Review on privacy and trust methodologies in cloud computing

Stavros Simou[1][0000-0002-1038-0065], Aikaterini-Georgia Mavroeidi[1] [0000-0002-3270-880X], Christos Kalloniatis[1] [0000-0002-8844-2596]

[1] Privacy Engineering and Social Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, University Hill, GR 81100 Mytilene, Greece
ssimou@aegean.gr, kmav@aegean.gr, chkallon@aegean.gr

Abstract. The vast adoption of cloud computing has led to a new content in relation to privacy and security. Personal information is no longer as safe as we think and can be altered. In addition, Cloud Service Providers (CSPs) are still looking for new ways to raise the level of trust in order to gain popularity and increase their number of users. In this paper, a systematic literature review was carried out to identify the different methodologies, models and frameworks regarding privacy engineering and trust in cloud computing. A detailed review is produced on the specific area to bring forward all the work that has been carried out the recent years using a methodology with a number of different steps and criteria. Based on the findings from the literature review, we present the state-of-the-art on privacy and trust methodologies in cloud computing and we discuss the existing conventional tools that can assist software designers and developers.

Keywords: Privacy, Trust, Methodologies, Privacy Requirements Engineering Methods, Cloud Computing.

1 Introduction

After a hesitant and uncertain start, cloud computing has prevailed over the completion in Information Technology (IT) and became dominant in the field. Although there are certain issues concerning users' privacy and security, due to its transformational nature, cloud computing continues to expand and has been accelerated especially in the pandemic according to Flexera report [1]. The same report highlights the role of cloud computing in the competition and its importance on the ways an organization approaches its cloud strategy.

Cloud computing dominant utilization poses new challenges for both providers and consumers, especially as far as privacy protection is concerned [2]. Users' privacy is of vital importance and the cloud vendor should provide all the necessary actions to warrant that no personal information will alter or leak. Despite the success of cloud technology, vendors still cannot provide transparency to users so that the users be able to know where their data resides, how it is managed and who has access to it, at all times. Razaque et al. [3], agrees that in order to build trust between users and cloud computing, Cloud Service Providers (CSPs) should find ways to preserve data privacy at all times.

Several scandals concerning stolen or misused data have been revealed, resulting in the users losing their trust in who they allow to handle their data [4].

The past years a number of researchers focused on finding solutions regarding on one hand the privacy in the cloud and on the other hand, to establish trust between users and companies/providers, among others. Several reviews have already been published regarding privacy requirements methods and trust methods [5-7]. Trust and privacy are two interdependent concepts, as by protecting users' privacy, trust is increased. So, a review which connects both methodologies is needed. Within this paper, a literature review is taking place regarding privacy engineering methodologies and users' trust in cloud computing. A detailed review is produced, based on the review of the area in order to bring forward all the work that has been carried out both in privacy engineering methodologies and users' trust. In addition, this research introduces the privacy engineering methods used for the analysis and elicitation of privacy requirements. Various privacy engineering methodologies have been proposed aiming to support software developers at the early stages of system design.

The remainder of the paper is as follows: Section 2 describes the literature review methodology (e.g., search method, keywords, exclusion, and inclusion criteria). In Sections 3 and 4, a presentation of the existing privacy engineering and trust methodologies in cloud environments is performed while in Section 5 a discussion on the findings of the study is presented. Finally, the conclusion of the study is expressed in Section 6.

2 Methodology

In order to produce this literature review, a number of different steps were followed. Since there are two areas (privacy and trust methodologies) with different content, the keywords used in the search were divided into two different categories. In this case, two literature reviews were conducted, the first one concerns privacy methods and the second one trust methods. Studies which are written in English were searched in Google Scholar, Scopus, IEEExplore, ACM Digital library and Google.

