2nd IEEE International Conference on Engineering and Technology (ICETECH), 17th & 18th March 2016, Coimbatore, TN, India.

An Analysis of Privacy Preservation Schemes in Cloud Computing

M. Thangavel,
Professor,
Department of MCA,
Erode Sengunthar Engineering
College, Thudupathi - 638057.
thangavelpamu@gmail.com

P. Varalakshmi,
Associate Professor,
Department of Computer Technology,
Madras Institute of Technology,
Anna University, Chennai - 600 044.
varanip@gmail.com

S. Sridhar,
PG Student,
Department of of MCA,
Erode Sengunthar Engineering College,
Thudupathi - 638057.
veerasri.492@gmail.com

Contact Author: - M. Thangavel, Email-id : thangavelpamu@gmail.com, Phone No: +91 9443213746

***Abstract* – The amount of data usage is high appreciated day by day with the next generation technologies. Technologies encourage the users to perform day to day and research activities in the field of data management, which also improves the automation of such human, machine interaction across the world. To handle the increased data population, in today's scenario the only technology house suggested is cloud data storage. The cloud computing model helps to manage and maintain the data with various services and deployment models. Outsourcing the data in the cloud gives a big relief for data storage in local machines. But, the security of the outsourced data is still an challenging issue. Privacy loss of the user's data affects the reliable service delivery in cloud. Most researchers have proposed some encryption techniques which helps to ensure privacy for a particular level in cloud. Based on the survey done by various researchers, No complete privacy preservation system is available in today's world. In this paper, comparative study on privacy preservation schemes in cloud provides a clear view on the privacy issues and methods to preserve in the cloud data storage.**

Keywords- Privacy, Cloud, Data Security, Access control, Data storage,

I. Introduction

Nowadays, the technology has been developed based on the human population in the world. Lots of technologies are invented today and each one serves to people in different ways. This technologies requires resources like hardware, software for the effective utilization. From the effective utilization it is processed with huge amount of data. The amount of data to handle in this world is completely panic. This situation brings us into a solution cloud computing. Cloud computing is a model for enabling convenient ubiquitous and on demand network access to a shared pool of configurable computing resources. This model provides different services and deployment models. The service models are provided as, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS). The deployment models are provided as Public cloud, Private cloud, Community cloud and Hybrid cloud [1]. Storage of data becomes a major consideration in the technical world. The amount of data to store and maintain is only easier with the help of cloud data storage services. This helps to store any large size of the data at different storage locations. Each location is operated in independent manner. The data storage part is handled by the Cloud Service Provider (CSP). The CSP is a responsible person to monitor and meter for accessing the data. The data storage service offers vary by companies and individuals. The client outsource the data in to the cloud storage. The outsourced data travel from client machine to storage server. A specific cloud service is selected for the outsourced data with suitable platform model. The virtual machine manager will put the data into any managed Virtual Machine (VM) locations. These virtual machines are created and maintained by the Virtual Machine Manager(VMM). A service model for corporations provided as Storage as a Service (STaaS). This is a business model for large size corporations to maintain the business data on a subscription basis. Google, Amazon, IBM are some examples of companies providing cloud data storage services. Outsourcing of data brings out security issues. It is an responsibility by CSP to provide security to the outsourced data and ensure the reliable service to its customers. The data storage must satisfies the Confidentiality, Integrity and Availability (CIA) property of security mechanism. The data must be accessed by the person who is authorized. It is safe to make the data in unknown form. The data must not be modified by unknown or any other persons than owner. These three security properties ensure the data storage service provided in a effective manner.

978-1-4673-9916-6/16/$31.00 ©2016 IEEE

Privacy

In general privacy refers the condition or state of hiding the presence or view. There is a need to attain this state in the places where the confidential things are used such as data and files. In cloud data storage the privacy is need to attain for the data, user identity and on controls. Violation of privacy leads to major failure in the system. To maintain the data privacy, it is possible for a successful deployment and usage of any service.

