International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

A Review: Privacy Preservation in Cloud Environment Issues and Challenges

Umar Khalid Farooqui[1], Professor P.K. Bharti [2], Dr. Rajiv Pandey [3], Prof. (Dr) Mohammad Hussain[4]
Research Scholar MUIT, Department of Computer Science & Engineering MUIT ,AIIT Amity UniversityLucknow, Department of Computer Science & Engineering M.G Institute of Management &Technology

Abstract: Cloud computing is the fastest growing service delivery model which offers multi-tenancy on metric basis and the user of cloud need to pay only for which he use ,it also remove the burden of expanding rigid infrastructure with the company growth. The customer of cloud believes in hiring IT resources from providers as per demand and release it as they finish the job, The cloud services sits upon virtualization and its interfaces are open to all.
However for cloud provider it's a challenge for maintaining trust and to provide privacy preservation ,Also the customer end privacy is a prime concern.
This paper made an attempt to review the research work related to privacy preservation in cloud environment and classify major issues and challenges .
Keywords: Privacy preservation, privacy, cloud.

I. INTRODUCTION

"Cloud computing is a fastest growing and proven platform which delivers computing resources as a service "[4] . Cloud computing is provisioning of data, information, file, any other computing resources to the intended user(s) as per their demand over the Internet.
Clouds computing is a recent technology used to represent a different way to architect and remotely manage computing resources; it is sharing resources/information as-a –service using internet. It describes both a platform and type of application[6].
Cloud computing offers a new road map for utilizing as well as delivering of computing resources. The provision is based on the Internet which are dynamically scalable and most of the time these are virtualized resources.
"Cloud is an environment of the hardware and software resources in the data centers that provide diverse services over the network or the Internet to satisfy user's requirements"[4].
Cloud users can utilize the services of cloud in a pay-per-use basis and they save noticeable upfront cost of building their own rigid infrastructure.The name and fame of cloud multiplies day by day however the customer of cloud is always keen to know about the protection of their sensitive data inside of cloud.
Also the sensitive data must be protected from cloud service providers (CSP) without compromising the data.[1]
Due to these reason customer of cloud may lose trust and this will lead in non practicing of cloud[3].Thus privacy preservation is a much concern area in cloud environment.
"The amount of data produces and managed by cloud is highly appreciated day by day with the advent of next generation technologies"[5]. IBM ,Google, Amazon, are some name of repute that provides storage services for cloud. But outsourcing of data may leads to security issues . The cloud service provider is responsible to ensure security to the outsourced data and promise the reliable services to its client. The data storage must assure confidentiality ,integrity and availability. The cloud service that provide storage as a service must ensure that data not modified or accessed or modified by unknown/unauthorized person.

II. PRIVACY AND NEED OF ITS PRESERVATION

Privacy could be stated as the process of hiding confidential and sensitive information related to an individual from rest of the world. Confidential things could be some data or file or any other information pertaining to an individual. In cloud environment mainly privacy of data stored is desirable, the data stored on cloud may be any sort of user identity or controls and violation/leakage of privacy might cause major failure of the system.
Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal them selectively[4].
Privacy has the following elements.

When: a subject may be more concerned about the current or future information being revealed than information from the past.
How: a user may be comfortable if his/her friends can manually request his/her information, but the user may not like alerts to be sent automatically and frequently.
Extent: a user may rather have his/her information reported as an ambiguous region rather than a precise point.

A. Significance of 'Privacy Preservation'

Privacy insures that the data stores on cloud storage accessed only by the intended users and the modification of data could only be performed by the intended user(s) who possess sufficient privileges of doing so.
It is also important to insure that bodies of local administration who are responsible of publishing / posting the user's data , cannot view or modify it[5].
In short after outsourcing no one including cloud service provider can view or modify the data content of user.
Privacy preservation provides means of security to the outsourced data .Privacy preservation generally requires cryptographic techniques.
For better implementation of privacy preservation policies it is important to understand what needs to be protected. Therefore in the next text we explore type of information need to be protected.

