International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 3990–4002

Review on Privacy Preservation Methods in Cloud Computing

Mrs.Sahana Lokesh R **Dr. H R Ranganatha**

Assistant Professor, Department of CSE Professor & Head, Department
of ISE
Sri Siddhartha Institute of Technology Sapthagiri College of
Engineering
Tumakuru, Karnataka Bengaluru,Karnataka
sahanalr@ssit.edu.in **hodise@**sapthagiri.edu.in

Abstract

Cloud computing is a pattern that procures contingent way of accessing the network and data is shared to a wide pool of gauge resources where entire infrastructure has shared by millions of users worldwide according to their demand. Even though upgrading in cloud computing technology organizations are slow in accepting it because of security issues which makes the cloud environment to be a origin of data breaching. Privacy is the major obstruction which prevents the adoption of public cloud infrastructure in a company. Some encryption techniques are proposed by many researches to ensure the privacy at some level in cloud. Many encryption methods are designed by researches to achieve privacy in cloud. In today's world the survey made by researches states that, in today's world no particular technique is successful in achieving complete privacy. This paper discuss various privacy preserving schemes in cloud and their comparative study where it gives the clarity on issues related to privacy and several methods to store and access data in cloud.

Keywords: *Anonymization, Cloud , Data splitting, Privacy,*

I. INTRODUCTION

Cloud computing is resistant to security risk [4], because it does not promote backup media, un bound connection to hijack. Cloud computing offers various model for information technology. This technology shares different resources like hardware's, software's and huge amount of information on cloud. As the user shares the information on the cloud, achieving privacy and confidentiality and is the major challenge in the cloud. The data or information published on the cloud contains much sensitive information about many people. The database may be hospital database, bank database. Several public and private firms share their organizational database on the cloud for many different purposes. This database may help many hospitals to track the patient's database, bank database to monitor their customers. All these database contains people sensitive information which should not be disclosed. It is very much essential to conserve the users and data preservation in cloud. As there is a huge rise in the technology of cloud computing the concern for preserving the privacy is also increasing. The data privacy must be achieved when sharing the information with third party and storing the same data over a cloud for long duration of time. There are many different mechanisms like encryption techniques, data anonymization, access control etc[20]. are available to resolve many privacy preserving issues in multi tenancy support, identity management of cloud users to reduce the privacy risk. Several privacy preserving techniques are discussed in this Survey to show how the privacy is preserved and what are all the methods involved in preserving the privacy.

Problem	Description
Information Leakage	Sensitive information will be leaked during data movement across the cloud.
Unauthorized secondary storage	During the data access data owner lacks the complete control over their data in the cloud.
Insufficient user control	Retrieval and accessibility of sensitive information is possible along with backups.

Table1: Some Issues of Privacy preserving

II.PRIVACY PRESERVING METHODS

The research literature on general privacy protection technologies can be classified into three categories, such as privacy by policy, privacy by statistical analysis, privacy by cryptography.

A. Privacy by Access control strategy

Information sharing is a necessary element in many distributed computing ap-plications, for example in review log frameworks, record storing administrations and informing administrations. As an outcome, get control an access on redistributed information is a typical usefulness in distributed computing, since information proprietors might need to control which information customers are permitted to get to some random information thing. This might be the situation, for example, when a medical organization needs to limit access to quiet history to just the approved faculty. In the run of cloud computing administration, access control is authorized by the CSP in the cloud premises. Notwithstanding, when re-appropriating delicate information this technique presents genuine secrecy issues.

Discretionary Access control

Provides an authority to access the resources which are available publicly is done by access control. This method is used for secure data access where it relies on the systems security which gives access to the particular object. The main purpose of the access control in the cloud environment is to restrict the access by unauthorized users and mediates each and every experiment of individual users to the objects that depends on access rights given to the system. Access control in the cloud relies on storage over a cloud,security and access options of the data. There are different ways of access control methodologies are there such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role based access control (RBAC), dRBAC, CoRBAC, ABAC. DAC is a traditional access control method where complete control over all the programs are given to users, here the user access will be given depending on the user identity and the authorization that defined for the open policies. The drawback in DAC is no guarantee on information flow and no restriction on the information usage, this leads to confusion on information usage and this leads to information loss and also the information can be easily hacked by the third party.