Privacy issues in cloud

Data in the cloud data storage has maintained at several distributed locations. CSP is the responsible person to maintain all the data securely. If proper security mechanism is implemented the security is violated at the storage service. Data can be accessed only by the person who is authorized. It is possible in this cloud model a CSP can read the client data for his purpose. Some competitor companies of data owner can give some amount to the CSP and get the access for the data. Internal workers in the CSP organization may access the data and give it to the business people for money. Government related data files like tender services, investigation documents, property checks may need by the industrialist. So the person contact the CSP and ask for the data. CSP can give it to the person on the basis of money or any other service. Identity of the famous person data like, Prime Minister, world famous sportsman, Actors personal data are accessed by the malicious persons to do such criminal activities. The access of a user is theft for performing some operation using their data. Some attackers are remove the data from the storage. Threats, malicious software are introduced to this storage for getting access and gain knowledge about the data.

Privacy preservation

Privacy deals with accessibility and availability of sensitive information to the intended recipients. Outsourced data accessed and modified only by the users who are having appropriate access privileges. Consider an organization have prepared and outsource their data in cloud. The outsourced data contents are given to the local administrator to place in cloud. It is recommended to ensure that the administrator cannot view or modify the data contents. After file outsourcing, no one including service provider can view or modify the contents. If service provider or local administrator is trying to read the file contents, it must not be done. Privacy preservation deals with the kind of security in outsourced data. This could be ensured by using Cryptographic techniques.

II. Privacy Preservation Schemes

Data place the major role in the concerned cloud arena. Security issues are arise because of lack in providing secure storage service. Some researchers define and derive some models to preserve the privacy of cloud data storage. The models are as follows:

Greveler et al. designed a Privacy preservation model to protect cloud and local administrators [43]. The machine readable rights and expressions are needed for accessing the data. That is a database is created with set of controls such as roles for users, are defined at the time of application launch. It is unchangeable. author found that a work is to secure the hard disk with set of decryption keys. Keys are to be stored at some space in the system. Microsoft Bit locker is worked based on this approach [19], [22] To store the decryption keys on separate space bit locker uses Trusted Platform Module chip (TPM) [41]. eXtensible Access Control Markup Language (XACML) is an eXtensible Markup Language (XML) based language used to define a fine grained access control policy [26], [27]. A tamper proof hardware token is used to provide access control [8]. Privacy manager with XACML policies are the techniques to provide controls. The author found that these techniques are not safeguarding against attacks as impersonation. The author work is based on some of the methods like TPM on Linux, XML signatures, XML Encryption, and Encryption proxies. Encryption proxy is a system model containing TPM, user and rule engine. Cloud database is stored with user credentials and metadata table information. Users can access the cloud data through the encryption proxy. Full disk encryption is performed with TPM protected key file and stored in proxy's secure storage. If user wants to access the data, he/she need to follow encryption proxy. If the user doesn't have control on existing rule, then access is restricted. This work is combined with several mechanisms. This leads to performance overheads. Each time there is a need for re calculation or redefining such rules. It gives confusion on huge requests. Entire control is on the encryption proxy. Compromising the proxy leads the system failure.