B. Classification of Privacy Sensitive Information

People often mean personal information in a distinct manner however in this paper we deal with privacy sensitive information that may include following:

1) *Information Pertaining to Personal Identity :* The information pertaining to an individual and which will be exploited to recognize or locate an individual (like – Person_name,SSN ,Emp ID,Addr_Detail) or any other information which could be used in conjunction to other information for identifying an individual (for example- IP_Address, Card_ number,bank account ID)
2) *Information which could be claimed as Sensitive:* This could be information on caste sect or religion , health , or any other information that needs to be private. These details requires adequate safety measures, some other examples are financial information and appraisal information, biometric information,CCTV information of public places.
3) *Usage Statistics:* Usage statistics presented by computing devices or nodes like; activity information such as viewing interest, recently browsed websites or usage statistics related to a product.
4) *Device Identity:* User devices are also generating information through which devices are uniquely identified such as IP addresses, RFID Tags ,Hardware identities .

III. MAJOR ISSUES AND CHALLENGES WHILE PRESERVING PRIVACY IN CLOUD

Privacy of data is another important concern, while outsourcing data to the cloud service provider. For instance, all the personal information about the customers along with the business logic is outsourced to the cloud service provider. In such case, the data owner worries about the data privacy, as the outsourced data may be misused [2].
In the following text we explore major area of concern while ensuring preservation of privacy in the cloud environment and categories them as client level concern and service provider level concern of cloud. Figure 1.1 shows this.

A. Cloud Client Side Issues and Challenges

Cloud computing offers an interface at client end through which one can access cloud services and to ensure preservation of privacy at this level one need to ensure it at the cloud interface level. The preservation of privacy mainly deals with the ways of securely exploiting cloud services by the end user.
For this partially honest condition few instructive guidelines have been proposed and it is obvious that this is a potential research field of preserving privacy ,also to enhance trust of cloud clients in an unknown cloud environment by empowering them to control process of preserving privacy by their own.
Next we discuss some crucial research areas related to privacy preservation.
"Optimization of efficiency" has been explored [7] mainly in few specific situation[8] .Like "secure computation homomorphic encryption uses the encryption and decryption to the outsourced data for some issues it is important to improve efficiency"[9]whereas [10] uses "bilinear aggregate signature and public key based homomorphic authentication".By the

"improvement of versatility and efficiency these cryptographic solution will be able to offer more and more safety to the sensitive data of cloud".

Another popular method is "noise obfuscation which protect private information". "Ardagna et.al emphasis on preservation of location in mobile environment and come up with a solution based on obfuscation operators " [11]. "YE et.al propose noise injection in search processing for protecting privacy by formulating noise injection as a way of minimizing problem" [12].

"Zhang et.al suggested a historical probability based noise generation strategy for preserving privacy and to improve the efficiency and achieve promising cost cutting in cloud environment" [13].

Briefly speaking noise obfuscation offers a method to preserve privacy at client end by obscuring personal information. Cloud interface level preservation of privacy will make prominent impression in the field of privacy and the triggering factors related to this area are fully dependent on the emergence of clients.

B. Cloud Service Provider Side Issues and Challenges

Preservation of privacy at cloud services end is quiet complex as it offers services which are generally open to all therefore multiple type of privacy risk have to address and analysis of various malicious cloud users unethical cloud services are required.

The cloud services are composite in nature and for cloud service provider it is essential to ensure privacy preservation at each level, here we address preservation of privacy issues at each level of CSP.