Table 1. Search strategy

Academic databases searched	IEEExplore Scopus ACM Digital library
Other data sources	Google (including google scholar)
Target items	Journals papers Workshop papers Conference papers Chapters
Search applied to	Titles Abstracts Keywords

Language	English
Publication period	From 2000 until today (privacy methods) From 2011 until today (trust methods)

Two main research questions were addressed. The aim of the first research question is to find which privacy engineering methodologies have been published and which steps have been recorded. The aim of the second research question is to record all trust methodologies and their phases. The search was applied to the titles, abstracts, and keywords of studies to be sure that each study will be appropriate for this research. The document type for both reviews was selected to be "conference papers", "journals", "workshop papers" and "chapters" while the publication stage was "final". The search strategy is presented in Table 1. Due to the large number of results, it was needed to define inclusion and exclusion criteria, as presented in Table 2.

Table 2. Inclusion and exclusion criteria

	Eligibility criteria
Inclusion criteria	Academic journal, conference, workshop, chapter papers which include privacy engineering methodologies and trust methodologies. Studies which include steps regarding methods Papers written in English. Publication date: since 2011
Exclusion criteria	Duplicates Studies without steps Studies whose full text is not accessible Papers available only in the form of abstracts Short papers Posters

The first keywords were used to search for results in the databases for the privacy methodologies, while the second keywords for the trust methodologies in relation to privacy. Regarding privacy engineering methods, the search string used to collect studies, was constructed using the Boolean OR and the Boolean AND, namely the search terms "privacy requirements engineering" OR "privacy requirements methods" OR "privacy frameworks" OR "privacy approaches" AND "cloud computing", were used. The search was limited to the last twenty years. The search results returned 220 papers, and after excluding duplicates, studies whose full texts were not accessible, short papers, posters, and papers in the form of abstracts 79 were screened. After reading all these, we came up to 11 papers.

Regarding trust methods, the search string used to collect studies, was also constructed using the Boolean OR and the Boolean AND, namely the search terms “trust methods” OR “trust frameworks” OR “trust approaches” AND “cloud computing” AND “privacy” were used. The searching process was limited to the last years (since 2011) and the language to English. Regarding the second research questions, the search results returned 712 papers. The next stage was to exclude all duplications, not accessible, short papers and posters. From this process, 46 articles were included. The last stage was to exclude all the irrelevant articles by reading them. The remaining papers that meet the criteria in relation to trust methodologies and privacy were 12. According to the results, most of the methodologies have been published during the last ten years. It is important to note that methods regarding trust, were started to be published in 2012. In figure 1, the publication date of all methods is presented.

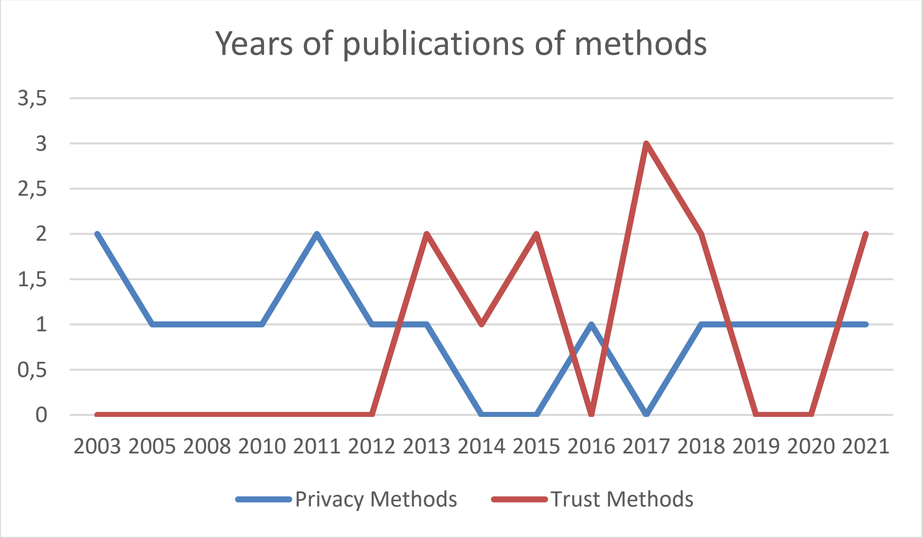

Fig. 1. Privacy and trust methods-publication per year

3 Privacy requirements engineering methods

The consideration of privacy as part of a system’s development process is an important aspect towards the development of privacy-aware systems. A number of privacy engineering methods have been developed in order to support privacy requirements elicitation for various software systems.