Nabeel et al. provides a fine grained access control with fine grained encryption technique for cloud data [39]. Some other models proposed by various researchers are also encrypting the data before outsourcing. But, it gives a computation and communication overhead. Author proposes a Two Layer Encryption (TLE) technique to address the findings. Coarse grained encryption performed at user side, fine grained encryption at the cloud server side. This model faces an issue on the decomposition of Access Control Policies (ACPs) at the time of two layer encryption. A group key management scheme is used here to addressing it. Some works are applying fine grained access control over encrypted data [12], [16]. For each group communication different symmetric keys are used. Distribution of these keys affects the relationship between data items. The re encryption of data gives computation overhead and the distribution of the keys gives communication overhead. Some approaches limiting the issues by the broadcast key management schemes. These schemes are performing single layer encryption. For user access control policies distribution, the owner needs to maintain at each add/revoke [35], [39], [50]. The fine grained access control allows a user for selective access to content. This task has done using expressive specification of policies. The two model of fine grained access control are, push based and pull based models. Push based models distribute the keys at the time of registration [12], [16]. So, it is difficult to maintain the key secrecy in a dynamic data sharing system. Redistribution of key is overcome but the support of expressive access control policies is not supported [35]. Pull based models required the data publisher to stay online to grant access. Such works ensures this, using third party storage services. Some other works enforce the data owner has the responsibility to enforcing the access control policies and the user privacy from data publisher. Multiple encryption technique is followed in some models. Such works are not concentrating on encrypted data when user is removed, access control policies are changed. Such models are following the Attribute Based Encryption (ABE) technique and some other based on proxy re encryption technique [20], [32]. Basic building blocks of this system are broadcast encryption [4] oblivious commitment based envelope protocols [21] privacy preserving attribute based group key management based on [39], [55], [35], [50], and Single Layer Encryption (SLE) [39]. Then policy decomposition and two layer encryption are discussed. Two layer encryption techniques has six phases as identity token issuance, policy decomposition, identity token registration, data encryption and upload, data downloading and encryption, encryption evolution management. Discussion of experimental results is concern on policy decomposition algorithms and single, two layer encryption techniques. Analysis performed as SLE vs TLE and on security, privacy concerns. This work enlarges the view on privacy issues and techniques followed to overcome it. It performs the two layered encryption with group key management policy to ensure the privacy on outsourced data. It has such overhead on computation at server side and in the access control policies. The author concluded that the attribute based keys, access control policies decomposition are the key to success of this model. And also the future work plan is to extend this model with alternate two layer encryption technique with minimal computation cost for access control policies.

L.A. Dunning et al. proposed an algorithm for anonymous sharing of private among N number of parties [49]. The ID numbers are assigned iteratively to the nodes from 1 to N. The received identities are unknown to the other members of the group. It is also verified that there is no collision in private communication channels use. This is distributed without using a trusted central authority. The newer algorithms are developed over a secure sum data mining operation using Newton‘s identities and Sturm‘s theorem. Markov chain process is used to realize the statistics on the required number of iterations. The computer algebra gives the results closer to the completion rates. Author found that some cloud based tools used for website management are providing access for a server to saw the visitor actions on a site. In a secure multiparty communication, it is allowed for multiple parties on a network to jointly take over a computation which depends on each user, while it is held by other but unknown to the parties [3], [2]. For network nodes, such applications are there for requiring dynamic unique ID [6]. This ID is required in sensor network services for administration activities or for security to the individual nodes [30]. It is not an anonymous network, the participants known and identifiable by each others. In mobile network anonymous communication, methods for assigning and using set of pseudonyms have developed [31], [37]. An algorithm for sharing simple integer data on top of secure sum is build. This is used with the anonymous ID assignment (AIDA) algorithm. It requires a large number and varied iterations. The author prescribing a review on secure sum, specified method of transmitting simple data with power sum, sharing complex data with an AIDA, and how to find an AIDA. Comparison of various AIDA like Slot selection AIDA, Prime modulus AIDA, Sturm‘s Theorem AIDA are discussed. Communications Requirements of AIDA methods are defined. Author concluding that the use of newton identities reduce the communication overhead greatly. So the use of many slots with less number of rounds is needed. The polynomial solution can be avoided by applying sturm‘s theorem. The non cryptographic algorithms are simulated. The requirements are based only on the secure algorithm chosen.