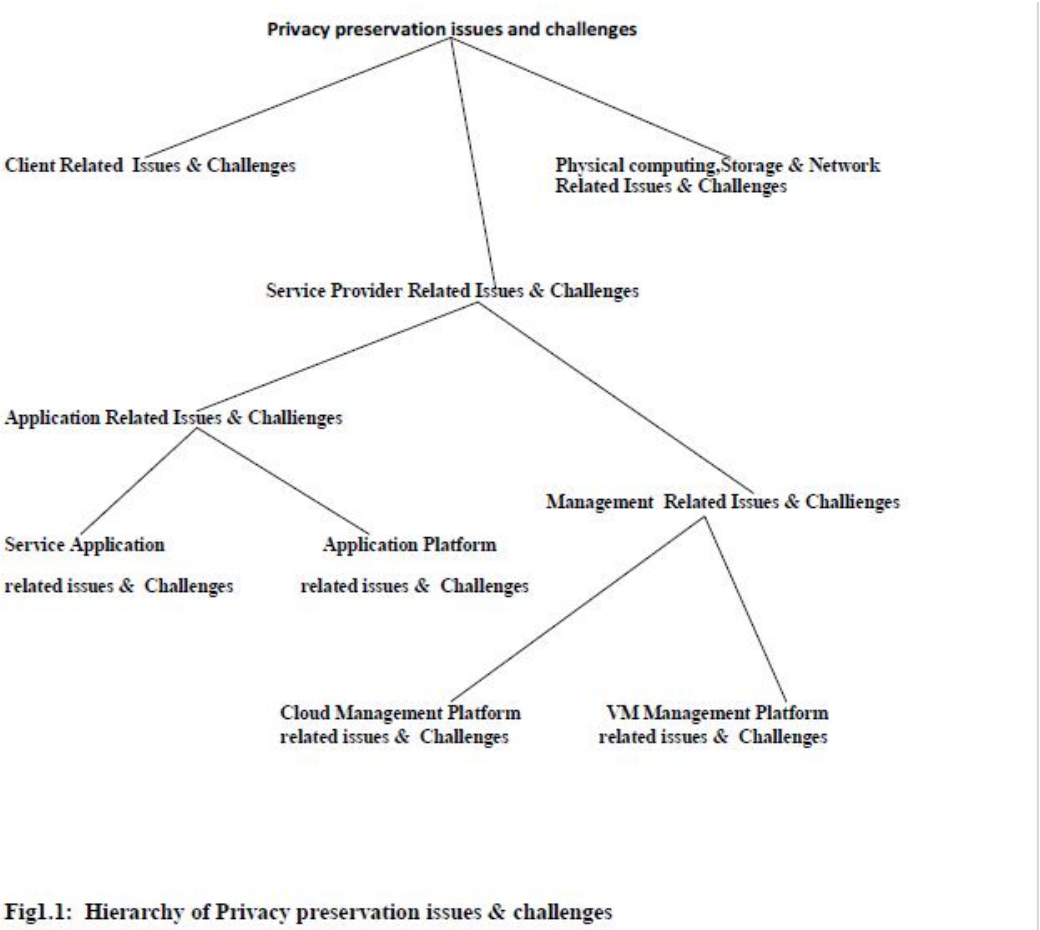

Fig1.1: Hierarchy of Privacy preservation issues & challenges

1) Application Related Issues and Challenges:

a) Cloud Service Application Related Issues and Challenges: The preservation of privacy at this level is of high concern and needed to be Specifically addressed however some existing preservation policies may be applied at this level to achive preservation of privacy up to certain extent.

Here we discuss some existing general work connected to this area –

Smit et al [14] "discover a frame work and methodology for managing privacy into clould". [15] "addresses this as a semi honest condition where the guest problem between the provider & the recipients has ben discussed", also a 'privacy bond' is advocated to utilize for achieving trust.

Also "privacy preserving data mining (PPDM) explores the risk of privacy leakage" [16]. "To protect client privacy evfimievski et al "[17] uses a "randomization operator to investigate and discus the process of association rule mining". Most of them aims on limited sets of data values and a group of data mining methodologies.

Also "liu et al [18] investigate and design an method to apply in real carge data sets".

Gold berg et al [19] apply information theories to dig deeply in PIR".

"In a condition of using multiple server a general method has been used to improve performance of PIR" [20] in cloud.