Mandatory Access Control

To overcome the limitations of DAC, MAC has introduced here access to the particular object is allowed only if some relation is satisfied. MAC takes the hierarchical approach depends on security level. MAC achieves greater security than DAC where the information flow in DAC is poorly managed but in MAC information flow is controlled based on the level of security assigned where it assigns the security clearance to each user. The considerable limitations in MAC is it cannot able to modify the security level once the level of security is identified to particular subject. To overcome the limitations of MAC another technique called Role Based Access Control (RBAC) has evolved.

Role Based Access Control

RBAC is one of the access control technique where access decisions are made on the basis of roles and responsibilities of the individuals within the cloud environment. RBAC provides hierarchy of roles and dependent on applications. Roles are assigned based on their least privilege of the particular objects which will helps to reduce the information damage by the intruders. RBAC has a several issues in allocating the user privileges. Family of four models are proposed in RBAC96[12]. In RBAC rights will be associated with roles and users and members will be made with appropriate roles. RBAC0 represents the core concepts of the model the RBAC specifies Permission-Role Assignment and User-Role Assignment which defines the relationship between three entities Users(U), Roles (R) and Permissions [12].Every user can be a member of various different roles and each role may have multiple users, in this context permission will be allocatated to many roles and roles may have multiple permissions. RBAC0[9] made structured by adding the roles hierarchy to represent the degree of authority and users responsibilities.

RBAC0: It consists of important concepts of the Model. The model includes three entities Users(U), Roles(R), Permissions. The relationship between these entities is defined by User-Role Assignment and Permission-Role Assignment [12]. A user can be member of many roles and each role can have many users.in this case Permission can be assigned to many roles and a role can have many permissions. Role hierarchy has been added to RBAC0 [15] for structuring roles to represent users responsibilities and degree of authority.

Attribute Based Access Control (ABAC) solves the drawback of RBAC by specifying the access control on set of user attributes. ABAC is more secure, flexible and scalable by providing hierarchical structure. ABAC is not much suitable for large distributed systems this problem will be solved by another method called distributed RBAC(dRBAC). dRBAC overcomes the limitations of giving access control for multiple organizations. dRBAC method derives high space complexity and high time complexity since there is a increasing nature of cloud users.

B .Privacy by Data Splitting

Information parting is an insurance system dependent on dividing sen-sitive information and putting away the pieces in clear structure in isolated areas. Parts ought to be with the end goal that a solitary piece neither permits re-recognizing the subject to whom it compares nor uncovers private data that can be connected to a specific subject. For instance, in the event that a piece comprises of the estimations of a property 'Determination', at that point obviously simply knowing a rundown of findings is futile to an interloper, be-cause he can't connect them with the comparing subjects. Inside the cloud situation, information might be redistributed by a neighborhood intermediary performing information parting to either separate cloud accounts inside the equivalent CSP, or to various mists, every one keep running by an alternate CSP giving a similar sort of administration[18][31]. For parting based information assurance to be powerful, capacity areas ought to stay free and unlinkable, so that CSPs can't conspire to total halfway information in the expectation of breaking information security. The work process of the information parting and capacity procedure is delineated in the below fig. Initially, the intermediary gets from the client the information to be re-appropriated, and evaluates the exposure dangers. To do as such, the intermediary depends on the security necessities characterized by the client (Step 0), which express the arrangement of qualities that may cause re-distinguishing proof; that is, which traits are identifiers or quasi identifiers.

The intermediary at that point chooses how information are part and what number of capacity areas are expected to avert exposure; each bit of information that can be securely put away together establishes an information piece. It likewise stores the parting standard and the capacity areas in a nearby database (Step 2) so the framework can appropriately process future questions on split information and total the fractional outcomes. At last, it advances every datum section to a different CSP (Steps 3).

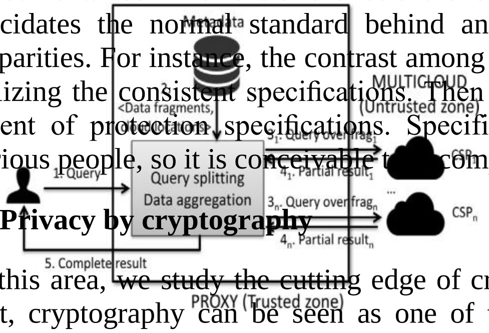

Fig 2.1:Data splitting mechanism

As such, the splitting procedure is lossless that is, it is conceivable to reconstruct the outcomes that would be gotten on the first informational index without putting away this informational index on neighborhood premises and preserving privacy.