H. Liu et al. reviewed that the existing solutions focus on the illegal access of data not on privacy issues when data sharing to others [57]. Author proposed a Shared Authority based Privacy preserving Authentication protocol (SAPA). This protocol achieved the shared access authority by anonymous access matching mechanisms with privacy and security considerations. An attribute based access control is used to prove that the user can only access own data fields. Proxy re-encryption is applied to prove data sharing among multiple users. A universal composability model [11], is established for multiuser applications. Anonymous ID based data sharing algorithm for the systems under distributed computing and multi party oriented. This gives an integer data sharing algorithm gives a unlimited number of anonymous assignment. Theorems of newton and sturm are used for data mining[49]. Multi owner data sharing scheme is derived for dynamic groups in cloud applications. It assures the user can share the data securely to dynamic user groups through a untrusted cloud server. A granted user is able to decrypt the files. No interaction required for accessing the data from its owner. Revocation of user is achieved by the revocation list. This list is not updating the secret keys of other users. Applied access controls are ensuring that any user in the group can use the resources anonymously. This gives computation overhead are not based on the amount of user [51]. A zero knowledge proof (ZKP) based authentication scheme supports the sharing of personalized contents and network services through TCP/IP network. A trusted third party can handle decentralized instructions [42]. A broadcast group key management scheme (BGKM) developed to improve the weakness of symmetric key cryptosystem in the public cloud models. It ensures that no need for a user depending public key cryptography. One can derive the symmetric keys dynamically at the time of decryption. An attribute based access control method used to attain user who are having the identity attributes can decrypt the contents. This BGKM is a feature of adding revoking users and access control policies [50]. A decentralized framework developed, to track or account the user data usage in the distributed data storage. An object centered approach that provides logging services with the user data and with policies. Jar program ensures that the data access authentication and auditing mechanisms described to strengthen the user data control. The author proposes that a protocol authenticating the data access and authorizing the privacy preserving access authority sharing. ABAC and proxy re-encryption techniques are applied for authentication and authorization. The SAPA model has system initialization with bilinear pairing. Protocols are described for access challenges and responses, data access control, access request matching and data access authority sharing. Security analysis with universal composability model is performed as security model, ideal functionality, real protocol, and security proof for sharing. The author concluding that a newer privacy issue is identified to achieve sharing of privacy preserving access authority. Through the wrapped values transmission data anonymity is achieved. Session identifiers are used for preventing the session correlation. This work is based on a novel security issue. The models defined are combined with a force. Security analysis shows that this work is secure.

J. Zhou et al. proposed a protocol for preserving privacy in cloud assisted e-healthcare storage systems [61]. e-healthcare facilitates monitor, model with latest inventions [24], [5]. Sharing the resource from various locations is accessed through mobile or any other devices, and it is uploaded into the cloud data storage. It is generally stored as person health information (PHI) into the cloud data storage. Providing this data to the untrusted, leads to security and privacy issues. The author found that the existing schemes are focusing the fine grained privacy preserving static model for text access and image analysis. The works proposed provide a secure privacy preserving data mining for dynamic data with image feature extraction scheme. As basis privacy preserving fully homomorphic data aggregation is derived for the proposed privacy preserving data mining model. Then the outsourced disease modelling and earlier intervention achieved by devising an efficient privacy preserving function correlation. A privacy preserving data aggregation supporting multivariate polynomial evaluation without secure communication channel proposed with a respect of aggregator model and participants only model [43]. By the use of paillier‘s cryptosystem [7] an image feature scheme is proposed with privacy preserving scale invariant feature transform (SIFT) [45]. The usage of this cryptosystem directly onto the images deviates the actual process. It is further exploited. It's in efficiency but it is not adaptable to resource concerned devices. It doesn‘t applied to outsourced medical image extraction. Since paillier‘s cryptosystem supports homomorphism of addition. Local extrema extraction through encrypted data comparison with an encrypted data of the same scale doesn‘t prevent chosen plain text attack. So the differences of guassian images and the thresholds are under the same randomness. A simple and provable additive homomorphic stream cipher is proposed to perform efficient aggregation of encrypted data. It is done by replacing the exclusive-OR (XOR) function operations found in stream cipher with modular addition [28]. A concealed data aggregation scheme is proposed based on the property of additive homomorphic encryption based on elliptic curve ElGamal cryptosystem. But it is required to perform the ElGamal encryption on each individual data [7]. An efficient privacy preserving data aggregation scheme in smart grid communications is proposed. It reduces the cost of ElGamal encryption on each data. But it only supports additive homomorphism [61]. Fully Homomorphic Encryption (FHE) [34], [13], [29], [33], [38], [36] provides a solution to secure outsourcing operations in addition and multiplication formats in the encrypted data. Most works are constructed with polynomial-bounded hard problems. The plain text has to be encrypted as bit by bit. So it can not applied to the small devices. It gives computation overhead [34], [29], [38]. A privacy preserving data aggregation model is proposed but it supports only statistical computation. The addition and multiplication aggregation operations are independent. It gives an additional burden for users [48]. A newly developed full homomorphic data aggregation is proposed. It supports addition and multiplication with unified mechanism from n individual data in the encrypted domain, needed to perform any such one way trap door function computation only once. The author describes the network architecture and security model. The proposed work functions are, privacy preserving data aggregation, Privacy Preserving Data Mining 1 (PPDM) for dynamic medical text mining, PPDM2 for medical image feature extraction. Security and performance analysis are performed using various factors. The comparison with [45] shows this work has reduced overheads. Author concludes that the model supports privacy preserving fully homomorphic data aggregation from any such one way trapdoor function. The dynamicity of data is still a questionable. The homomorphic function is not effectively used.