In [8], LINDDUN, a privacy threat analysis framework, has been described for the elicitation and fulfillment of privacy requirements. LINDDUN first step concerns the design of a data flow diagram and the identification of threats. As authors mention, there are seven types of threats, Linkability, Identifiability, Non-repudiation, Detectability, Information Disclosure, Content Unawareness, Policy, and consent Noncompliance. For the collection of threat scenarios of the system, threat trees and misuse cases are implemented. Developers are supported for the selection of the appropriate techniques for the satisfaction of privacy requirements through privacy-enhancing technologies (PET's).

The method SQUARE for privacy [9] is an extension of the SQUARE methodology [10]. The first approach concerns security requirements, while in SQUARE for privacy also the elicitation and prioritization of privacy requirements is presented. The same steps are used in conjunction with the Privacy Requirements Elicitation Technique (PRET tool) [11], which uses a database of privacy requirements based on privacy laws and regulations. According to Kalloniatis et al. [12], PriS method is a goal-oriented approach. PriS considers privacy requirements as organizational goals. This method uses privacy-process patterns to describe the affected organisational processes by the privacy goals. Additionally, the aim is to model organisational processes regarding privacy and to support the selection of the most appropriate techniques and architectures for the satisfaction of these processes. In this method, for the identification of privacy goals eight privacy concepts have to be considered, i.e., authentication, authorization, identification, data protection, anonymity, pseudonymity, unlinkability and unobservability. A formal case tool has been developed for the implementation of this method [13].

In [14], a model-based approach which considers privacy and security requirements has been presented. Specifically, two engineering methods were integrated and Secure Tropos with PriS was developed. Secure Tropos aim is the identification of security requirements. While privacy concepts are also important, Secure Tropos has been extended by introducing PriS method. Thus, security and privacy requirements are considered in parallel at the early stages of system development [15]. The RBAC framework [16] is an agent-oriented framework. The aim is linking privacy requirements and low-level access control policies. Authors present how to model privacy requirements as constraints and contexts of permissions and users' roles in order to define policies.

The STRAP [17] model is based on a structure analysis of privacy vulnerabilities. It is a goal-oriented approach, and the aim is to support developers to identify privacy requirements during development processes. This method includes four steps, namely, Analysis, Refinement, Evaluation, and Iteration. In [18], i* method is presented which focuses on analyzing, modeling and designing the organisation's processes at the early stages of system design. The target of this method is to design a model which captures all the involved actors and their dependencies. A case tool has been developed for this method, called Organisation Modelling Environment (OME) [19].

An interesting approach was published in 2019, where the aim is to support users to identify the privacy requirements in a software system [20]. The recommender-based privacy requirements elicitation approach EPICUREAN includes modelling and data mining techniques to recommend privacy settings to users and describes three phases, Preparation, Training, Application. The Privacy Criteria Method and the PCM tool [21] support agile software developers to elicit privacy requirements. This method can be used with any requirements specification technique. The PCM tool includes eight steps, i.e., Basic Information Specification, Actors Specification, Trust Relation of Actors

Specification, Personal Information Specification, Purpose of Task Context Specification, Privacy Constraint Specification, Risk Scenario Specification, Privacy Mechanism(s) Specification.

