[24] Duncan Hull, Steve R. Pettifer, and Douglas B. Kell. 2008. Defrosting the digital library: Bibliographic tools for the next generation web. *PLoS Computational Biology* 4, 10 (Oct. 2008), e1000204. DOI: https://doi.org/10.1371/journal.pcbi.1000204

[25] N. Huynh, M. Frappier, H. Pooda, A. Mammar, and R. Laleau. 2016. SGAC: A patient-centered access control method. In *Proceedings of the 2016 IEEE 10th International Conference on Research Challenges in Information Science (RCIS'16)*. 1–12. DOI: https://doi.org/10.1109/RCIS.2016.7549286

[26] N. Huynh, M. Frappier, H. Pooda, A. Mammar, and R. Laleau. 2019. SGAC: A multi-layered access control model with conflict resolution strategy. *Computer Journal* 62, 12 (2019), 1707–1733. DOI: https://doi.org/10.1093/comjnl/bxz039

[27] International Organization for Standardization. 2014. ISO 22600-1:2014. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/26/62653.html.

[28] Michael Jefford and Rosemary Moore. 2008. Improvement of informed consent and the quality of consent documents. *Lancet Oncology* 9, 5 (May 2008), 485–493. DOI: https://doi.org/10.1016/S1470-2045(08)70128-1

[29] Joshua Joy, Minh Le, and Mario Gerla. 2016. LocationSafe: Granular location privacy for IoT devices. In *Proceedings of the 8th Wireless of the Students, by the Students, and for the Students Workshop (S3'16)*. ACM, New York, NY, 39–41. DOI: https://doi.org/10.1145/2987354.2987365

[30] Jane Kaye, Liam Curren, Nick Anderson, Kelly Edwards, Stephanie M. Fullerton, Nadja Kanellopoulou, David Lund, et al. 2012. From patients to partners: Participant-centric initiatives in biomedical research. *Nature Reviews: Genetics* 13, 5 (April 2012), 371–376. DOI: https://doi.org/10.1038/nrg3218

[31] Atif Khan and Ian McKillop. 2013. Privacy-centric access control for distributed heterogeneous medical information systems. In *Proceedings of the 2013 IEEE International Conference on Healthcare Informatics*. 297–306. DOI: https://doi.org/10.1109/ICHI.2013.42 ISSN: null.

[32] Barbara Kitchenham. 2004. *Procedures for Performing Systematic Reviews*. Technical Report TR/SE-0401. Keele University, Keele, UK.

[33] S. Kiyomoto, M. S. Rahman, and A. Basu. 2017. On blockchain-based anonymized dataset distribution platform. In *Proceedings of the 2017 IEEE 15th International Conference on Software Engineering Research, Management, and Applications (SERA'17)*. 85–92. DOI: https://doi.org/10.1109/SERA.2017.7965711

[34] Paul Koster, Muhammad Asim, and Milan Petkovic. 2011. End-to-end security for personal telehealth. *Studies in Health Technology and Informatics* 169 (2011), 621–625.

[35] C. S. Kouzinopoulos, K. M. Giannoutakis, K. Votis, D. Tzovaras, A. Collen, N. A. Nijdam, D. Konstantas, G. Spathoulas, P. Pandey, and S. Katsikas. 2018. Implementing a forms of consent smart contract on an IoT-based blockchain to promote user trust. In *Proceedings of 2018 Innovations in Intelligent Systems and Applications (INISTA'18)*. 1–6. DOI: https://doi.org/10.1109/INISTA.2018.8466268

[36] Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado. 2017. Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association* 24, 6 (Nov. 2017), 1211–1220. DOI: https://doi.org/10.1093/jamia/ocx068

[37] Gary Leeming, James Cunningham, and John Ainsworth. 2019. A ledger of me: Personalizing healthcare using blockchain technology. *Frontiers in Medicine (Lausanne)* 6 (2019), 171. DOI: https://doi.org/10.3389/fmed.2019.00171

[38] Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. 2016. Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS'16)*. ACM, New York, NY, 254–269. DOI: https://doi.org/10.1145/2976749.2978309

[39] W. Ma and K. Sartipi. 2014. An agent-based infrastructure for secure medical imaging system integration. In *Proceedings of the 2014 IEEE 27th International Symposium on Computer-Based Medical Systems*. 72–77. DOI: https://doi.org/10.1109/CBMS.2014.87

[40] Weina Ma and Kamran Sartipi. 2014. An agent-based infrastructure for secure medical imaging system integration. In *Proceedings of the 2014 IEEE 27th International Symposium on Computer-Based Medical Systems*. 72–77. DOI: https://doi.org/10.1109/CBMS.2014.87

[41] Eve Maler. 2015. Extending the power of consent with user-managed access: A standard architecture for asynchronous, centralizable, Internet-scalable consent. In *Proceedings of the 2015 IEEE Security and Privacy Workshops*. 175–179. DOI: https://doi.org/10.1109/SPW.2015.34

[42] Paul Malone, Mark McLaughlin, Ronald Leenes, Pierfranco Ferronato, Nick Lockett, Pedro Bueso Guillen, Thomas Heistracher, and Giovanni Russello. 2010. ENDORSE: A legal technical framework for privacy preserving data management. In *Proceedings of the 2010 Workshop on Governance of Technology, Information, and Policies (GTIP'10)*. ACM, New York, NY, 27–34. DOI: https://doi.org/10.1145/1920320.1920325