TABLE 1 : COMPARISON OF PRIVACY PRESERVING SCHEMES

Comparison Factor / Paper	Greveler et al.	Nabeel et al.	L.A dunning et al.	H. Liu et al.	J. Zhou et al.	Y. Wang et al.	J.K. Liu et al.
Access Control	Fine grained	Fine grained Course grained	No	Attribute based	Fine grained	Attribubte based	Fine grained
Encryption	XML Encryption	Two layer encryption	No	Proxy re encryption	Homomorphic, one way trap door function	Yes	Yes
Key management	No	Group key	No	Broadcast group	No	yes	Yes
Policy	XACML Policy	Group key management policy	Anonymous ID management	No	No	Threshold based scheme	Two factor authentication
proxy	Encryption Proxy	No	No	Re encryption	No	No	No
Security person	No	No	No	No	No	Sometime	No
Signature	XML signature	No	No	No	No	Yes	Yes
Central authority	Trusted platform module	No	No	No	No	No	No

Y. Wang et al. designed a privacy preserving cloud data storage using array Belief Propagation (BP) - Xor codes [60]. Technique of Belief Propagation decoding process is used with Low Density Pair Check (LDPC) and with Luby Transform (LT) codes [49], [57]. It is used for sharing secrets. Secret sharing schemes are BP-XOR secret sharing scheme, pseudo BP-XOR secret sharing scheme, and Threshold LDPC sharing secret scheme. Threshold LDPC [50] scheme is designed by utilizing array coded design. For reconstruction and distribution of a secret less number of XOR operations are utilized from the BP-XOR/LDPC scheme. In a threshold scheme number of participants can know the secret by grouping them. It is very difficult to handle it. In the secret sharing scheme reconstruction and redistribution is a hard task. Author explain about various number of codes and about the schemes construction. Threshold based secret sharing scheme is defined for privacy protection of cloud data. It uses only XOR operations so the updates and error recovery are easily performed. It overcomes update complexity of Shamir secret sharing scheme. This scheme guaranteed that data file is not required for any checking. Performance is better compared to existing schemes. Because this scheme is based on XOR operation. Author gives importance to the schemes rather than the cloud model. It requires more computation for operations performed with encryption texts and collude attacks are possible. The system has setup, user key generation, and access authentication algorithms. Proof of Knowledge model is designed to support proof check. Security analysis and various threat models are defined.

J.K Liu et al. designed a fine grained two factor authentication access control system for the computing services based on web [61]. Attribute based access control scheme is designed by taking secret key and a device. Both are required to get access, (i.e) the same computer is required for every access. Personal usage system like e-Banking services is an suitable application. The device used must support algorithm functions and tamper proof. This scheme supports a fine grained attribute based access control. Mediated cryptography was designed for the immediate revocation of public keys [4]. A Security Mediator (SEM) model is designed based on this cryptography. But it gives a pressure that this SEM always stay to perform any transactions. Modified version of this model designed as security mediated certificate less cryptography. In this system, user has secret key, public key, identity, and signing algorithm. Secret key and SEM model are also needed. It solves the revocation problems. User is anonymous to this model. So it leads to a security issue. Key insulated cryptography is used to store long term keys in a secured device and short term signatures in unsecured device. All users are needed to update the key for every time and the device is requested to do this task [20]. Bilinear pairing algorithm is used as initial step. (Boneh-Boyen-Shacham) BBS signature scheme used to check the credentials. It requires less amount of requirements. Performance analysis and security analysis are performed. It enables a security system model to provide privacy support for the data. It always requires the device to ensure the privacy. So it is not effective under different cloud services storage mechanism.