In [22], P-RAMS framework is presented for smart-grid-specific privacy requirements, which extends previous privacy requirements engineering approaches. Authors present a threat tree analysis, which delivers a classification of privacy specific threats. In [23], a Core Ontology for Privacy requirements engineering (COPri) was presented. The aim is to support software developers by providing privacy concepts during the elicitation of privacy requirements. It includes five main phases, namely, scope & objective identification, Knowledge acquisition, Conceptualization, Implementation, Validation. In 2021, COPri v.2 [24] was proposed which has been extended based on the feedback received from privacy and security experts. Specifically, authors extended the analysis support and the implementation and validation steps.

4 Trust methodologies

Since the beginning of the cloud computing introduction, users are seeking solutions to keep their data safe and built a level of trust with the ones who host and handle their data. This is a difficult task since it involves different aspects and entities. Nevertheless, many researchers proposed their works and developed trust mechanisms in the cloud. In this section, the trust methodologies, and models, identified in the literature review, are discussed. In order to find recent methodologies and up-to-dated, the years included were dated back to 2011.

In 2013, Wu proposed [25] a trust evaluation model based on the theory of belief functions, also referred Dempster–Shafer evidence theory (D-S) and sliding windows for cloud computing. According to their theory, there is a dynamic form of the interaction evidence, and the trust evaluation involves and depends on interaction between the Cloud Service Provider (CSP) and the Cloud User (CU). The model is simple in execution while the extensibility of the system is improved by allowing only valid interactions to affect the trust degree of entities. The experimental evaluation shows that the success interaction rate of the system is increased due to the identification of the malicious entities and the service provision refusal [25]. The same year Huang categorizes the trust mechanisms for cloud computing in five different categories: reputation based, SLA verification based, transparency mechanisms, trust as a service, and formal accreditation, audit and standards [26]. They developed an informal and abstract framework for analyzing and modeling trust in cloud. A policy-based trust mechanism is used to trust the provider or the service, whenever it conforms to a trusted policy and a presentation of a general structure of evidence-based trust is produced as evidence for trust judgment to support the mechanism.

The following year, the privacy monitoring framework for enhancing transparency in cloud computing [27] is presented by Shabalala. The framework facilitates compliance with privacy laws, regulations and standards, it provides the mechanism that catches the events and alerts the user, and it prevents unauthorized users from accessing confidential data by encrypting data in transit and at rest. It uses an information events and access logs analyzer component to enable user to build a detailed timeline of past events, in relation to its data (where it is stored, who has access, how to protect). The component monitors the operation carried out on the outsourced data. The experimental results show that the framework is easy to use, it provides transparency on how the data is always handled and user awareness [27]. Although the framework could be included in the previous section (section 3), we decided to integrate it in this section since the transparency is a basic ingredient of the trust.

Salih and Lilien, in 2015, proposed a mechanism named Active Privacy Bundles using a Trusted Third Party (APB-TTP) for protecting users' data and privacy in the healthcare field [28]. They use TTPs for maintaining data on the trust levels of visited hosts (VHs) and providing them to APBs upon their request. The issue with this approach is that the authors did not validate the specific mechanism to get a better picture on a real case scenario. Another mechanism to handle users' data in a proper and secure way is presented by Polash and Shiva that focuses on users' transparency in the cloud [29]. It presents the cloud service certification process and moves a step forward by providing a comparative analysis of the existing cloud service certification organization. The authors point out the importance of the confirmation of the standards and best practices the providers follow (cloud service certification process) and present the aspects that can help to increase users' cloud confidence. By doing so, they assist customers to judge the acceptability of a cloud service certification scheme.

Based on the third-party auditor (TPA), Razaque and Rizvi presented a triangular data privacy-preserving (TDPP) model that supports public auditing in cloud environment and provides the line of trust among all the key stakeholders [3]. The model authenticates all the stakeholders, ensures the integrity of the TPA, enforces the Service Level Agreements (SLAs) between users and cloud providers, ensures the message authentication at the provider side and determines the conspiracy role of TPA. The authors provide detailed tests in a variety of different scenarios in order to evaluate the model. The results show that the model effectively develops a TPA-centric trust between users and providers by minimizing the insider threats and increasing fairness in the cloud environment [3].