"Privacy preserving data publishing (PPDP) is a connected field of data publish of web services" [21]

"SuLQ framework [22] considers privacy aware statistical databases by improving the bounds on noise required for privacy".

"Considering a trade off between privacy utility [23], PPDP has been enhanced as it realizes pay per use style of cloud".

Briefly speaking preserving privacy at cloud services and application level is a potential field pertaining to preservation of privacy and the triggering forces for research related to this area solely dependent to the emergence of service applications.

b) *Cloud Application Podium Related Issues and Challenges.:* Some common platforms for cloud applications like hadoop is being used to support cloud services. The major area of concern related to privacy risk at this level is the risks involved by platform itself and the concern is not only about private data or conditions but also taking care of data about data or methods with cloud services processes.

We found that this approach is a potential area for research in the field of privacy preservation of cloud .

"Map reduce" [24], is a popular platform used is a cloud environment and privacy concern in map reduce may involve consideration of solving some privacy risk.

By the use of preservation of privacy word search could be enhanced [25]. "The hybrid approach [26] can make cloud data intensive instances". Other application platforms besides Hadoop are enhancing by fixing system flaws.

Recently beside map reduce, other application platforms also considering preservation of privacy. Therefore it is found a promising research are.

In nut shell preserving privacy at the level of application platform attract more attention in recent days. And the triggering factors of this field solely depends on the emergence of cloud clients & services.

2) Management Related Issues and Challenges:

a) *Cloud Management Platform Related Issues and Challenges:* "To utilize services provided by cloud, some cloud management platform have been proposed and utilized extensively like open stack" . At this stage some basic privacy concerns are required to be taken into account like management of resources, provisioning of interfaces.

Therefore in particular cloud management platform, preserving privacy focuses on the analyses and fixing of privacy volatilities and flaws.

We found it as a new topic in the field of privacy and also a potential research area.

At this level preserving privacy is based on few mature areas like "Amazon Elastic computer cloud [ec2]" "begiel et al" [27] present a type of "image attack focuses on extracting sensitive information while the user is actually unaware". Preserving privacy is a crucial one specially in the field of open source and developing platform for managing cloud.

In nut shell cloud privacy preservation is a immature areas at this level ,also it is a novel and promising research are in the field of cloud computing. The triggering forces pertaining to this research field are fully dependent on to the emergence of service markets of cloud.

b) *Virtual Machine Management Platform Related Issues And Challenges:* The cloud sits on the visualization concepts and mainly operated by virtual machine (UM), UK KUM, Len and Vmware, presently VM management are deploying in mature cloud service providers. It is a primitive level which administering various computing stakes and connect to the upper level i.e. cloud administering platform level. [28] "preservation of privacy in VM basically focuses on to isolate sensitive information on the basis of secure kernal or hardware".

Therefore by enhancing VM themselves one can achieve privacy preservation. Some of the remarkable approaches are listed below [29] " Introduces an approach to investigate and to obtain a strong isolated computing to keep information secure based on specific hardware". "Abstract user model addresses one kind of hypervisor attack. Surface which can threat privacy in cloud" [30]. Preserving privacy at VM administering platform level developed on the basis of current works. Therefore preservation of privacy

at 'Virtual Machine administering platform end' is a promising and developed field and higher standards for preserving privacy are required for this area.
The triggering forces pertaining to this research field fully dependent on to the emergence of services and commercially used eco systems of cloud.

C. Storage and physical computing related issues and challenges

Preserving privacy at storage end and real computing end requires few fundamental means to secure data, here we summaries some important research works.
"Specific privacy problems are major concern of current research work for example Simoens et al" [31] present a "biometric encryption system for preserving privacy in biometric". "A hierarchical identify based Cryptography" [32] realizes "mutual authentication in hybrid cloud.Some
fully developed approaches can enhance privacy" like "old school protocols: SSH, Kerberos, and IKE".
For preserving client privacy at the bottom layer proxies and anonymity network have been extensively used and the objective is maintaining obscureness or unclearness in a suspicious network. "Onion routing and TQR" [33] provide a more sophisticated Scenario, which create difficulties to attackers for tracking customer via analysis of the network traffic.
"Trust [34] has been used to improve anonymous communication especially in cloud environment".
In nut shell Preserving privacy at storage end and real computing end is potential area of preservation of cloud privacy , also the recent researches focuses on advancement of existing approaches like at the virtual machine administering platform level, on this side security & privacy are closely related to each other.
The triggering forces for this domain are fully dependent on the emergence of various services of cloud.