III. Discussion

From the comparative study of existing privacy preservation models, most of the researchers proposed various techniques and methods to ensure the privacy of outsourced data. Many access control mechanisms proposed provide privileges to the user for who can access and which part of data to access. It is also provided on the basis of user roles, attribute based, policy based, group based, course grained, and fine grained access control schemes. Cryptography techniques such as encryption are performed to the files. Single standard encryption, multilevel encryption, XML encryption, Attribute based encryption are such mechanisms used to scramble the data. So the owner only extract the knowledge from the data. Group management policies and key management services are used for controlling the based on certain constraints which are required to satisfy at the time of access. Identity based, and anonymous ID based tokens are provided and used for verification at each time access. Revocation of certificates and controls are necessary to obtain security. Such mechanism support only static file contents. It is not supporting data updates and deleting services. In these cases, the entire file is need to re-encrypt and update as whole file replacement. This kind of task gives additional burden. Proxy based access controls given to the users, so the owner not need to present. If the proxy is compromised or meets failure at heavy traffic stage, there is a chance for the failure of entire system. Homomorphic encryption based techniques are not supported for all type of operations on the data. If the data files are used for analytics operations, it is not supported by the homomorphic encryption. Different cryptography techniques and related scheme are defined. But no such security solution provided for ensuring the privacy.

IV. Conclusion

Cloud computing is used by the people for digital data access. All applications and services are deployed on the cloud services. The data storage and retrieval increased day by day. So, the cloud needs to be secured to provide a reliable service delivery. Considering the data part, it is mandatory to ensure the privacy of data at transmits and rest. Cryptographic mechanism, proxy based service models are used for providing these services. To verify the data in rest, it is essential to provide a guarantee to the users. Owner as well as any other person can perform the task with hash functions and signature values. Additionally such models provide error localization and data recovery techniques. This scheme are defined as a way to secure the cloud data storage. In a real time fast changing world requires updated security for the data storage services. It is necessary to ensure the reliability of entire IT services. In future by the outcome of this literature a combined a model of cloud security system is designed to ensure all security services.

Refernces

[1] R. G. Gallager, Low Density Parity Check Codes. Cambridge, MA, USA: MIT Press, 1963.

[2] A. Yao, “Protocols for secure computations,” in Proc. 23rd Ann. IEEE Symp. Foundations of Computer Science, IEEE Computer Society, pp. 160–164, 1982.

[3] 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.

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

[5] 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.

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

[7] P. Paillier, “Public key cryptosystems based on composite degree residuosity classes,” Eurocrypt, pp. 223–238, 1999.

[8] J. Kubiatowicz, D. Bindel, Y. Chen, S. Czerwinski, P. Eaton, D. Geels, R. Gummadi, S. Rhea, H. Weatherspoon, C. Wells, and B. Zhao, “Oceanstore: an architecture for global-scale persistent storage,” SIGOPS Oper. Syst. Rev., vol. 34, pp. 190– 201, November 2000.

[9] U. Maheshwari, R. Vingralek, and W. Shapiro, “How to build a trusted database system on untrusted storage,” in Proceedings of the 4th USENIX Symposium on Operating System Design and Implementation, Berkeley, CA, USA, 2000.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[16] 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.

[17] 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

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

[19] 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.

[20] 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.

[21] 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.

[22] N. Ferguson, “AES-CBC+ Elephant diffuser A Disk Encryption Algorithm for Windows Vista,” Microsoft, 2006. [Online]. Available:http://download.microsoft.com/download/0/2/3/0238acafd3bf-4a6d-b3d6-0a0be4bbb36e/bitlockercipher200608.pdf

[23] 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: Springer-Verlag, pp. 508--524, 2006.