In 2017, Drucker and Gueron used a Private Trusted Proxy (PTP) to extend the idea of Trusted Proxy (TP) in order to guarantee the data privacy [30]. It uses a secret key that is not shared to an adversary and provides user's confidentiality. Besides the usefulness of the specific scheme, the evaluation tests of the PTP solution seems to be more effective and gives better performances (the time for executing the modeled workload for the entire data as a function of the latency) in relation to the PT solution [30]. The privacy and trust issues between the user and the cloud service provider are also identified by another research [31]. In order to address the issues, a Security Assertion Markup Language (SAML) with Single Sign-On and hash-based encryption algorithm is used. The algorithm provides secure communication between the user and the provider, in that way, the trust issue between them can be overcome. The proposed system also provides a high level of security for user identity management.

Mbanaso and Chukwudebe proposed a configurable policy-based architecture to provide trust, confidentiality and privacy at the same time [32]. The policy mechanism specifies the data to be shared, who is shared with, and the privacy and confidentiality settings of the data. The policy framework also uses Requirements (used to express a party's obligations) and Capabilities (used to express the competences of the relaying party) form elements to guarantee confidentiality, trust and privacy dynamically and concurrently between two or more cooperating entities. Authors are making a number of assumptions in order to provide the required trust and end-to-end privacy and confidentiality.

The use of cloud computing in the healthcare domain is a special case since privacy is of vital importance. Marwan et al. proposed a framework for fueling the integration of cloud applications in the healthcare sector [33]. The framework is based on segmentation and genetic algorithms in order to afford optimal privacy protection. They use a trusted third party to provide secure data exchanges between users and CSPs and Secure Sockets Layer (SSL) technique to establish a secure connection for transmitting medical records. The data is also encrypted before the transfer. Their results show that the framework provides an adequate image analysis using public clouds and improves both security and performance, while ensuring privacy protection [33].

The same year, Tahir and Rajarajan proposed another framework in relation to encryption in the cloud and the trusted servers [34]. The authors use the cryptographic approach of Searchable Encryption (SE) that is based on probabilistic trapdoors and facilitates search over encrypted data stored on the Hyperledger-Fabric, a blockchain technology. The data is encrypted and stored on the blockchain while the search is realized with the use of a privacy-preserving SE. The use of Hyperledger-fabric provides permissioned membership, scalability, higher level of trust and modular architecture. The security analysis that applied on the framework shows that it provides higher level of security and privacy guarantees [34].

Finally, in 2021, Qin et al. suggested that due to the lack of trust among edge computing participants and users' continuous concern over privacy, new solutions need to be presented in the marine field [35]. In order to preserve data privacy, they proposed to use blockchain technology with the federated learning technology to preserve privacy and security under an edge computing framework. The proposed framework on one hand addresses the security issues at node level by using the block chain and on the other a proof of parameters quality (PoQ) consensus mechanism is designed [36].

5 Discussion

Even though a great number of researchers dealt with the issue of trust in cloud computing and proposed various solutions in regards methodologies, frameworks, models and mechanisms, only few of them took under consideration the trust in relation to privacy. Some researchers, in order to develop a policy approach or a framework for the trust in cloud environments, they focused on trust mechanism analysis. They identified different trust attributes and mechanisms and categorized them to address specific aspects of trust. A user can use the framework/policies to compare different services (CSPs) to make trust judgment on the service or the CSP. Comparing different trust mechanisms in the cloud the user can evaluate the level of trust between cloud service providers and choose accordingly. They use techniques to find the level of interaction and assessment between CSPs and consumers to establish the trust degree of the entities. In that way, they identify malicious entities and provide security to all stakeholders. They produce reports to evaluate cloud services' processes and procedures to aware users about the services' standards. The reports provide the cloud service with a certification process resulting in the increase of trust among cloud consumers. They use auditing methodologies to assess CSPs and their services. Cloud users are able to compare the reports, understand the differences and choose the provider that suits him/her.

