# Analysis of Security and Privacy in Public Cloud Environment

Abdul Sattar Raja
Department of Information Systems, College of Computer Science, King Khalid University, Abha, Saudi Arabia
raraja@kku.edu.sa

Dr. Shukor Abd Razak
Faculty of Computing, Universiti Teknologi Malaysia
Skudai, 81300, Malaysia
shukorar@utm.my

*Abstract*— **Computing as a utility, is a long held dream that comes true in the form of evolutional paradigm known as Cloud computing. It provides a gigantic storage with ubiquitous platform access and minimal hardware requirement at user end. Ultimate features and multidisciplinary utilization made its future incontestable, and equally attractive in academia and industry. With the immense growth in the area is proportionally rising the security concern. Cloud user can really relish the maximum advantage of cloud computing if the security and privacy concerns that inherit with storing sensitive and personal identifiable information (PII) in cloud are categorically addressed. To provide flexible user authentication and preserve user privacy digital identity management services are vital. Anonymous authentication, revocation, unlinkability and delegation of authentication for multiple cloud services are obligatory user privacy parameters that require to be addressed through identity management services in cloud. In this paper we analyzed the existing work and emphasized the requirement of user privacy preserving identity management system for public cloud environment.**

***Keywords***— ***Cloud Computing Security, User Privacy, Identity Management, Anonymity, Revocation, Unlinkability, Delegation of Authentication***

## I. Introduction

Cloud computing term became popular in the year 2007 when a collaborative project announced by IBM and Google [1]. It is a composite form of grid computing, parallel computing and distributed computing [2]. Computing as a utility is a long held dream that has ability to transform a large part of industry as a service that comes true in form of cloud computing. It became a popular topic in academia and industry [3]. X as a service is common facility provided by cloud computing where X denotes to every service provided by the cloud [4]. Cloud is based on pay per use business model [5]. With its multi-dimensional advantages cloud has been considered as paradigm shift in IT industry [6].

Through its evolving age several definitions has been quoted [7] [8]; one of the most known and widely used cloud computing definition introduced by National Institute of Standards and Technology (NIST) is “a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. NIST categorize the cloud computing into three service models; Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The deployment models are categorized into; Private Cloud, Public Cloud, Community Cloud and Hybrid Cloud [9]. While there are several others forms of service models which have been proposed in research work like, Identity Management as a Service, Security as a Service, Digital Intellectual Property as a Service DIPaaS etc. [10] [11].

This paper is organized into following order; section II briefly discuss about the cloud computing security issues, section III highlights the traditional techniques proposed in cloud computing authentication, section IV discuss the role of identity management in cloud computing for authentication purpose, section V describe the role of user privacy and its requirements, section VI highlight the existing work proposed to address user privacy through identity management systems, section VII concludes our analysis and directions to the future work.

## II. Cloud Computing Security

Security in cloud computing has been the most discussed as an active research since the domain introduced. Cloud environment has opened a many new security areas which may never be discussed earlier. Availability and reliability are the two research challenges to be addressed for user satisfaction [1, 12]. Jensen et al., [13] described the security issues with respect to internet domain like XML signature and browser security. Kandukuri et al. [14] emphasized that due to uncertain nature of cloud computing vendor should provide a clear and well defined service level agreement to update the user on security issues.

In cloud computing security, some issues are new and some are not but still they are well established challenges; phishing, password weakness, data loss are not new in cloud but require to be resolved as mentioned earlier. Virtual machines issues and fate sharing are new threat areas in cloud computing. Cloud computing security issues introduce some novel elements that require more attention to be resolved. Protecting the activity pattern, accountability of malicious activity, long term business relations and mutual auditability are novel elements of cloud computing threat landscape [15].