			Challenges	**Issues**	**Known Solutions**
Client Related Issues & Challenges			**How user can use cloud services safely**	**Semi honest condition**	**- Secure Computation protocol.** **- Homomorphic encryption.** **- Bilinear aggregation signature.** **- Public key based homomorphic authentication.** **- use of 'obfuscation operator'** **-noise injection in searching process.** **- probability based noise generation strategy.**
Service Provider Related Issues & Challenges	**Application Related Issues & Challienges**	**Service Application related issues & Challenges**	**Development of complex cloud service applications**	**- malicious cloud users** **- unethical cloud services.**	**- Privacy preserving data mining (PPDM).** **- use of randomize operators.** **- privacy preserving data publishing (PPDP).** **- SuLQ framework.**
		Application Platform related issues & Challenges	**Development of complex services and versatile customers**	**Analyze and withstand privacy risks by platforms.**	**- MapReduce application.** **- Hybrid Approach.**

	Management Related Issues & Challienges	**Cloud Management Platform related issues & Challenges**	**- Analyzing & fixing privacy vulnerabilities and flaws. - Open source & developing cloud management platform.**	**Resource management and Interface provisioning.**	**- Still at early stage**
		VM Management Platform related issues & Challenges	**- To secure VM as it is basic level which manage resources. - openness. - Higher privacy preservation standards required.**	**- how to virtualized or isolate sensitive information. - secure kernel or hardware.**	**- Strong isolated computing to keep information secure based on specific hardware. - Strict user model.**
Physical computing,Storage & Network Related Issues & Challenges			**Use of some basic mechanism to ensure privacy preservation.**	**At this level security and privacy are linked together.**	**- Biometric encryption system - Hierarchical identity based cryptography. - old school protocols: SSH,Kerberos and IKE. - onion routing &TOR**

Table 1.1: Assessment of privacy preservation issues and challenges in cloud environment

IV. CONCLUSIONS AND FUTURE WORK

Different kind of privacy attacks or threats has been experience by the development and expansion of cloud computing model, to address their severe issues like malicious nodes or clients and kinds of vulnerabilities various preserving techniques have been presented so far in the context of privacy. However legacy privacy threats and attacker can co exist in cloud and new advancement in cloud generally introduces new privacy threats and challenges.

Therefore we can say that preserving privacy is a complex area which attracts researches also preserving privacy in cloud environment is big task and requires in-depth & multidimensional investigations obviously it is impractical to comprise all the dimensions of investigation into a single paper.

However we succeeded to analyze open research problems pertaining to preservation of privacy and transparently categorize the major areas of concern for preserving privacy, also we successfully present assessment of privacy preservation issues and challenges in cloud environment (see table 1.1).

We also realize that existing privacy preservation schemes are insufficient to deal with emerging security & privacy challenges and the subject requires further investigation and future work to address all the security & privacy issues.

REFERENCES

[1] Jayashree Agarkhed; Ashalatha R , “A privacy preservation scheme in cloud environment”Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio Informatics(AEEICB),2017.

[2] Arjun, U., and S. Vinay. "A short review on data security and privacy issues in cloud computing." Current Trends in Advanced Computing (ICCTAC), IEEE International Conference on . IEEE, 2016.

[3] Mark D. Ryan, "Cloud Computing Privacy Concerns on Our Doorstep," *Communications of the ACM* 54(1): 36-38, 2011.

