2012 Second International Conference on Cloud and Green Computing

Key Research Issues for Privacy Protection and Preservation in Cloud Computing

Gaofeng Zhang, Yun Yang
Faculty of Information and Communication Technologies
Swinburne University of Technology
Hawthorn, Melbourne, Australia 3122
{gzhang,yyang}@swin.edu.au

Xuyun Zhang, Chang Liu, Jinjun Chen
Faculty of Engineering and Information Technology
University of Technology, Sydney
Broadway, NSW, Australia 2007
{xyzhanggz,changliu.it}@gmail.com
Jinjun.Chen@uts.edu.au

***Abstract*--Cloud computing promises an open and promising environment where customers or users can utilise and deploy IT services in a pay-as-you-go style while saving huge capital investments on their own IT infrastructure. The openness and virtualisation features in cloud environments make privacy protection and preservation be a challenging issue. Currently, in existing privacy protection and preservation fields, many approaches and methods have been investigated and presented to withstand different kinds of attackers and risks. On the basis of this, many researchers start to consider these in cloud environments. But current work is still at the early stage. Therefore, a systematic investigation and an overall classification of key issues in cloud privacy protection and preservation are necessary to keep current research on the right track while reducing unnecessary work as much as possible. Hence, in this paper, we investigate and classify various privacy issues in cloud environments. Especially, we focus on some key areas of cloud privacy protection and preservation from the perspective of cloud roles and cloud service levels. This paper can help to provide an overall picture of cloud privacy protection and preservation and point out potential key areas in cloud privacy protection and preservation.**

***Keywords*--cloud computing, privacy protection and preservation**

I. INTRODUTION

Cloud computing is positioning itself as a new promising platform for delivering information infrastructures and resources as IT services [1, 2]. Cloud users can deploy or utilise these services in a pay-as-you-go style while saving a huge capital cost on building their own hardware and software [3]. However, customers always instinctively concern about whether their private sensitive information can be protected or not, when facilitating their IT services in cloud environments since they do not have much control inside cloud [4]. Without it, customers may eventually lose the confidence in and desire to take cloud computing into practice [5]. Therefore, privacy protection and preservation are as crucial as one of the most concerned research areas in cloud computing.

Currently, in traditional privacy protection and preservation areas, different kinds of ways and measures for stealing and jeopardising privacy have been analysed; many strategies and mechanisms have been discussed and designed to deal with them. Especially in distributed systems, "unethical" or malicious members have analysed: how to obtain unauthorised priority or sensitive information in whole processes of data operations or service executions? Much privacy protection and preservation research work has been presented to deal with these malicious attackers, and many approaches protect privacy safe already, such as cryptograph, identity management, privacy enhanced protocol, and so on.

As a novel and promising computing architecture, cloud computing requires privacy protection and preservation to investigate and deal with all actual and potential privacy attacks which are brought by cloud computing, or existing privacy attacks depraved by cloud computing [6]. In general, cloud computing is a customer-oriented computing environment which can provide various kinds of cloud services to facilitate cloud customers. Hence, to support this, we discuss cloud privacy protection and preservation by different kinds of cloud service levels in cloud environments on the basis of existing privacy approaches, so privacy protection and preservation can be embedded into cloud service levels and facilitate cloud customers.

Generally speaking, in cloud environments, the architecture provides several levels of cloud services from the perspective of virtualisation. As shown in Figure 1, cloud architecture focuses on how to provide cloud services for the goal of the pay-as-you-go style in terms of its market model. At different levels, different cloud services can be managed by service providers and utilised by cloud customers directly or indirectly. Therefore, privacy protection and preservation in cloud environments can be considered at these different levels and organise various privacy protection and preservation approaches to match this structure.

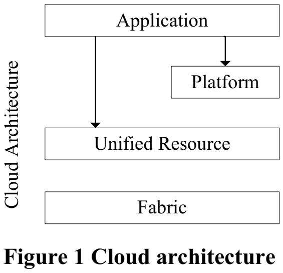

Figure 1 Cloud architecture

In the view of cloud customers, cloud services are so simple to be utilised thanks to the virtualisation feature. In Figure 2, from the perspective of cloud customers, when cloud customers start to use or run a cloud service, cloud service levels have to take part in and corresponding privacy protection and preservation approaches play an important role

978-0-7695-4864-7/12 $26.00 © 2012 IEEE
DOI 10.1109/CGC.2012.47

in the whole processes. Besides, in existing privacy protection and preservation areas, different kinds of approaches have been investigated to keep privacy secured for privacy risks at different cloud service levels. Hence, it is a suitable view to classify privacy protection and preservation approaches in cloud environments by cloud service levels in the view of cloud customers. In the following parts of this paper, cloud service levels mean cloud service levels in the view of cloud customers in Figure 2.