Other researchers focused on the users control aspect to build trust between user and CSP, using different components for monitoring data while other use Trusted Third Party (TTP) or Third Party Auditors (TPA) for auditing consumers' data on a regular basis. These techniques provide a line of trust among all the key stakeholders and assure privacy in cloud at the required level of trust. The privacy monitoring method can provide the required transparency and enables users to comprehend how their data is handled.

Another approach is the use of cryptography to encrypt stored data. To safely process digital data in an untrusted cloud environment, encryption techniques can be used to ensure confidentiality and privacy protection. This approach guarantees a higher level of security and privacy of the consumers' data, increases the cloud providers' trust and assures the quality and effectiveness of the services. Consumers feel confident using cloud services since their personal and sensitive information cannot be used in case of a breakage. New technologies such as blockchain and federated learning are used to establish trust among participants. These technologies can be used to solve security and privacy issues and establish trust among participants. The encryption technology guarantees the security of data on the chain while the federated learning improves computational efficiency.

The specific solutions cover different areas in relation to applicability. Most of them are used as a generic solution to establish trust between the parties involved. There are also approaches specialized in the demanding sector of healthcare with its sensitive personal data. The people responsible for processing medical digital records should ensure the privacy and confidentiality of the users and maintain trust at all times using appropriate tools and methods. The Marines is another field of applying new technologies to provide privacy protection and increase the level of trust.

The software industry is growing rapidly, and many methodologies and tools have been published in order privacy protection to be ensured while using systems. In the previous Section, a number of them are presented based on the results of the review. They include several processes regarding the elicitation and analysis of privacy requirements which may differ in parts but in general their common aim is to ensure that privacy requirements will be considered from the early stages of the software lifecycle until the late design stages prior to implementation.

Another part which is interesting to mention is the differences regarding the privacy concepts that each method includes. For instance, in PriS eight privacy concepts are reported, namely authentication, authorisation, identification, data protection, anonymity, pseudonymity, unlinkability, and unobservability, while in LINDUUN authors focus on Linkability, Identifiability, Non-repudiation, Detectability, Information Disclosure, Content Unawareness, Policy, and consent Noncompliance. Additionally, there are some methods which do not focus only on privacy. In i* method security requirements are also considered along with privacy requirements. Similarly, Secure Tropos with PriS supports the parallel identification of security and privacy requirements of a system. Several differences can be recognized regarding the content of all methods. STRAP succeeds privacy requirements analysis through a structured analysis of privacy vulnerabilities and it included four steps, while EPICUREAN includes modelling and data mining techniques to recommend privacy settings to users and describes three phases.

6 Conclusion

Cloud computing is an important technology and most of the companies and organizations now days are cloud dependent. The aim of this paper is to introduce a systematic literature review on the existing privacy engineering and trust methodologies in cloud environments. We identify both the privacy engineering methods that have been developed in order to support privacy requirements elicitation for various software systems and the trust methodologies and models that will raise the level of trust between the parties.

A series of privacy methodologies have been introduced in order to support the development of privacy-aware systems. It has been noticed that several steps and requirements are provided but the common part of all privacy requirements engineering methods is to ensure that privacy will be protected in cloud computing systems. Specifically, some of these methods have proposed specific tools to support their aim which can be used by software developers. On the side of trust methods, the purpose is to ensure that trust level will be increased, and many relevant methods are published to achieve it.

The discussion of the findings presented in this paper contributed to a better understanding of cloud environments and specifically on how to preserve privacy and maintain the trust. Even though a number of steps is in the right direction, there is plenty of work to be done in relation to privacy and trust in cloud. The different techniques have been highlighted and they provide appropriate knowledge aiming to support software designers and developers at the early stages of system design.