[4] Sun, Yunchuan, et al. "Data security and privacy in cloud computing." International Journal of Distributed Sensor Networks (2014).

[5] M.Thangavel,S.Sridhar, “An Analysis of privacy preservation schemes in cloud computing”,2nd IEEE International Conferenceon Engineering & Technology ,March 2016.

[6] Umar Khalid Farooqui,Ashish. K.Trevedi et al , “Architecting Distributed Domain Reducer in Cloud Environment”.IJCA 40(12):24-29,2012.

[7] Florian Kerschbaum, "Automatically Optimizing Secure Computation," 18th ACM Conference on Computer and Communications Security (CCS' 11), pp. 703-714, Chicago, Illinois, USA, October 17-21, 2011.

[8] Lior Malka, "VMCrypt: Modular Software Architecture for Scalable Secure Computation," 18th ACM Conference on Computer and Communications Security (CCS' 11), pp. 715- 724, Chicago, Illinois, USA, October 17-21, 2011.

[9] Michael Naehrig, Kristin Lauter, and Vinod Vaikuntanathan,"Can Homomorphic Encryption Be Practical?," 3rd ACM Workshop on Cloud Computing Security Workshop (CCSW'2011), pp. 113-124, Chicago, Illinois, USA, October 17-21, 2011.

[10] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li,"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems*, 22(5): 847-859, 2011.

[11] Claudio A. Ardagna, Marco Cremonini, Sabrina De Capitani di Vimercati, and Pierangela Samarati, "An Obfuscation-Based Approach for Protecting Location Privacy," *IEEE Transactionson Dependable and Secure Computing*, 8(1): 13-27, 2011.

[12] Shaozhi Ye, Felix Wu, Raju Pandey, and Hao Chen, "Noise Injection for Search Privacy Protection," 2009 International Conference on Computational Science and Engineering (CSE'09), pp. 1-8, Vancouver, Canada, August 29-31, 2009.

[13] Gaofeng Zhang, Yun Yang, and Jinjun Chen, "A Histrotical Probability based Noise Generation Strategy for Privacy Protection in Cloud Computing," *Journal of Computer and System Sciences*, 78(5): 1374-1381, 2012.

[14] Michael Smit, Kelly Lyons, Michael McAllister, and Jacob Slonim, "Detecting Privacy Infractions in Applications: A Framework and Methodology," IEEE 6th International Conference on Mobile Adhoc and Sensor Systems (MASS '09),pp. 694-701, Macau, China, October 12-15, 2009.

[15] Philippe Golle, Frank McSherry, and Ilya Mironov, "Data Collection with Self-Enforcing Privacy," *ACM Transactions on Information and System Security*, 12(2): 1-24, 2008.

[16] Rakesh Agrawal and Ramakrishnan Srikant, "Privacy-Preserving Data Mining," *ACM SIGMOD Record*, 29(2): 439-450, 2000.

[17] Alexandre Evfimievski, Johannes Gehrke, and Ramakrishnan Srikant, "Limiting Privacy Breaches in Privacy Preserving Data Mining," 22nd ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS 2003), pp. 211-222, San Diego, California, USA, June 09 - 11 2003.

[18] Li Liu, Murat Kantarcioglu, and Bhavani Thuraisingham, "The Applicability of The Perturbation Based Privacy Preserving Data Mining for Real-World Data," *Data and Knowledge Engineering*,65(1): 5-21, 2008.

[19] Ian Goldberg, "Improving the Robustness of Private Information Retrieval," 2007 IEEE Symposium on Security and Privacy (SP'07), pp. 131-148, Oakland, California, USA, May 20-23, 2007.

[20] Ryan Henry, Femi Olumofin, and Ian Goldberg, "Practical PIR for Electronic Commerce," 18th ACM Conference on Computer and Communications Security (CCS'11), pp. 677-690, Chicago,Illinois, USA, October 17-21, 2011.

[21] Benjamin C. M. Fung, Ke Wang, Rui Chen, and Philip S. Yu,"Privacy-Preserving Data Publishing: A Survey of Recent Developments," *ACM Computing Surveys*, 42(4): 1-53, 2010.