Almorsy et al.,[16] analysis are more compact where the possible threats are analyzed in each service model. Virtual

978-1-4673-6618-2/15/$31.00 ©2015 IEEE

machine security, hypervisor security are crucial areas in IaaS. Denial of service, man in the middle, dictionary and replay attacks are critical in PaaS; mutual authentication, authorization and API security are also critical in platform as a service model. SaaS model inherits the security issues from the other two domains as well as the web vulnerabilities are added as this model delivers the products through web services.

There are three major group involved in the cloud security; cloud providers, organization who use the cloud services and the Government or third party regulatory authorities. Sengupta et al.,[17] mapped the security concern with respect to these groups categorized the cloud security into four categories; cloud infrastructure, data, access and compliance. For each category number of research question has been mentioned that specifies a roadmap for the cloud user and provider to satisfy the security requirements. Bahaduria et al., [18] argued that privacy, latency, reliability, portability, interoperability, data breach and data storage are the known barriers to cloud computing. Carroll et al., [19] analyzed cost efficiency has highest advantage and security as a major obstacle of cloud. Cloud lacks evaluative standards which can actually help to the cloud user to compare the service quality. On the other hand service providers are quite reluctant to be evaluated on “appropriate standards or independent auditors” [20].

Data life cycle which starts from the data generation and ends at destruction data includes seven phases. Chen and Zhao [21] discussed the cloud security problem which involved in the seven phases of data life cycle. Rong et al., [22] emphasized in their work to security of SLAs, data sharing and accountability in cloud computing. Due to the distributed nature of cloud environment many international organizations including European network and information security agency (ENISA) issued their reports on cloud computing security issues which include technical, legal, policy and organization issues. Most of the issues are still an open challenge and taken into consideration for designing the new techniques [23].

## III. AUTHENTICATION IN CLOUD

Authentication is a process which identifies the identity of an entity by another entity. In digital life it is software or the part of software which performs authentication process. The most commonly known authentication methods are username and password, multifactor, biometric, and digital device authentications. Authentication in the cloud has been addressed into different ways; the traditional ways and through identity management. In the following we analyzed the two separately and discussed the related work.

### *A. Traditional Proposed Techniques*

Researchers proposed several authentication scheme to achieve secure authentication in cloud computing. Urien et al., [24] proposed a SSL smart card authentication scheme that works in remote authentication dial in user service (RADIUS) protocol environment. Choudhry et al., [25] proposed a two factor smart card based authentication scheme. Hao et al., [26] proposed mutual authentication smart card scheme. Proposed schemes have many flaws with respect to their efficiency and scalability. Proposed scheme does not provide any method for delivery and activation of smart cards. What if the smart cards are stolen? What will be the alternate methods for user to login? Smart card use is device limited; the user must have a special device installed in local machine to use the smart card. Cloud computing is utility computing which provides the service 24*7 anywhere at any time. User can access the services from thick and thin client in heterogeneous networks. The analysis shows that use of digital device, biometric and smart cards schemes are not practical in cloud computing.

Wu et al., [27] an access control scheme in collaborative cloud environment, the scheme use Kerberos authentication in organizational environment and gateways are installed at every organizational domain which are mutually authenticated using public key infrastructure (PKI). Gateway of one organization represent the request to the gateway of second organization to access the services and vice versa, user of one organization are anonymous to the other organizational environment. The proposed scheme is utilization is scalable to community cloud while the use of Kerberos authentication in organizational environment leads to several security flaws. An internal intruder can compromise the security of whole domain by compromising the any single organizational authentication scheme.

Kerberos authentication protocol has been proposed by researchers to use as authentication mechanism in cloud computing [28] [29] [30] [31]. Kerberos is a single sign on authentication protocol that works in extranet environment using single set of credentials [32]. Kerberos consists of authentication server (AS), ticket granting server (TGS) as part of key distribution center (KDC) and Kerberos authentication database [33]. Kerberos works on encrypted data using symmetric key encryption schemes and provides the facility of mutual authentication by adding a shared key between different principles of realm. Kerberos is a widely used protocol however it has vulnerabilities against password-guessing attacks, replay attacks, clock synchronization problem, and key storage problem. An unintentional limitation of Kerberos token size is grow to the point where it reaches to issue of Denial of Service (DoS) [34].