[24] L. Gatzoulis and I. Iakovidis, “Wearable and portable e-health systems,” IEEE Eng. Med. Biol. Mag., vol. 26, no. 5, pp. 51–56, 2007.

[25] 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.

[26] M. Bartel, J. Boyer, B. Fox, B. LaMacchia, and E. Simon, XML Signature Syntax and Processing (Second Edition), D. Eastlake, J. Reagle, D. Solo, F. Hirsch, and T. Roessler, Eds., 2008. [Online]. Available: http://www.w3.org/TR/xmldsig-core/

[27] 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.

[28] C. Castelluccia, A. C.-F. Chan, E. Mykletun, and G. Tsudik, “Efficient and provably secure aggregation of encrypted data in wireless sensor networks,” ACMTrans. Sen. Netw., vol. 5, no. 20, pp. 1–36, 2009.

[29] C. Gentry, “Fully homomorphic encryption using ideal lattices,” in Proc. STOC, pp. 169–178, 2009.

[30] D. Jana, A. Chaudhuri, and B. B. Bhaumik, “Privacy and anonymity protection in computational grid services,” Int. J. Comput. Sci. Applicat., vol. 6, no. 1, pp. 98–107, Jan. 2009.

[31] J. W. Yoon and H. Kim, “A new collision-free pseudonym scheme in mobile ad hoc networks,” in Proc. 7th Int. Conf. Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOPT’09), Piscataway, NJ, IEEE Press, pp. 376–380, 2009.

[32] X. Liang, Z. Cao, H. Lin, and J. Shao, “Attribute Based Proxy Re-Encryption with Delegating Capabilities,” Proc. Fourth Int’l Symp.Information, Computer, and Comm. Security (ASIACCS ’09), pp. 276- 286, 2009.

[33] C. Gentry, S. Halevi, and V. Vaikuntanathan, “i-hop homomorphic encryption and rerandomizable Yao circuits,” in Proc. CRYPTO’10, LNCS 6223, Springer, pp. 155–172, 2010.

[34] M. V. Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, “Fully homomorphic encryption over the integers,” in Proc. EUROCRYPT ‘10, LNCS 6110, Springer, pp. 24–43, 2010.

[35] N. Shang, M. Nabeel, F. Paci, and E. Bertino, “A Privacy-Preserving Approach to Policy-Based Content Dissemination,” Proc. IEEE 26th Int’l Conf. Data Eng. (ICDE ’10), 2010.

[36] N. P. Smart and F. Vercauteren, “Fully homomorphic encryption with relatively small key and cipher text sizes,” in Proc. PKC’10, LNCS 6056, Springer, pp. 420–443, 2010

[37] J.W. Yoon and H. Kim, “A perfect collision-free pseudonym system,” IEEE Commun. Lett., vol. 15, no. 6, pp. 686–688, Jun. 2011.

[38] K. Lauter, M. Naehrig, and V. Vaikuntanathan, “Can homomorphic encryption be practical?,” in Proc. ACM CCSW, 2011.

[39] M.Nabeel, E. Bertino, M. Kantarcioglu, and B.M. Thuraisingham,“Towards Privacy Preserving Access Control in the Cloud,” Proc. Seventh Int’l Conf. Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom ’11), pp. 172-180, 2011.

[40] P. Mell and T. Grance, The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September, 2011

[41] Trusted Computing Group, TPM Main Specification Version 1.2, Revision 116, 2011. [Online]. Available: http://www.trustedcomputinggroup.org/resources/-tpm main specification.

[42] S. Grzonkowski and P.M. Corcoran, “Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking,” IEEE Trans. Consumer Electronics, vol. 57, no. 3, pp. 1424-1432, Aug. 2011.

[43] U. Greveler, B. Justus, D. Loehr, A Privacy Preserving System for Cloud Computing, ICCIT, IEEE, pp- 648 - 653, 2011.

[44] A. Mishra, R. Jain, and A. Durresi, “Cloud Computing: Networking and Communication Challenges,” IEEE Comm. Magazine, vol. 50, no. 9, pp. 24-25, Sept. 2012.