[22] Avrim Blum, Cynthia Dwork, Frank McSherry, and Kobbi Nissim, "Practical Privacy: The SuLQ Framework," 24th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS 2005), pp. 128-138, Baltimore, Maryland, USA, June 13-16, 2005.

[23] Vibhor Rastogi, Dan Suciu, and Sungho Hong, "The Boundary Between Privacy and UItility in Data Publishing," Proceedings of the 33rd International Conference on Very Large Data Bases (VLDB 2007), pp. 531-542, Vienna, Austria, September 23-27,2007.

[24] Jeffrey Dean and Sanjay Ghemawat, "MapReduce: Simplified Data Processing on Large Clusters," 6th conference on Symposium on Opearting Systems Design & Implementation (OSDI' 04), pp. 137-150, San Francisco, California, USA,December 6-8, 2004.

[25] Erik-Oliver Blass, Roberto Di Pietro, Refik Molva, and Melek Onen, "PRISM -- Privacy-Preserving Search in MapReduce,"*Cryptology ePrint Archive, Report 2011/244, Available at :http://eprint.iacr.org/2011/244.pdf*, 2011.

[26] Kehuan Zhang, Xiaoyong Zhou, Yangyi Chen, XiaoFeng Wang,and Yaoping Ruan, "Sedic: Privacy-Aware Data Intensive Computing on Hybrid Clouds," 18th ACM Conference on Computer and Communications Security (CCS' 11), pp. 515-526, Chicago, Illinois, USA, October 17-21 2011.

[27] Sven Bugiel, Stefan Nürnberger, Thomas Pöppelmann, Ahmad-Reza Sadeghi, and Thomas Schneider, "AmazonIA: When Elasticity Snaps Back," 18th ACM Conference on Computer and Communications Security (CCS'11), pp. 389-400,Chicago,Illinois, USA, October 17-21, 2011.

[28] Chunxiao Li, Anand Raghunathan, and Niraj K. Jha, "A Trusted Virtual Machine in an Untrusted Management Environment,"*IEEE Transactions on Services Computing, Published online:http://doi.ieeecomputersociety.org/10.1109/TSC.2011.30*, 2011.

[29] Ahmed M. Azab, Peng Ning, and Xiaolan Zhang, "SICE: AHardware-Level Strongly Isolated Computing Environment for x86 Multi-core Platforms," 18th ACM Conference on Computer and Communications Security (CCS' 11), pp. 375-388, Chicago,Illinois, USA, October 17-21, 2011.

[30] Jakub Szefer, Eric Keller, Ruby B. Lee, and Jennifer Rexford,"Eliminating the Hypervisor Attack Surface for a More Secure Cloud," 18th ACM Conference on Computer and Communications Security (CCS' 11), pp. 401-412, Chicago,Illinois, USA, October 17-21, 2011.

[31] Koen Simoens, Pim Tuyls, and Bart Preneel, "Privacy Weaknesses in Biometric Sketches," 30th IEEE Symposium on Security and Privacy (SP' 09), pp. 188-203, Oakland, California,USA, May 17-20, 2009.

[32] Liang Yan, Chunming Rong, and Gansen Zhao, "Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography," 1st International Conference on Cloud Computing (CloudCom' 09), pp. 167-177, Beijing, China, December 1-4, 2009.

[33] Dingledine Rogerm, Nick Mathewson, and Paul Syverson, "Tor:The Second-Generation Onion Router," 13th USENIX Security Symposium, pp. 303-320, San Diego, California, USA, August 9-13, 2004.

[34] Aaron M. Johnson, Paul Syverson, Roger Dingledine, and Nick Mathewson, "Trust-based Anonymous Communication:Adversary Models and Routing Algorithms," 18th ACMConference on Computer and Communications Security(CCS'11), pp. 175-186, Chicago, Illinois, USA, October 17-21,2011.