In our point of view, the practical implementation of authentication schemes in cloud environment the approaches can be categorize into two ways; for an enterprise decentralized approach should be adopted to provide authentication and access control based on user assigned roles in organization, and for common user the approach should be centralized to ensure and secure total communication between user and cloud.

### *B. Identity Management*

Digital identity consists of set of data bytes that represents the user. What these bytes contain and how they are verified? Who is the user and what he/she allowed to do? A user identity management system provides the answer of all these questions which contains the set of rules, techniques for providing and verifying the digital identities and their attributes and all other relevant information about the user. Microsoft provides windows live identity, Google applications requires Google identity , Amazon EC2 or S3 demands amazon provided identity, all these examples shows the importance of identity in the use of digital life [35].

Identity management has a superior place in the domain of cloud security issues. Cloud computing is a combination of various traditional technologies to provide the hardware and software service to the user elastically. Hence number of new dimension has entered in cloud paradigm that traditional identity management solutions does not meet [36].

Based on user attributes authenticate the user and provide the access controls are the main responsibilities of identity management services in cloud. Services are required to preserve the user privacy and support interoperability across multiple domains of cloud or in inter-cloud environment [37]. Alpar et al., [38] argued that identity management is a confusing matter because of the several parties are involved i.e. users, service providers, organization and others depends upon scenario of identity management designing. The scope of existing techniques is limited to a single organization or premises of an enterprise which is not true in current cloud or distributed environment scenario. The identity management turns into complex and complete process that deals with the several issues raised in new paradigm. Researchers concluded that existing identity management techniques are "suffering from several shortcomings that need to be addressed before they can be considered truly secure, privacy friendly and usable". In existing identity management approaches privacy and interoperability are unresolved issues and a challenging task especially in public cloud environment.

In our point of view aforementioned issues are actually two folds; first the communication between user and cloud provider and second is the communication between several services of same cloud provider or cloud to cloud environment where several cloud providers are involved. The later one is extension of first one. If an identity management scheme does not maintain the user privacy in terms of interoperability of the various transactions performed by same user in cloud environment then the security breaches involves and user privacy might have been lost.

## IV. User Privacy

Security of user's personal information or password from deciphering, interception, or any other mean of utilization without prior permission is called user privacy. Privacy and security are the paramount concern of information which is basic unit of exchange. In cloud environment service provider are the third party who holds your data on off-premises [39] [40]. Cloud may accidentally or deliberately disclose data or use it for unauthorized purpose, which directly impact on the privacy and confidentially concerns [41] [42].

Privacy of personal information has significant implications in cloud computing [43]. Savola et al., [44] argued that privacy metrics are not clearly defined since the privacy values vary to different people in different situations. Researchers argued that "how can the privacy measured? And what can be used as reference to the measurement?" Researchers conducted interviews from several experts and concluded transparency of privacy and security is important and development of privacy metrics is a challenging task.

Privacy is one of the human fundamental rights. It is related to collection, use, storage and destruction of data which is called personally identifiable information (PII). Arockiam et al., [45] argued that PII has a life cycle which is similar to the data life cycle which contains the seven phases from generation to destruction of information and each phase has its own security breaches to the user privacy. Pearson [46] argued that privacy concern varies according to the type of cloud and context. According to researcher point of view privacy issues are "lack of user control, unauthorized secondary usage, litigation and legal uncertainty" are the key privacy issues.

Cloud computing is a packaged service environment, where several services from the same cloud provider or from the multi cloud providers are provided to the user. Different cloud providers may have terms of service, privacy policies and different ways of authentication. Traditional authentication and authorization application need to be changed to work in cloud environment [22]. Due to distributed nature of cloud environment a proper digital identity management is required to provide anonymity and privacy. In packaged service cloud environment secure and seamless attribute sharing is required. Existing identity management approaches do not cover all aspects of privacy consideration; anonymity, accountability, unlinkability and delegation of authentication [47].