Using Probabilistic Hybrid Logics

Hsu et al. proposed a mix of essential crossover rationale and quantitative vulnerability rationale with a fulfillment administrator. This method is featured separately in correlation with the other methodology because of its unique highlights. The rationale is expressive and flexible enough to speak to many existing protection criteria, for example, k-anonymity,l-diversity, t-closeness, and d-disclosure[16]. The fundamental commitment of the rationale is twofold. From one viewpoint, the consistency of the system elucidates the normal standard behind an assortment of protection prerequisites and features their disparities. For instance, the contrast among syntactic and semantic security criteria is effectively seen by utilizing the consistent specifications. Then again, the sweeping statement of the structure broadens the extent of protection specifications. Specifically, one can indicate heterogeneous necessities between various people, so it is conceivable to accomplish customized security specification.

C. Privacy by cryptography

In this area, we study the cutting edge of cryptographic strategies arranged to distributed computing. In fact, cryptography can be seen as one of the most grounded and most basic structure obstructs in a considerable lot of the security plans conveyed to address protection worries in the cloud. Current cryptography has developed by tending to different true security needs, a large number of which apply to distributed computing. As a field, cryptography considers a wide scope of data secu-rity goals, client designs and functionalities.

Searchable Encryption Scheme

Searchable Encryption Scheme (SES) is a cryptographic technique that allows to search specific information in an encrypted data. There are several methods in this scheme like practical techniques, psuedorandom function, sequential scan and several cryptographic schemes[22] were used.all these methods easily supports searching methodology and gives fast result.The limitation is the sequential scan is conducted on whole encrypted data which is not suitable for large sized data and causes overhead in updating the index. Next to this is symmetric public key encryption, secure search is made on encrypted data on cloud but it is very costly in terms of computation. Later Boolean keyword search technique is introduced, search is made using Boolean operators like AND,OR and NOT. This is efficient and comfortable for small easy information needs but this method doesn’t support document ranking to overcome this ranked keyword searchable encryption technique has evolved where relevance score is employed to make a secure searchable index. This method enhances system usability by reurning the matching files in the ranked order. This technique eliminates the network traffic but no concern with privacy.

Homomorphic encryption

These are cryptosystems that empower processing on encoded information. Homomorphic encryption (HE) goes under single-peruser designs, and it enables clients to encode their information with the goal that tasks on the produced ciphertexts can be done so that they mean number juggling activities on the fundamental plaintexts. In the history, homomorphic encryption plans[19] are characterized in three classifications as indicated by their homomorphic properties:

Partially Homomorphic Encryption (PHE) plans bolster only a solitary math activity on ciphertexts. In the event that the activity on ciphertexts yields the encoded variant of the entirety of the cor-reacting plaintexts, at that point the homomorphic plan is called additive.

Somewhat Homomorphic Encryption (SHE) plans bolster both expansion and increase of ciphertexts, however by and by they permit a set number of tasks. Most SHE plans concede countless augmentations and few items on ciphertexts. This constrains the calculations that can really be re-appropriated to the cloud, thus it confines the appropriateness of SHE conspires for specific applications.

Fully Homomorphic Encryption (FHE) plans bolster an unlim-ited number of the two increments and duplications on ciphertexts. By scrambling data in an a little bit at a time style, we note that expansion and increase can be deciphered as XOR AND doors which are complete for the class of Boolean circuits.

D. Privacy by Anonymization Models

K-Anonymity

K-Anonymity is a model of security protection where each record distributed on its QI property must be unclear from in any event (k-1) others. The quasi-identifiers are the credits accessible to an enemy with the end goal that a tableT satisfies k-anonymity if there are k−1 other tuples ti1, ti2,. To the degree that t[C] = ti1 [C] = ti2 [C] =. For all C = tik−1 [C].[3]. The security gave by k-anonymity that strategies are straightforward, and in the event that a table fulfills k-anonymity for some worth k, at that point any individual who knows just one person's quasiidentifier qualities can not distinguish that person's relating record with certainty more prominent than 1/k [4]. While k-anonymity shields from exposure of personality, it doesn't give sufficient insurance against revelation of characteristics. Numerous scientists have noticed this, for example [5, 8, 11]. Two attacks have been recognized in this technique a).Homogeneity attack b) Background Knowledge attack.