[43] Pooya Mehregan and Philip W. L. Fong. 2016. Policy negotiation for co-owned resources in relationship-based access control. In *Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies (SACMAT'16)*. ACM, New York, NY, 125–136. DOI: https://doi.org/10.1145/2914642.2914652

[44] David Moher. 2009. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA statement. *Annals of Internal Medicine* 151, 4 (Aug. 2009), 264. DOI: https://doi.org/10.7326/0003-4819-151-4-200908180-00135

[45] Wanda Montalvo and Elaine Larson. 2014. Participant comprehension of research for which they volunteer: A systematic review. *Journal of Nursing Scholarship* 46, 6 (Nov. 2014), 423–431. DOI: https://doi.org/10.1111/jnu.12097

[46] Victor Morel, Mathieu Cunche, and Daniel Le Métayer. 2019. A generic information and consent framework for the IoT. In *Proceedings of the 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and the 13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE'19)*. 366–373. DOI: https://doi.org/10.1109/TrustCom/BigDataSE.2019.00056

[47] A. Norta, D. Hawthorne, and S. L. Engel. 2018. A privacy-protecting data-exchange wallet with ownership- and monetization capabilities. In *Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN'18)*. 1–8. DOI: https://doi.org/10.1109/IJCNN.2018.8489551

[48] Hans-Ulrich Prokosch, Till Acker, Johannes Bernarding, Harald Binder, Martin Boeker, Melanie Boerries, Philipp Daumke, et al. 2018. MIRACUM: Medical informatics in research and care in university medicine. *Methods of Information in Medicine* 57, Suppl. 1 (July 2018), e82–e91. DOI: https://doi.org/10.3414/ME17-02-0025

[49] C. Pruski. 2010. e-CRL: A rule-based language for expressing patient electronic consent. In *Proceedings of the 2010 2nd International Conference on eHealth, Telemedicine, and Social Medicine*. 141–146. DOI: https://doi.org/10.1109/eEMED.2010.27

[50] A. R. Rajput, Q. Li, M. Taleby Ahvanooey, and I. Masood. 2019. EACMS: Emergency access control management system for personal health record based on blockchain. *IEEE Access* 7 (2019), 84304–84317. DOI: https://doi.org/10.1109/ACCESS.2019.2917976

[51] Fatemeh Rezaeibagha, Khin Than Win, and Willy Susilo. 2015. A systematic literature review on security and privacy of electronic health record systems: Technical perspectives. *Health Information Management* 44, 3 (Oct. 2015), 23–38. DOI: https://doi.org/10.1177/183335831504400304

[52] Marco Robol, Travis D. Breaux, Elda Paja, and Paolo Giorgini. 2019. Consent verification under evolving privacy policies. In *Proceedings of the 2019 IEEE 27th International Requirements Engineering Conference (RE'19)*. 422–427. DOI: https://doi.org/10.1109/RE.2019.00056

[53] Ramkinker Singh and Vipra Gupta. 2013. Dynamic federation in identity management for securing and sharing personal health records in a patientcentric model in cloud. *International Journal of Engineering and Technology* 5, 3 (2013), 9.

[54] Rudi Studer, V. Richard Benjamins, and Dieter Fensel. 1998. Knowledge engineering: Principles and methods. *Data & Knowledge Engineering* 25, 1 (March 1998), 161–197. DOI: https://doi.org/10.1016/S0169-023X(97)00056-6

[55] Integrating the Healthcare Enterprise. 2020. *IHE IT Infrastructure ITI Technical Framework*. 1. https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf.

[56] Integrating the Healthcare Enterprise. n.d. Advanced Patient Privacy. Retrieved February 1, 2021 from https://wiki.ihe.net/index.php/Advanced_Patient_Privacy_Consents.

[57] Integrating the Healthcare Enterprise. n.d. Audit Trail and Node Authentication. Retrieved February 1, 2021 from https://wiki.ihe.net/index.php/Audit_Trail_and_Node_Authentication.

[58] Integrating the Healthcare Enterprise. n.d. Basic Patient Privacy Consents. Retrieved February 1, 2021 from https://wiki.ihe.net/index.php/Basic_Patient_Privacy_Consents.

[59] Nguyen Binh Truong, Kai Sun, Gyu Myoung Lee, and Yike Guo. 2019. GDPR-Compliant personal data management: A blockchain-based solution. *IEEE Transactions on Information Forensics and Security* 15 (2019), 1746–1761. DOI: https://doi.org/10.1109/TIFS.2019.2948287

[60] Max-R. Ulbricht and Frank Pallas. 2016. CoMaFeDS: Consent management for federated data sources. In *Proceedings of the 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW'16)*. 106–111. DOI: https://doi.org/10.1109/IC2EW.2016.30

[61] J. Patrick Woolley, Emily Kirby, Josh Leslie, Francis Jeanson, Moran N. Cabili, Gregory Rushton, James G. Hazard, et al. 2018. Responsible sharing of biomedical data and biospecimens via the "Automatable Discovery and Access Matrix" (ADA-M). *npj Genomic Medicine* 3, 1 (July 2018), 1–6. DOI: https://doi.org/10.1038/s41525-018-0057-4

[62] Bo Yu, Duminda Wijesekera, and Paulo C. G. Costa. 2014. An ontology for medical treatment consent. In *Proceedings of the 9th International Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS'14)*. 72–79.

[63] Lelethu Zazaza, H. S. Venter, and George Sibiya. 2019. The current state of electronic consent systems in e-health for privacy preservation. In *Information Security*. Communications in Computer and Information Science, Vol. 973. Springer, 76–88.

Received April 2020; revised September 2020; accepted November 2020