Acknowledgements

The research project was supported by the Hellenic Foundation for Research and Innovation (H.F.R.I.) under the '2nd Call for H.F.R.I. Research Projects to support Faculty Members & Researchers' (Project Number: 2550)

References

1. Flexera, State of the Cloud Report, (2021), [online] Available: https://www.flexera.com/blog/cloud/cloud-computing-trends-2022-state-of-the-cloud-report/
2. Cook, A., Robinson, M., Ferrag, M. A., Maglaras, L. A., He, Y., Jones, K., & Janicke, H.: Internet of cloud: Security and privacy issues. In: Shankar, B., et al. (eds) Cloud Computing for Optimization: Foundations, Applications, and Challenges, pp. 271-301. Springer (2018).
3. Razaque, A., & Rizvi, S. S.: Triangular data privacy-preserving model for authenticating all key stakeholders in a cloud environment. Computers & Security, 62, 328-347 (2016).
4. Kaiser, C., Stocker, A., Festl, A., Djokic-Petrovic, M., Papatheocharous, E., Wallberg, A., Ezquerro, G., Ortigosa Orbe, J., Szilagyi, T., & Fellmann, M.: A Vehicle Telematics Service for Driving Style Detection: Implementation and Privacy Challenges. VEHITS, 29-36 (2020).
5. Canedo, E.D. & Bandeira, Ian & Calazans, Angelica & Costa, Pedro & Cançado, Emille & Bonifacio, Rodrigo. (2022). Privacy requirements elicitation: a systematic literature review and perception analysis of IT practitioners. Requirements Engineering. 27. 10.1007/s00766-022-00382-8.
6. Pattakou, A., Kalloniatis, C., & Gritzalis, S. Security and Privacy under a Unified Framework: A Review. International Journal On Advances in Security, Vol. 11, No. 1-2, pp. 39-51, 2018, IARIA
7. Ibrahim, F. A., & Hemayed, E. E. (2019). Trusted cloud computing architectures for infrastructure as a service: Survey and systematic literature review. Computers & Security, 82, 196-226.
8. Deng, M., Wuyts, K., Scandariato, R., Preneel, B., and Joosen, W.: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements, Requirements Engineering 16(1), 3–32 (2011).
9. Bijwe A. and Mead, N. R.: Adapting the SQUARE Process for Privacy Requirements Engineering, 1-32 (2010).
10. Mead, N. R., Hough, E. D. and Ii, T. R. S.: Security Quality Requirements Engineering (SQUARE) Methodology. Carnegie Mellon Software Engineering Institute, Pittsburgh PA (2005).