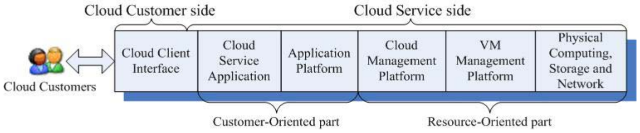

Figure 2 Cloud service levels in the view of cloud customers

Besides, as the two main roles in cloud environments, cloud customers and cloud services providers have to investigate privacy protection and preservation in cloud service processes among them and themselves. So, cloud customer sides and cloud service sides are key views to discuss privacy protection and preservation in cloud environments. As a kind of complex commercial bio-environments, some unclear or malicious service providers may exist in cloud environments. So, it is necessary to take certain actions at cloud customer sides to protect customer privacy. This is the privacy protection and preservation at the first level of cloud service levels, or at cloud customer sides. Privacy protection and preservation at other levels of cloud service levels also require other approaches and mechanisms applied at cloud service sides. They focus on how to build a more privacy-safe cloud service and withstand malicious customers or other services, in a position of cloud service providers [7]. In other words, they are privacy protection and preservation at cloud service sides. Therefore, privacy protection and preservation can be considered at different cloud levels and roles to obtain a comprehensive privacy protected situation.

Privacy adversaries in cloud who steal privacy and break privacy protection and preservation, could be customers or users of cloud services, and 'malicious' service providers in these opaque environments. That is why cloud privacy protection and preservation have to consider these risk sources and take actions at both customer and service sides. In other words, cloud architecture is not the only reason to classify cloud privacy protection and preservation into cloud customer sides and cloud service sides, these various privacy leakage risks are also a reason. We will discuss these types of privacy protection and preservation in the next section.

A lot of existing privacy protection and preservation approaches can be utilised directly in cloud environments [8]. That is because privacy is a long-standing topic in distributed computing and some areas are universal. Besides, cloud computing builds on existing distributed computing and virtualisation, and there are a lot of things in common. At these cloud service levels, different existing privacy protection and preservation approaches and mechanisms can be classified into these levels and play an important role in enhancing cloud privacy.

On the other hand, cloud computing requires privacy protection and preservation to consider this novel situation and protect customer privacy. For example, the pay-as-you-go style and the virtualisation feature make cloud service levels more obvious than ever before. So, specific privacy requirements in cloud can be divided into different service levels and guide privacy protection and preservation independently, which is totally different in existing computing situations. Existing privacy protection and preservation methods have to adjust them into cloud environments or be replaced by novel approaches and methods [5, 9].

The remainder of the paper is organised as follows. In Section II, we present the key research issues of cloud privacy protection and preservation approaches. Then, in Section III, we present further discussions on cloud privacy protection and preservation. Finally in Section IV, we discuss our conclusions and point out future work.

II. KEY RESEARCH ISSUES

In this section, we discuss current cloud privacy protection and preservation, and classify them by cloud service levels in the view of cloud customers as introduced in Section I. In general, we classify those issues into customer side and service side. Figure 3 shows this.

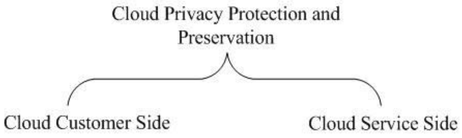

Figure 3 Cloud privacy protection and preservation at cloud customer side and cloud service side

A. Privacy protection and preservation at cloud customer side

In this section—privacy protection and preservation at cloud customer side, there is one cloud service level—cloud client interface level. So, privacy protection and preservation at cloud customer sides means privacy protection and preservation at cloud client interface level. So, we can focus on privacy protection and preservation at this level.

Just like introduced before, at cloud customer sides, privacy protection and preservation consider how to use cloud services safely depends on clients own. So, on the basis of this semi-honest condition, some instructive approaches and ideas have been discussed. And we believe this kind of approaches is a promising research area in cloud privacy protection and preservation to give cloud customers confidence by controlling privacy protection processes on their own. In the following parts, we introduce some typical research areas.

Secure computation starts to combine a bunch of nodes mistrusted each other to complete a task together by cryptography [10]. Optimisation on the efficiency has been discussed [11], especially in some specific situations [12]. From the perspective of cloud privacy protection and preservation, it could be a promising approach with a significant efficiency improvement in future. So, at cloud clients interface level, private data or information can be protected in cloud service processes under secure computation protocols. For existing secure multi-party computations, cloud client interface level is a major applied area in cloud environments for controlling computing processes by cloud customers, and other cloud service levels also could utilise this idea for reference.