Id	Zipcode	Age	Disorder
1	14278	33	Heart disease
2	14233	35	Heart disease

3	14266	36	Heart disease
4	45455	55	Gastriris
5	45477	63	Heart disease
6	45499	57	Cancer
7	67873	44	Heart disease
8	67805	47	Cancer
9	67855	49	Cancer

Table 2:Original Table

Id	**Zipcode**	**Age**	**Disorder**
1	142**	3*	Heart disease
2	142**	3*	Heart disease
3	142**	3*	Heart disease
4	454**	>=50	Gastriris
5	454**	>=50	Heart disease
6	454**	>=50	Cancer
7	678**	4*	Heart disease
8	678**	4*	Cancer
9	678**	4*	Cancer

Table 3: 3 anonymous version of Table1

Table I shows the first example. Table II shows the anonymized variant of Table I discusses 3-anonymous information. In table II, assume Ram realizes that, sham is 37-years age man living at Zip code 12378, and he can easily conclude that, he is having Heart related issues by revealing person's identity. This describes homogeneity attack. Since all the delicate qualities esteems are comparable, It got conceivable to decide personality of sham. In the event that Lakshman realizes that Ram's Age and Zipcode, and he is having foundation information [4] that Ram is having less possiblity of having Heart ailment, he can infer that, Ram is having cancer. This background information empowers Lakshman to find Ram's character. To address these restrictions, Machanavajjhala presented l-diversity variety as solid thought of protection [5].

L-diversity

L-diversity is a group-based model of anonymization that helps to preserve data privacy by reducing data representation granularity by generalizing and suppressing data [6]. In L-diversity, a class of equivalence is said to have l-diversity if the sensitive attribute has at least l "well-represented" value. A table is said to have l-diversity if each table equivalence class has l-diversity and if it contains at least l "wellrepresented" values for the sensitive attribute S, a q block is ldiversity. If each q block is at least l-diversity [6, 3], a table is l-diversity. The disadvantage of k-anonymization due to the knowledge attack can be eliminated by diversifying the sensitive attribute values within a block. The l -diversity template prevents privacy protection attribute disclosure [2].

The important propery of L-Diversity is it doesn't permit the information distributer to have indistinguishable subtleties from the adversary. The higher the estimation of l, the more data is expected to avoid conceivably touchy property estimations. Different adversaries may have distinctive foundation data which prompts various inductions. This shields against every one of them at the same time without the requirement for inductions that can be made with Background Knowledge [5].

Id	Age	Zipcode	Disorder
1	33	16745	Stomach ulcer
2	35	16800	Headache
3	55	15249	Gastriris
4	57	15200	Gastriris

Table 4: Original Pattern

Id	Age	Zipcode	Disorder
1	3*	160**	Stomach ulcer
2	3*	160**	Headache
3	5*	152**	Gastriris
4	5*	152**	Stomach ulcer

Table 5: 2 diversity micro data

At the point when the sensitive qualities in a equivalence class are differ in nature but semantically similar, an enemy can learn significant data. In Table 11, think about that, an attacker knows Amogh's age is around 20 and realizes his postal district. Indeed despite the fact that the qualities are various, stomach ulcer and gastritis are stomach related illness. In this way, he can come to the conclusion that Amogh is having stomach related illness. To conquer such issues, another methodology proposed called as T-closeness.

T-closeness

In this methodology, privacy can be estimated as far as data picked up by the observer. An observer can pick up data dependent on earlier conviction before observing the discharged information and post conviction in the wake of seeing the discharged information. Thus, the data gain is can be spoken to as the distinction between the prior belief and the postirier belief. The methodology represents the data gain into two sections: about the entirety populace in discharged information and about the particular people.

Consider A0 as an earlier conviction of an onlooker and A1 is conviction of an eyewitness changed subsequent to seeing the summed up information. The eyewitness increases some more data by knowing quasiidentifier values in proportionality class and changes his conviction to B2 dependent on expecting to which equality class the individual has a place with.