## V. Related Work

To address the user privacy and aforementioned parameters several identity management solutions are proposed. In the following we analyzed the existing approaches and their shortfalls. To provide an anonymous authentication group schemes are commonly used method in decentralized environment, where trusted third party (TTP) is responsible for creating and managing the identities. In such schemes no anonymity has been considered to the TTPs. Trust and risk is the two sides of coins and having no anonymity against TTPs is not only undesirable, it also leads to breaches in user privacy.

Bertino et al., [48] proposed first privacy preserving DIM for cloud computing. The researcher proposed multifactor authentication technique based on look up table, ontology mapping and dictionaries techniques. Proposed protocol uses aggregate zero knowledge proofs of knowledge to prove the users their identity to the cloud provider. They used decentralized environment where no anonymity has been considered to the third party. In their research scenario registrar is supposed to be always available online to provide the identities and their verification which leads to the single point of failure in system. The researchers left the unlinkability and delegation of authentication as open challenges in their future work.

An entity centric approach for privacy and identity management in cloud computing has been proposed by Angin et al., [49]. Research introduces the concept of “IDM Wallet” which contains the user attributes and privacy policies and a virtual machine to implement those privacy policies. In their approach zero knowledge proof algorithms has been used to provide an anonymous identity to the user while the discloser policies are implemented to release the user personal identifiable information. Virtual machines are prone to side channel attacks. There is an apoptosis method proposed for the IDM wallet if the required trust level not maintained but did not mentioned any algorithm or process to implement this technique. Revocation, Unlinability and delegation are not their work scope. Researchers also favored the implementation of identity management system without TTPs.

Sutar et al., [49] proposed a privacy management using homomorphic function in cloud. The study used third party mechanism to achieve user privacy. The researcher aims to propose a mechanism to categorize personal information using Paillier homomorphic encryption algorithm to achieve privacy, reduction of server overhead cost and competency. Researchers proposed to encrypt the data using homomorphic encryption and decrypt at server side using homomorphic decryption. Anonymity has been achieved during the communication only. No anonymity has been considered between the user and server. Unlinkability, revocation and delegation are not the scope of proposed research.

Chow et al., [50] proposed an addition to Bertino et al., [48] work and address addresses the issues of anonymity, traceability, unlinkability and delegation of authentication. Group signature is the base technique for proposed scheme and registrar as a trusted third party to provide authentication certificate to every single user. Proposed architecture does not require user anonymity to the trusted third party. In proposed scheme registrar issues a single credential to user and user used the same credential to randomize and hide the attributes for authentication. Since the same credential are used for generation different certificate, in this case service provider can easily link the various transaction performed by the same user and disclose the user personal identifiable information.

Li et al., [51] proposed a service oriented identity authentication method using fuzzy set as conditions for authentications. In their scheme identity information is partitioned and organized in the form of hierarchal tree structure using fuzzy algorithms. Later using the fuzzy algorithms the authentication information is securely transmitted in cloud. The proposed scheme is support only a cloud environment providing single service. Xiong et al., [52] introduced a Privacy preserving access management scheme named “PRAM”. In the proposed scheme public key method is used to secure the transmission between user and CSP. User privacy has been considered in terms of secure transmission. Anonymity and other privacy parameters are not addressed in the proposed architecture. Khalid et al., [53] proposed an enhanced authentication and authorization protocol for cloud. In their research authorization is dominant than authentication. Researcher enhance the work presented by Zahang et al., [54] for anonymous public key certificates for document exchange. In proposed scheme anonymous identities are allocated to the registered user using the same way. Unlinkability is not the scope of their scheme. We believe that no system can be called anonymous and preserve user privacy until it provider unlinkability of the user transactions.