Similar to secure computation, homomorphic encryption extends the usage of encryption and decryption in the view of outsourcing in cloud. And some issues in this area try to improve it to take it into practice, such as efficiency [13]. Besides, [14] uses bilinear aggregate signature and public key based homomorphic authenticator to improve practicality. In general, with the improvement on efficiency and versatility, these cryptography approaches will be able to grant more safety to private data in cloud environments.

Noise obfuscation is another widely adopted method for protecting private information. For example, Ardagna et al. [15] focus on the location privacy protection in a mobile environment, and present a solution based on different obfuscation operators. Ye et al. [16] describe noise injection in searching processes for privacy protection, by formulating noise injection problem as a mutual information minimisation problem. Zhang et al. [17] present a historical probability based noise generation strategy for privacy protection to improve the efficiency of current noise privacy protection and obtain a promising cost-saving in cloud environments. In short, noise obfuscation presents another approach to protect privacy at customer sides: obfuscate private information, not to cover it directly.

In brief, privacy protection and preservation at cloud client interface level will get more attentions than ever before in cloud environments. And the driving force of this research area depends on the development of cloud customers.

B. Privacy protection and preservation at cloud service side

Just like introduced before, at cloud service sides, privacy protection and preservation have to consider these adversaries at cloud customer sides or cloud service sides. So, the situation of privacy protection at cloud service sides is quite complex. Various types of privacy risks have to be analysed and addressed, such as from malicious cloud users, or other unethical cloud services. And enhancing privacy protection processes in cloud services can avoid some potential privacy risks. In general, for cloud service providers, cloud service levels can be utilised to organise privacy protection and preservation in this part. So, we introduce privacy protection and preservation in this part level by level.

1) *Privacy protection and preservation at cloud service application level*

Privacy protection and preservation at this level has been discussed as an important concerned area in cloud privacy protection and preservation. And on existing privacy protection and preservation, many approaches can be applied in cloud environments directly. So we discuss some existing typical privacy protection and preservation to protect privacy at this level.

Let us start with some general work in this area. Smit et al. [18] describe a whole framework and methodology for managing privacy policy in a computing environment. In a typical semi-honest condition [19], the trust problem between pollsters and respondents has been discussed, and a 'privacy-bond' can be utilised to keep mutual trustworthy, just like in cloud. These approaches can jump out of the limitation of specific computing environments, and most of them can be utilised in cloud directly or specialised in cloud. On the basis of these general papers, specific methods focused on technical situations are introduced in the following parts.

Privacy-Preserving Data Mining (PPDM) reveals a view of privacy leakage in the minutiae [20]. To protect customer privacy, Evfimievski et al. [21] use a randomisation operator to investigate and discuss the process of association rule mining. Many privacy preserving methods focus on a typical small datasets and a particular family of data mining algorithms, and Liu et al. [22] inspect and design some approaches to apply it in the real large datasets.

Privacy Information Retrieval (PIR) mainly prevents database operators from knowing users' interested records. Beimel et al. [23] and Goldberg et al. [24] apply information theories to dig deeply in PIR. In multiple-servers conditions, a general method has been presented to improve practical performance of PIR [25], just like in cloud.

Privacy-Preserving Data Publishing (PPDP) has a wide utilised field in data publish of service Web [26]. In general, a SuLQ framework [27] considers privacy-aware statistical databases by improving the bounds on noise required for privacy. In the case considering a trade-off between privacy and utility [28], PPDP has been enhanced to be practical, which matches the pay-as-you-go style of cloud.

In brief, privacy protection and preservation at cloud service application level is a relatively mature area in cloud privacy protection and preservation. And the research driving force of this area depends on the development of cloud service applications.

2) *Privacy protection and preservation at application platform level*

Generally speaking, common application platforms can be utilised at this level to support cloud services, like Hadoop. To deal with privacy concerns from cloud customers, a major idea of privacy protection and preservation is to analyse and withstand privacy risks by platforms' improvements at this level. So, at this service level, privacy protection and preservation may not consider specific private data or conditions, but analyses metadata or procedures with privacy feature in cloud service processes. To some extent, we believe that this kind of approaches is one of the most promising research areas in cloud privacy protection and preservation. As far as we concerned, the cloud application platform level is viewed as a key part of cloud environments for bringing many novel technologies in cloud environments.