[45] C. Y. Hsu, C. S. Lu, and S. C. Pei, “Image feature extraction in encrypted domain with privacy-preserving SIFT,” IEEE Trans. Image Process., vol. 21, no. 11, pp. 4593–4607, Nov. 2012.

[46] J. Chen, Y. Wang, and X. Wang, “On-Demand Security Architecture for Cloud Computing,” Computer, vol. 45, no. 7, pp. 73-78, 2012.

[47] I.T. Lien, Y.H. Lin, J.R. Shieh, and J.L. Wu, “A Novel Privacy Preserving Location-Based Service Protocol with Secret Circular Shift for K-NN Search,” IEEE Trans. Information Forensics and Security, vol. 8, no. 6, pp. 863-873, June 2013.

[48] J. Taeho, X. Mao, and X. Li, “Privacy-preserving data aggregation without secure channel: Multivariate polynomial evaluation,” in Proc.IEEE INFOCOM, pp. 2634–2642, 2013.

[49] L.A. Dunning, R. Kresman, “Privacy Preserving Data Sharing With Anonymous ID Assignment”, Transaction on Information Forensics and Security, IEEE, Vol. 8, No. 2, pp. 402-413, February, 2013.

[50] M. Nabeel, N. Shang, and E. Bertino, “Privacy Preserving Policy Based Content Sharing in Public Clouds,” IEEE Trans. Knowledge and Data Eng., vol. 25, no. 11, pp. 2602-2614, Nov. 2013.

[51] M. X. Liu, Y. Zhang, B. Wang, and J. Yan, “Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,” IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.

[52] R. Moreno-Vozmediano, R.S. Montero, and I.M. Llorente, “Key Challenges in Cloud Computing to Enable the Future Internet of Services,” IEEE Internet Computing,vol.17,no. 4,pp. 18-25,http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6203493, July/Aug.2013.

[53] Y. Wu, Z. Wei, and R. H. Deng, “Attribute-based access to scalable media in cloud-assisted content sharing networks,” IEEE Trans.Multimedia, vol. 15, no. 4, pp. 778–788, Jun. 2013.

[54] Bertino, " Privacy Preserving Delegated Access Control in Public Clouds", Transactions on knowledge and data engineering, IEEE, Vol. 26, No. 9, pp- 2268 - 2280, September 2014.

[55] M. Nabeel and E. Bertino, “Attribute Based Group Key Management,” to appear in Trans. Data Privacy, 2014.

[56] Y. Chen, Z. L. Jiang, S. M. Yiu, J. K. Liu, M. H. Au, and X. Wang, “Fully secure cipher text-policy attribute based encryption with security mediator,” in Proc. ICICS, pp. 274–289, 2014.

[57] H. Liu, H. Ning, Q. Xiong, L.T. Yang, “Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing,” Transactions on Parallel and Distributed Systems, Vol. 26, No. 1, pp-241-251, January, 2015.

[58] HP. Pooja and N. Nagarathna, Privacy Preserving Issues and their Solutions in Cloud Computing: A Survey, IJCSIT, Vol. 6, No. 2, pp-1588-1592, 2015.

[59] J. Zhou, Z. Cao, X. Dong, X. Lin, “PPDM: A Privacy-Preserving Protocol for Cloud-Assisted e-Healthcare Systems,” Journal of selected topics in signal processing, IEEE, Vol. 9 No.7, pp. 1332-1344, October, 2015.

[60] Y. Wang, "Privacy-Preserving Data Storage in Cloud Using Array BP-XOR Codes," IEEE Transactions on Cloud Computing, Vol. 3, Issue. 4, pp. 425-435, 2015.

[61] J. K. Liu, M. H. Au, X. Huang, R. Lu, J. Li, “Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services,”, Transactions on Information Forensics and Security, Vol. 11, No. 3, pp. 484-497, March, 2016.

[62] J. Zhou, X. Lin, X. Dong, and Z. Cao, “PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing system,” IEEE Trans. Parallel Distrib. Syst., to be published.