E. Perturbative masking

Perturbative masking comprises in producing an altered form of the informational collection to such an extent that the veiled qualities can be seen as unique qualities in addition to some noise. Thus, the individual masked values are not honest by and large. However, perturbative masking may safeguard the factual properties of the original information better than non-perturbative masking. The known pertubative masking echniques are:

Noise Addition: Each record in the original data set is added a noise vector. For example, if the noise vector is drawn from a $N(0, \alpha\sum)$ distribution, where $\sum$ is the variance–covariance matrix of the data set and α is a parameter that defines the amount of noise to be added, the anonymized data can be expected to preserve the original means and correlations [40]. Even though noise addition was in principle only suitable for continuous attributes, it has been recently adapted to handle categorical attributes [41]. It can be applied to both quasi-identifiers and confidential attributes, in order to avoid identity and attribute disclosure at the same time. Since noise is added to individual records independently, noise addition has linear complexity in the number of records, which makes it an efficient option for large amounts of data.

Data Swapping: It arbitrarily trades the estimations of characteristics among various records [35]. Along these lines, univariate distribu-tions are actually safeguarded. On account of numerical traits, esteem trades are confined inside a specific range with the goal that the difference covariance grid isn't modified excessively. For categor-ical properties that can be positioned, just trades between classes whose positions are not very unique are made (this variation is known as rank trading). Expansions of trading for ostensible cate-gorical traits that have no characteristic positioning can be found in [42,43]. As verified by [44], information trading has an elevated level of client acknowledgment as the qualities themselves don't endure any adjustment. It very well may be applied to semi identifiers as well as con-fidential traits; regardless, the connection among characters and secret qualities is adjusted, which forestalls characteristic revelation.

Microaggregation: It bunches records into bunches containing each in any event k comparative records and discharges the normal record estimation of each gathering [45]. The more comparable the records in a group the more data utility is preserved.

Moreover perturbative techniques may create untruthful qualities at a record level, they have a few points of interest over the non-perturbative strategies discussed below with respect to information utility conservation. Such promotion vantages make them ideal on the off chance that we are for the most part keen on outsourcing total calculations on enormous informational indexes to the cloud.

F. Non-Pertubative masking

Non-perturbative masking doesn't modify the honesty of the information, in spite of the fact that it diminishes their exactness. The veiled information are gotten from the first information through partial supperssions or reduction of detail, yet they remain honest [36]. The primary strategies that can be utilized to re-appropriate information by means of non-perturbative masking are:

Sampling: The masked information are an example of the original data, which is understood as the population. Along these lines, if an intruder iden-tifies a remarkable record in the discharged information (test), he can't be certain it was one of a kind in the original data(populace), which defeats re-distinguishing proof. The lighter the sampling fraction, the more protection [37], despite the fact that the likelihood of discharging pop-ulation uniques is rarely zero.

Local suppression: In the event that a mix of Quasi identifier trait esteems is uncommon (that is, shared by too not many records), this may leads to re-distinguishing proof (personality revelation). Local suppression is a counter measure that works by stifling certain property estimations (for example supplanting them with missing qualities) so as to build the quantity of records sharing the mix, which decreases the danger of identity disclosure [38].

Generalization: (a.k.a. global recoding). This is an alternative to local suppression to handle rare combinations: values of the quasi-identifier attributes are recoded into new (more general) categories so as to reduce detail and thereby make combinations less rare and re-identification more difficult [38]. For categorical attributes (e.g., job), generalizations are obtained from value generalization hierarchies, taxonomies or ontologies [39]. For numerical attributes (e.g., age), generalizations correspond to increasingly larger intervals (e.g., 25 → [20 − 30] → [0 − 50]).