11. Meis, R., & Heisel, M.: Computer-aided identification and validation of intervenability requirements. Information 8(1), 30 (2017).
12. Kalloniatis, C., Kavakli, E., & Gritzalis, S.: Addressing privacy requirements in system design: the PriS method. Requirements Engineering 13(3), 241-255 (2008).
13. Kalloniatis, C., Kavakli, E., & Kontellis, E.: Pris tool: A case tool for privacy-oriented requirements engineering. In 4th Mediterranean Conference on Information Systems, MCIS, 71 (2009).
14. Islam, S., Mouratidis, H., Kalloniatis, C., Hudic, A., & Zechner, L.: Model based process to support security and privacy requirements engineering. International Journal of Secure Software Engineering (IJSSE) 3(3), 1-22 (2012).
15. Mouratidis, H., Kalloniatis, C., Islam, S., Huget, M. P., & Gritzalis, S.: Aligning Security and Privacy to Support the Development of Secure Information Systems. Journal of Universal Computer Science 18(12), 1608-1627 (2012).
16. He, Q., & Antón, A. I.: A framework for modeling privacy requirements in role engineering. In 9th International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ'03) on Proceedings, pp. 137-146. (2003).
17. Jensen, C., Tullio, J., Potts, C., & Mynatt, E. D.: STRAP: a structured analysis framework for privacy. Georgia Institute of Technology (2005).
18. Liu, L., Yu, E., & Mylopoulos, J.: Security and privacy requirements analysis within a social setting. In 11th IEEE International Requirements Engineering Conference 2003 on Proceedings, pp. 151-161. IEEE (2003).
19. Horkoff, J., Yu, Y., & Eric, S. K.: OpenOME: An Open-source Goal and Agent-Oriented Model Drawing and Analysis Tool. iStar 766, 154-156 (2011).
20. Stach, C., & Steimle, F.: Recommender-based privacy requirements elicitation-EPICUREAN: An approach to simplify privacy settings in IoT applications with respect to the GDPR. In 34th ACM/SIGAPP Symposium on Applied Computing on Proceedings, pp. 1500-1507. Limassol Cyprus (2019).
21. Peixoto, M. M.: Privacy Requirements Engineering in Agile Software Development: a Specification Method. In REFSQ-2020 Workshops on Proceedings. Pisa Italy (2020).
22. Neureiter, C., Eibl, G., Veichtlbauer, A., & Engel, D.: Towards a framework for engineering smart-grid-specific privacy requirements. In IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society on Proceedings, pp. 4803-4808. IEEE, Vienna Austria (2013).
23. Gharib, M., & Mylopoulos, J.: A core ontology for privacy requirements engineering. arXiv preprint arXiv:1811.12621. (2018).
24. Gharib, M., Giorgini, P., & Mylopoulos, J.: COPri v. 2 – A core ontology for privacy requirements. Data & Knowledge Engineering, 133, 101888 (2021).
25. Wu, X., Zhang, R., Zeng, B., & Zhou, S.: A trust evaluation model for cloud computing. Procedia Computer Science, 17, 1170-1177 (2013).
26. Huang, J., & Nicol, D. M.: Trust mechanisms for cloud computing. Journal of Cloud Computing: Advances, Systems and Applications, 2(1), 1-14 (2013).

27. Shabalala, M. V., Tarwireyi, P., & Adigun, M. O.: Privacy monitoring framework for enhancing transparency in cloud computing. In 6th International Conference on Adaptive Science & Technology (ICAST), pp. 1-7, IEEE (2014).
28. Salih, R. M., & Lilien, L. T.: Protecting users' privacy in healthcare cloud computing with APB-TTP. In International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), pp. 236-238, IEEE (2015).
29. Polash, F., & Shiva, S.: Building trust in cloud: service certification challenges and approaches. In Ninth International Conference on Complex, Intelligent, and Software Intensive Systems, pp. 187-191, IEEE (2015).
30. Drucker, N., Gueron, S., & Pinkas, B.: Faster secure cloud computations with a trusted proxy. IEEE Security & Privacy 15(6), 61-67 (2017).
31. George, J. A., Veni, S., & Soomroo, S.: Improving privacy and trust in federated identity using SAML with hash based encryption algorithm. In 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS), pp. 1-5, IEEE (2017).
32. Mbanaso, U. M., & Chukwudebe, G. A.: Requirement analysis of IoT security in distributed systems. In 3rd International Conference on Electro-Technology for National Development (NIGERCON), pp. 777-781, IEEE (2017).
33. Marwan, M., Kartit, A., & Ouahmane, H.: A cloud-based framework to secure medical image processing. Journal of Mobile Multimedia, 319-344 (2018).
34. Tahir, S., & Rajarajan, M.: Privacy-preserving searchable encryption framework for permissioned blockchain networks. In IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1628-1633, IEEE (2018).
35. Qin, Z., Ye, J., Meng, J., Lu, B., & Wang, L.: Privacy-Preserving Blockchain-Based Federated Learning for Marine Internet of Things. IEEE Transactions on Computational Social Systems 9(1), 159-173 (2021).
36. Basha, S. M., Ahmed, S. T., Iyengar, N. C. S. N., & Caytiles, R. D.: Inter-Locking Dependency Evaluation Schema based on Block-chain Enabled Federated Transfer Learning for Autonomous Vehicular Systems. In Second International Conference on Innovative Technology Convergence (CITC), pp. 46-51, IEEE (2021).