Nunez and Agudo [11] presented a scheme “BlindIDM” as part of their PhD work and proposed privacy preserving identity management scheme for an environment where a particular organization is obtaining some services from the cloud. In our point of view the scheme is suitable to private cloud and/or community cloud environment. In the proposed scheme host organization manage its registered employees using SAML as base layer and use the proxy re-encryption technique to communicate their identities to the cloud. In this research user privacy is maintained during the communication of host organization and the CSP. The scheme is more likely the trusted third party mode. Kuzhalvaimozhi and Rao [55] proposed a TTP based privacy scheme using group signature schemes. As mentioned earlier that TTPs scheme does not consider any anonymity against third party which is not desirable for user privacy. The proposed scheme is closed user group in private cloud environment. Symmetric scheme has been used for signing the different messages between user and CSP, where CSP can easily link the user transactions and disclose the user personal identifiable information.

## VI. Conclusion and Future work

The research shows that phishing, man in the middle attacks and denial of service attacks are possibilities are always high in third party schemes which causes identity theft and disclosure of personal identifiable information. Delegation of authentication is a challenging task and no direction transformation of anonymous attributes are possible and make the schemes delegatable [2]. We believe that there is strong need for TTP free user privacy preserving identity management algorithm for public cloud environment that satisfies the privacy parameters; anonymity, revocation/accountability, unlinkability and delegation of authentication for packaged public cloud service environment. In our future work we will further analyze the user privacy requirements in public cloud domain and propose an algorithm to address the aforementioned.

## References

[1] M. A Vouk, "Cloud computing–issues, research and implementations," CIT. Journal of Computing and Information Technology, vol. 16, pp. 235-246, 2008.

[2] Y. Zhang and J.-L. Chen, "A delegation solution for universal identity management in SOA," *Services Computing, IEEE Transactions on,* vol. 4, pp. 70-81, 2011.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, *et al.*, "A view of cloud computing," *Communications of the ACM,* vol. 53, pp. 50-58, 2010.

[4] G. Pallis, "Cloud Computing: The New Frontier of Internet Computing," *IEEE Internet Computing,* vol. 14, pp. 70-73, 2010.

[5] X. Xu, "From cloud computing to cloud manufacturing," *Robotics and computer-integrated manufacturing,* vol. 28, pp. 75-86, 2012.

[6] J. Voas and J. Zhang, "Cloud computing: new wine or just a new bottle?," *IT professional,* vol. 11, pp. 15-17, 2009.

[7] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," in *Grid Computing Environments Workshop, 2008. GCE'08*, 2008, pp. 1-10.

[8] G. Reese, Cloud application architectures: building applications and infrastructure in the cloud: " O'Reilly Media, Inc.", 2009.

[9] P. Mell and T. Grance, "The NIST definition of cloud computing," *National Institute of Standards and Technology,* vol. 53, p. 50, 2009.

[10] A. R. Mohammad, K. Mohiuddin, Q. N. Naveed, A. S. Raja, and U. T. M. FSKSM, "Digital Intellectual Property Resources as a Service (DIPaaS) to Cloud Users by Using Service-Oriented Architecture (SOA)," 2012.

[11] D. Nuñez and I. Agudo, "BlindIdM: A privacy-preserving approach for identity management as a service," *International Journal of Information Security,* vol. 13, pp. 199-215, 2014.

[12] F. Sabahi, "Cloud computing security threats and responses," in *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*, 2011, pp. 245-249.

[13] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," in *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on*, 2009, pp. 109-116.

[14] B. R. Kandukuri, V. R. Paturi, and A. Rakshit, "Cloud security issues," in *Services Computing, 2009. SCC'09. IEEE International Conference on*, 2009, pp. 517-520.

[15] Y. Chen, V. Paxson, and R. H. Katz, "What's new about cloud computing security," *University of California, Berkeley Report No. UCB/EECS-2010-5 January,* vol. 20, pp. 2010-5, 2010.