Factor/Paper	***f*1**	***f2***	***f*3**	***F4***	***f*5**	***f*6**	***f7***	***f8***
Policy	No	XACML	Hash chain	No	No	Group key manageme nt	No	Anonymous ID managemen t
Proxy	Yes	No	Encryption proxy	No	No	No	No	No
Access control	No	Role based	Fine grained	No	No	Attribute based	Fine grained	No
Encryption	SSE	No	No	AES/ MD5	XML signatur e	No	Homomorp hic,oneway trapdoor	No

							function	
Signature	Yes	No	No	No	No	No	No	No
Central authority		No	No	No	Yes	No	No	No

Table2: Comparision of Privacy preserving Methods

III. DISCUSSION

Literature survey introduces various privacy preserving schemes and we have made a comparative study. Various techniques are proposed by many researchers to ensure the privacy. Researches proposed many access control mechanisms and providing the access privilages are also restricted in such a way who and which part of data has to access by the user. This access control also make available on the basis of user roles, policy based, attribute based, fine grained, course grained access control schemes along with this many cryptographic methods have implemented on files to secure the data from privacy breaches. Some of the mechanisms like multilevel encryption, homomorphic encryption, XML encryption, Attribute based encryption are used to move the data to achieve data authentication and privacy. Authors have discussed many key management policies and group management services which are used for access control based on certain limitations which are very essential to satisfy the data access time. It is very much necessary to obtain Certificate revocation and controls to achieve security, but these mechanisms supports for static file contents but failed to support data updates and data deleting services. In such cases, the entire file need to perform re-encryption and whole file replacement. But this kind of mechanism leads to more burden. Many authors discusses proxy access control to users where the owner not necessarily present but there is a chance of proxy failure at the stage of heavy traffic where it leads to the failure of whole system. To overcome this Homomorphic encryption is introduced but it was not successful in supporting all type of operations on the data. Many cryptographic schemes have introduced by many researchers but no complete security solution is successful in ensuring the privacy.

IV. CONCLUSION AND FUTURE WORK

Large number of people are currently using Cloud computing technology for digital data access and retrieving several services are deployed on cloud servers. Since the data storage and data retrieval has increased every day the cloud needs to be more secure and provides reliable service delivery. Many schemes like access control, policy based many encryption algorithms we have seen in the literature survey but using these methods still there is a security and privacy breaches. In future new privacy preserving model for cloud will be proposed by applying anonymization techniques to cloud. This method transforms the data and prevents disclosure of sensitive information by an unauthorized user.

REFERENCES

[1] Y. Chen and R. Sion, “On securing untrusted clouds with cryptography,”in.Proceedings of the 9th annual ACM workshop on Privacy in the electronic society, New Your k,ACM, 2018, pp.109–114.

[2] C. Wang, et al., “Privacy-preserving public auditing for data storage security in cloud computing,” in INFOCOM,2010 Proceedings IEEE, San Diego march 2017, pp. 1–9.

[3] Q. Wang et al. “Enabling public auditability and data dynamics for storage security in cloud computing,” in Parallel and Distributed Systems, IEEE Transactions on, vol. 22, no. 5,IEEE, 2015. pp. 847–859.

[4] R. Laurikainen, “Secure and anonymous communication in the cloud, ”in Aalto University School of Science and Technology, Department of Computer Science and Engineering, Tech. Rep. TKK-CSE-B10, 2010, pp. 1-5

[5] M. Mowbray and S. Pearson, “A client-based privacy manager for cloud computing,” in Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middle waRE, ser. COMSWARE ’09, New York, ACM, 2009, pp. 5:1–5:8.

[6] E.M. Hernandez-Ramirez et al. “A Comparison of Redundancy Techniques for Private and Hybrid Cloud Storage,” in JART Journal of Applied Research and Technology, vol. 10, no. 6, pp. 1-9, 2012.

[7] M. Jensen et al., “Towards an anonymous access control and accountability scheme for cloud computing,” in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, Miami, IEEE. 2010, pp. 540 –541.

[8] D. Chaum and E. Van Heyst, “Group signatures,” in Advances inCryptologyEUROCRYPT91. 1991, pp. 257–265.

[9] P. Angin et al., “An entity-centric approach for privacy and identity management in cloud computing,” in Reliable Distributed Systems, 201029th IEEE Symposium on, New Delhi, IEEE. 2010, pp. 177–183.

[10] .F. Ferraiolo, R. Sanhu, et al., Proposed standard for role-based access control,ACM Trans. Inf. Syst. Secur. 4 (3) (2000) 224–274..

[11] M. Blanton, “Online subscriptions with anonymous access,” in Proceedings of the 2008 ACM symposium on Information, computer and communications security, ser. ASIACCS ’08, New York, ACM. 2008, pp. 217–227.