MapReduce [29] is a popular programming platform in cloud environments. And privacy protection and preservation in MapReduce have been considered to solve some privacy risks: Word search could be enhanced by privacy-preserving in cloud computing [30]. The hybrid approach [31] can make cloud data-intensive instances be more practical. Besides, other cloud application platforms, like some ones in Hadoop, can be enhanced by privacy protection and preservation in terms of fixing system flaws. Currently, besides MapReduce, other application platforms have started considering from the perspective of privacy protection and preservation. So, it is promising for related research work at this level.

In brief, privacy protection and preservation at application platform level can get more attentions than ever before in cloud environments. And the driving force of this research area depends on the development of both cloud customers and services.

3) Privacy protection and preservation at cloud management platform level

In general, to operate cloud and provide cloud service, some cloud management platforms have been proposed and utilised step by step, such as Openstack [32]. At this level, compared to privacy protections and preservations introduced above, some basic privacy issues need to be considered, like in resource management and interface providing. So, in specific cloud management platforms, privacy protection and preservation focus on analysing and fixing privacy vulnerabilities and flaws. As a novel area of cloud, we believe privacy protection and preservation at this level is still a new topic and a promising research area in cloud privacy protection and preservation, and we summarise some valuable approaches at this level in this part.

Currently, at this level, privacy protection and preservation have started in some mature cloud environments. On the basis of Amazon Elastic Compute Cloud (EC2), Bugiel et al. [33] present one type of image attack which focuses on extracting sensitive information caused by unaware users. It is predictable that in other open-source and developing cloud management platforms, privacy protection and preservation can be crucial topics. In general, privacy protection and preservation at this level are still at an early stage and will attract much more attentions as key issues in cloud privacy protection and preservation.

In brief, privacy protection and preservation at the cloud management platform level can be a novel and promising area in cloud environments. And the driving force of this research area depends on the development of cloud services and markets.

4) Privacy protection and preservation at VM management platform level

In cloud environments, virtualisation is a key feature mainly operated by Virtual Machine (VM), such as KVM, Xen and VMWare. Currently, VM managements have been deployed in mature cloud service providers and developing cloud environments, regardless public cloud, community cloud, private cloud or hybrid cloud. At cloud service levels, VM management platform level is a basic level which manages basic system resources and provides interfaces to the upper level—the cloud management platform level. From existing privacy protection and preservation approaches [34], privacy protection and preservation in VM mainly focus on how to virtualise or isolate sensitive information on the basis of secure kernels or hardware. So, at this level, privacy protection and preservation have to consider 'enhancing' virtual machines themselves on the basis of existing approaches and novel cloud environments. We summarise some valuable approaches at this level in this part.

In [35], one kind of approaches has been investigated to obtain a strong isolated computing to keep information secure based on specific hardware. Besides, one kind of hypervisor attack surface can threat privacy in cloud, and a strict user model is necessary to address it [36]. Briefly, privacy protection and preservation at VM management platform level build on existing work, and underline system complexity with the openness feature of cloud.

So, privacy protection and preservation at VM management platform level is a relatively mature area in cloud privacy protection and preservation. And cloud environments require higher privacy protection and preservation standards in this area. Besides, at this level, it is hard to distinguish these concept 'security' and 'privacy' for its fundamental. It means that much security work can be utilised to enhance privacy at this level. The driving force of this research area depends on the development of cloud services and commercial eco-systems.

5) Privacy protection and preservation at physical computing, storage and network level

At this level, privacy protection and preservation consider some basic mechanisms to secure privacy-sensitive data. Just like introduced before, these privacy protection and preservation approaches are important roles to keep privacy safe under VMs. Hence, on the basis of existing mature research work, we summarise some valuable approaches at this level to support the entire cloud privacy protection and preservation.

In general, specific privacy problems are major parts of current research work. For instance, Simoens et al. [37] present a biometric encryption system for privacy protection in the biometric search area. A hierarchical identity-based cryptography [38] can realise mutual authentication in hybrid cloud. Besides, fully developed approaches can enhance privacy protection from the perspective of data and communication in cloud environments, such as old-school protocols: SSH, Kerberos, and IKE.

Proxies and anonymity networks have been widely discussed to protect customer privacy at the bottom level. The major goal is to keep anonymity or invisibility in a complex or dangerous network. Onion routing and its successor TOR [39] provide a more sophisticated privacy protection scenario, making it difficult for attackers to trace customers via network traffic analysis. Trust [8] has been considered to improve anonymous communication, especially in cloud.

In brief, privacy protection and preservation in physical computing, storage and network level are relatively mature areas in cloud privacy protection and preservation, and current researchers focus on improving existing approaches for cloud environments. Just like at the VM management platform level, at this level these concept 'security' and 'privacy' have been closely linked together, too. And the research driving force of this area depends on the development of cloud services.