[16] M. Almorsy, J. Grundy, and I. Müller, "An analysis of the cloud computing security problem," in *Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov*, 2010.

[17] S. Sengupta, V. Kaulgud, and V. S. Sharma, "Cloud computing security--trends and research directions," in *Services (SERVICES), 2011 IEEE World Congress on*, 2011, pp. 524-531.

[18] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, "A survey on security issues in cloud computing," *arXiv preprint arXiv:1109.5388,* 2011.

[19] M. Carroll, A. Van Der Merwe, and P. Kotze, "Secure cloud computing: Benefits, risks and controls," in *Information Security South Africa (ISSA), 2011*, 2011, pp. 1-9.

[20] N. Borenstein and J. Blake, "Cloud computing standards: Where's the beef?," *Internet Computing, IEEE,* vol. 15, pp. 74-78, 2011.

[21] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, 2012, pp. 647-651.

[22] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," *Computers & Electrical Engineering,* vol. 39, pp. 47-54, 2013.

[23] C. L. Liu, W. H. Chen, and D. K. Tung, "Identification of critical security issues for cloud computing," *Applied Mechanics and Materials,* vol. 145, pp. 272-276, 2012.

[24] P. Urien, E. Marie, and C. Kiennert, "An innovative solution for cloud computing authentication: Grids of eap-tls smart cards," in *Digital Telecommunications (ICDT), 2010 Fifth International Conference on*, 2010, pp. 22-27.

[25] A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, "A strong user authentication framework for cloud computing," in *Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific*, 2011, pp. 110-115.

[26] Z. Hao, S. Zhong, and N. Yu, "A time-bound ticket-based mutual authentication scheme for cloud computing," *International Journal of Computers, Communications and Control,* vol. 6, pp. 227-235, 2011.

[27] Y. Wu, V. Suhendra, and H. Guo, "A gateway-based access control scheme for collaborative clouds," in *ICIMP 2012, The Seventh International Conference on Internet Monitoring and Protection*, 2012, pp. 54-60.

[28] S. K. Pippal, A. Kumari, and D. S. Kushwaha, "CTES based Secure approach for Authentication and Authorization of Resource and Service in Clouds," in *Computer and Communication Technology (ICCCT), 2011 2nd International Conference on*, 2011, pp. 444-449.

[29] D. Bajpai, M. Vardhan, and D. S. Kushwaha, "Authentication and authorization interface using security service level agreements for accessing cloud services," in *Contemporary Computing*, ed: Springer, 2012, pp. 370-382.

[30] Y. Zhao and N. Thomas, "A Simplified Solution of a PEPA Model of Kerberos Protocol," in *CyberC*, 2011, pp. 257-264.

[31] M. Hojabri and M. Heidari, "Union of RSA algorithm, Digital signature And KERBEROS in cloud security," in *International Conference on Software Technology and Computer Engineering (STACE-2012), ISBN*, pp. 978-93.

[32] V. Radha and D. H. Reddy, "A Survey on Single Sign-On Techniques," *Procedia Technology,* vol. 4, pp. 134-139, 2012.

[33] A. Kumari and D. S. Kushwaha, "Kerberos Style Authentication and Authorization through CTES Model for Distributed Systems," in *Computer Networks and Intelligent Computing*, ed: Springer, 2011, pp. 457-462.

[34] X. You and L. Zhang, "Improved Authentication Model Based on Kerberos Protocol," in *Advances in Multimedia, Software Engineering and Computing Vol. 1*, ed: Springer, 2012, pp. 593-599.

[35] S. Eludiora, O. Abiona, A. Oluwatope, A. Oluwaranti, C. Onime, and L. Kehinde, "A user identity management protocol for cloud computing paradigm," *Int'l J. of Communications, Network and System Sciences,* vol. 4, p. 152, 2011.

[36] A. Gopalakrishnan, "Cloud computing identity management," *SETLabs briefings,* vol. 7, pp. 45-54, 2009.