[12] J. Camenisch and A. Lysyanskaya, “Signature schemes and anonymous credentials from bilinear maps.” in Advances in Cryptology– CRYPTO2004, 24th Annual International Cryptology Conference, Santa Barbara, California, USA. 2004, pp. 56–72.

[13] R. Lu et al., “Secure provenance: the essential of bread and butter of data forensics in cloud computing,” in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS ’10, New York, ACM, 2010, pp. 282–292.

[14] Fischer-Hubner, IT-Security and Privacy: Design and Use of PrivacyEnhancing Security Mechanisms, Springer-Verlag, Berlin, 2001.

[15] . Spiekermann, L.F. Cranor, Engineering privacy, IEEE Trans. Softw. Eng. 35 (1)(2009).

[16] . Ni, E. Bertino, C. Brodie, C.M. Karat, J. Karat, J. Lobo, A. Trombetta, Privacy-aware role-based access control, ACM Trans. Inf. Syst. Secur. (TISSEC) 13 (3) (2010) 35–43.

[17] O. Goldreich, S. Micali, and A. Wigderson, “How to play any mental game,” in Proc. 19th Ann. ACM Conf. Theory of Computing, ACM Press, pp. 218–229, Jan. 1987.

[18] A. Fiat and M. Naor, “Broadcast Encryption,” Proc. 13th Ann. Int’l cryptology Conf. Advances in Cryptology (CRYPTO ’93), pp. 480-491, 1994.

[19] I. Iakovidis, “Towards personal health record: Current situation, obstacles and trends in implementation of electronic healthcare records in Europe,” Int. J. Med. Inf. , vol. 52, no. 1, pp. 105–115, 1998.

[20] J. Smith, “Distributing identity [symmetry breaking distributed access protocols,” IEEE Robot. Autom. Mag., vol. 6, no. 1, pp. 49–56, Mar. 1999.

[21] . He, 2003,Privacy enforcement with an extended role-based access control model. Tech. rep. TR-2003-09, Department of Computer Science, NorthCarolina State University.

[22] G. Karjoth, M. Schunter, A privacy policy model for enterprises, in: Proceedings of the 15th Computer Security Foundations Workshop, IEEE, Los Alamitos, CA, 2002, pp. 271–281..

[23] . Karjoth, M. Schunter, A privacy policy model for enterprises, in: Proceedings

of the 15th Computer Security Foundations Workshop, IEEE, Los Alamitos, CA,

2002, pp. 271–281.

[24] M. Luby, M. Mitzenmacher, M. Shokrollahi, and D. Spielman, “Efficient erasure correcting codes,” IEEE Trans. Inf. Theor., vol. 47, no. 2, pp. 569–584, Feb. 2001.

[25] R. Canetti, “Universally Composable Security: A New Paradigm for Cryptographic Protocols,” Proc. 42nd IEEE Symp. Foundations of Computer Science (FOCS ’01), pp. 136-145, Oct. 2001.

[26] E. Bertino and E. Ferrari, “Secure and Selective Dissemination of XML Documents,” ACM Trans. Information and System Security, vol. 5, no. 3, pp. 290-321, 2002.

[27] J. Domingo-Ferrer, “A provably secure additive and multiplicative privacy homomorphism,” in Proc. ISC’02. LNCS, Heidelberg, Germany, Springer, vol. 2433, pp. 471–483, 2002.

[28] M. Luby, “LT codes,” in Proc. 43rd Symp. Found. Comput. Sci., pp. 271–280, 2002. [15] Y. Dodis, J. Katz, S. Xu, and M. Yung, ‘‘Key-insulated public key cryptosystems,’’ in Proc. EUROCRYPT, pp. 65---82, 2002.

[29] G. Miklau and D. Suciu, “Controlling Access to Published Data Using Cryptography,” Proc. 29th Int’l Conf. Very Large Data Bases (VLDB ’03), pp. 898-909, 2003.

[30] D. Boneh, X. Ding, and G. Tsudik, “Fine-grained control of security capabilities,” ACM Trans. Internet Technol., vol. 4, no. 1, pp. 60–82, 2004

[31] C. Fruhwirth, “LUKS On-Disk Format Specification Version 1.1,” 2005. [Online]. Available: http://code.google.com/p/cryptsetup/

[32] E. Mykletun, J. Girao, and D. Westhoff, “Public key based crypto schemes for data concealment in wireless sensor networks,” in Proc. IEEE ICC, pp. 2288–2295, 2006.