[37] D. Núñez, I. Agudo, P. Drogkaris, and S. Gritzalis, "Identity management challenges for intercloud applications," in *Secure and Trust Computing, Data Management, and Applications*, ed: Springer, 2011, pp. 198-204.

[38] G. Alpár, J.-H. Hoepman, and J. Siljee, "The identity crisis. security, privacy and usability issues in identity management," *arXiv preprint arXiv:1101.0427,* 2011.

[39] H. Katzan Jr, "On the privacy of cloud computing," *International Journal of Management & Information Systems (IJMIS),* vol. 14, 2011.

[40] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *Communications Surveys & Tutorials, IEEE,* vol. 15, pp. 843-859, 2013.

[41] C. ComPUtING, "Cloud computing privacy concerns on our doorstep," *Communications of the ACM,* vol. 54, 2011.

[42] M. D. Ryan, "Cloud computing security: The scientific challenge, and a survey of solutions," *Journal of Systems and Software,* vol. 86, pp. 2263-2268, 2013.

[43] R. Gellman, "Privacy in the clouds: risks to privacy and confidentiality from cloud computing," in *Proceedings of the World privacy forum*, 2012.

[44] R. M. Savola, A. Juhola, and I. Uusitalo, "Towards wider cloud service applicability by security, privacy and trust measurements," in *Application of Information and Communication Technologies (AICT), 2010 4th International Conference on*, 2010, pp. 1-6.

[45] L. Arockiam, G. Parthasarathy, and S. Monikandan, "PRIVACY IN CLOUD COMPUTING: ASurvey," 2012.

[46] S. Pearson, "Privacy, security and trust in cloud computing," in *Privacy and Security for Cloud Computing*, ed: Springer, 2013, pp. 3-42.

[47] R. Sánchez, F. Almenares, P. Arias, D. Díaz-Sánchez, and A. Marín, "Enhancing privacy and dynamic federation in IdM for consumer cloud computing," *Consumer Electronics, IEEE Transactions on,* vol. 58, pp. 95-103, 2012.

[48] E. Bertino, F. Paci, R. Ferrini, and N. Shang, "Privacy-preserving Digital Identity Management for Cloud Computing," *IEEE Data Eng. Bull.,* vol. 32, pp. 21-27, 2009.

[49] P. Angin, B. Bhargava, R. Ranchal, N. Singh, M. Linderman, L. B. Othmane, *et al.*, "An entity-centric approach for privacy and identity management in cloud computing," in *Reliable Distributed Systems, 2010 29th IEEE Symposium on*, 2010, pp. 177-183.

[50] S. S. Chow, Y.-J. He, L. C. Hui, and S. M. Yiu, "Spice–simple privacy-preserving identity-management for cloud environment," in *Applied Cryptography and Network Security*, 2012, pp. 526-543.

[51] X. Li, J. He, and T. Zhang, "A Service-oriented Identity Authentication Privacy Protection Method in Cloud Computing," *International Journal of Grid & Distributed Computing,* vol. 6, 2013.

[52] J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, and T. Zhang, "PRAM: privacy preserving access management scheme in cloud services," in *Proceedings of the 2013 international workshop on Security in cloud computing*, 2013, pp. 41-46.

[53] U. Khalid, A. Ghafoor, M. Irum, and M. A. Shibli, "Cloud Based Secure and Privacy Enhanced Authentication & Authorization Protocol," *Procedia Computer Science,* vol. 22, pp. 680-688, 2013.

[54] N. Zhang, Q. Shi, and M. Merabti, "Anonymous public-key certificates for anonymous and fair document exchange," *IEE Proceedings-Communications,* vol. 147, pp. 345-350, 2000.

[55] S. Kuzhalvaimozhi and G. R. Rao, "Privacy protection in cloud using identity based group signature," in *Applications of Digital Information and Web Technologies (ICADIWT), 2014 Fifth International Conference on the*, 2014, pp. 75-80.