[33] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage,” ACM Trans. Information System Security, vol. 9, pp. 1-30, Feb. 2006.

[34] J. Li and N. Li, “OACerts: Oblivious Attribute Certificates,” IEEE Trans. Dependable and Secure Computing, vol. 3, no. 4, pp. 340-352, Oct.-Dec. 2006.

[35] N. Ferguson, “AES-CBC+ Elephant diffuser A Disk Encryption Algorithm for Windows Vista,” Microsoft, 2006. [Online]. Available:http://download.microsoft.com/download/0/2/3/0238acafd3bf4a6d-b3d6-0a0be4bbb36e/bitlockercipher200608.pdf

[36] S. S. M. Chow, C. Boyd, and J. M. G. Nieto, ‘‘Security-mediated certificate less cryptography,’’ in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3958. Berlin, Germany: SpringerVerlag, pp. 508---524, 2006.

[37]Chandramouli, A framework for multiple authorization types in a healthcare

application system, in: Proceedings of the 17th Annual Computer Security Applications Conference, IEEE, Los Alamitos, CA, 2001, p. 137..

[38] W.-S. Yap, S. S. M. Chow, S.-H. Heng, and B.-M. Goi, ‘‘Security mediated certificate less signatures,’’ in Applied Cryptography and Network Security (Lecture Notes in Computer Science), Germany: Springer-Verlag Berlin, vol. 4521, pp. 459---477, 2007.

[39] Evfimievski, J. Gehrke, R. Srikant, Limiting privacy breaches in privacypreserving data mining, in: Proceedings of the 22nd ACM SIGMOD-SIGACTSIGARTSymposium on Principles of Database Systems, June 2003, pp.211–222.

[40] C. Ardagna, S. De Capitani di Vimercati, S. Paraboschi, E. Pedrini, and P. Samarati, “An XACML-based privacy centered access control system,” in Proceedings of the first ACM workshop on Information security governance. New York, NY, USA: ACM, pp. 49–58, 2009.

[41] R. Brand, Microdata protection through noise addition, in: Inference Control in Statistical Databases, in: Lecture Notes in Computer Science, vol. 2316, Springer, 2002, pp. 97–116.

[42] M. Rodríguez-Garcia, M. Batet, D. Sánchez, A semantic framework for noise addition with nominal data, Knowl.-Based Syst. 122 (2017) 103–118.

[43] V. Torra, Rank swapping for partial orders and continuous variables, in: Proceedings of the Intl. Conf. on Availability, Reliability and Security (ARES 2009), IEEE Comp. Soc., 2009, pp. 888–893.

[44] M. Rodriguez-Garcia, M. Batet, D. Sánchez, Utility-preserving privacy protection of nominal data sets via semantic rank, Inf. Fusion 45 (2019) 282–295.

[45] K. Muralidhar, R. Sarathy, J. Domingo-Ferrer, Reverse mapping to preserve the marginal distributions of attributes in masked microdata, in: Proceedings of Privacy in Statistical Databases - UNESCO Chair in Data Privacy, Intl. Conference (PSD 2014), 2014, pp. 105–116.

[46] J. Domingo-Ferrer, J.M. Mateo-Sanz, Practical data-oriented microaggregation for statistical disclosure control, IEEE Trans. Knowl. Data Eng. 14 (1) (2002)189–201.

[47] D. Defays, P. Nanopoulos, Panels of enterprises and confidentiality: the small aggregates method, in: Proceedings of the 92 Symp. on Design and Analysis of Longitudinal Surveys, 1993, pp. 195–204.

[48] S. Martínez, D. Sánchez, A. Valls, Semantic adaptive microaggregation of categorical microdata, Comput. Secur. 31 (5) (2012) 653–672.

[49] J. Soria-Comas, J. Domingo-Ferrer, D. Sánchez, S. Martínez, T-closeness through microaggregation: Strict privacy with enhanced utility preservation, in: IEEE Trans. Knowl. Data Eng., IEEE Computer Society, 2016, pp. 1464–1465.