III. FURTHER DISCUSSION

With the development of cloud computing, privacy protection and preservation are analysing different kinds of privacy attackers or flaws, even some potential ones in cloud. To withstand these 'malicious' nodes or vulnerabilities, a lot of privacy protection and preservation approaches have been presented. Traditional privacy risks and attackers can exist in cloud environments, and new features of cloud can bring some new privacy risks or deteriorate some existing privacy risks. So, privacy protection and preservation are crucial research areas in cloud computing, and that is one important background of what we discussed in this paper.

Just like discussed before, cloud privacy protection and preservation are the combination of many privacy risks and protections in cloud environments. And it is hard to collect all privacy attacking or stealing behaviours in one paper for the variability. Due to the comprehensive privacy protection and preservation classification, although some specific privacy protection and preservation methods in cloud environments may not be discussed thoroughly in this paper, we still can obtain a comprehensive view of privacy protection and preservation in cloud environments from this paper. That is the main goal of this paper. Hence, in this section, we present further discussions to obtain a clear view on future cloud privacy protection and preservation.

In the following parts, we discuss cloud privacy protection and preservation in this view, and make some future discussions.

A. Privacy protection and preservation in cloud client interface level

At the cloud client interface level, we believe that privacy protection and preservation have become very important issues in cloud computing. In existing distributed systems, privacy protection and preservation at customer sides are not the emphasis in whole privacy protection architectures, for the efficiency and economics. But in cloud environments, customers have to deploy all data or information into clouds, so they need confidence for their privacy. Privacy protection and preservation at cloud service sides are necessary and crucial to establish the confidence, and privacy protection and preservation approaches grasped by customers are indispensable issues to support the confidence in opaque and unknown cloud environments. Hence, privacy protection and preservation at cloud customer interface level are promising areas in privacy.

In the future, we believe that about cloud privacy protection and preservation at cloud client interface level, there are some aspects which are quite important: 1) for pre-actioned privacy protection and preservation approaches, cryptograph approaches, including secure computation, should consider to be practical in cloud environments, especially in efficiency, such as [11, 40]; 2) for post-actioned privacy protection and preservation approaches, noise obfuscation is a suitable method to decrease the extent of damage after private information leaking, such as [17, 41].

B. Privacy protection and preservation in cloud service application level

In current research, much work focuses on this cloud service application level, which is obvious in Section II. That is because: 1) at this level, kinds of cloud service applications with different cloud service providers can express various privacy requirements. Therefore, kinds of privacy protection and preservation approaches have to be developed to match these privacy requirements. 2) Many existing traditional privacy protection and preservation approaches can be utilised directly at this level. For cloud service providers, cloud service applications are quite similar to service applications in other distributed environments. So, privacy protection and preservation approaches are quite similar, too. 3) At this level, different types of privacy can be discussed and investigated one by one. And for these types of privacy, more different appropriate privacy functions or protocols can be designed in cloud environments on the basis of existing privacy protection and preservation approaches. In general, privacy protection at cloud service application level is an important part of whole cloud privacy protection, currently.

In the future, we believe that about the cloud privacy protection and preservation at cloud service application level, there are some aspects should obtain adequate attentions: 1) for ‘new’ service applications in cloud environments compared to traditional environments, particular privacy protection and preservation approaches have to be considered and presented. As an interesting beginning, Itani et al. [42] discuss the “privacy as a service” idea to push cloud privacy protection into business. 2) It is promising to investigate the cooperation among different kinds of privacy protection and preservation approaches in cloud environments, for complicated private information and roles in cloud.

C. Privacy protection and preservation in application platform level

At the application platform level, privacy protection and preservation are important issues. In brief, privacy protection and preservation at application platform level are quite novel fields in privacy protection and preservation. As far as we concerned, this research field is a new and promising area. There are two main reasons: 1) application platforms are key issues in cloud services. For cloud service customers and providers, application platforms are necessary to organise and manage cloud systems to support cloud service applications. 2) Some common application platforms could make privacy protection and preservation at this level face a great versatility as a privacy challenge. Cloud service applications are various to match customers’ requirements, but application platforms have some common standards to be utilised as a foundation for service applications.

In the future, we believe that about cloud privacy protection and preservation at application platform level, there are some aspects which should get adequate attentions: 1) about ‘new’ application platforms, types of particular privacy protection and preservation approaches have to be considered and presented in different operating conditions. 2) About hybrid cloud architecture, it is promising to be practical for its combination of utility and privacy. An interesting work [31] on MapReduce in hybrid cloud has been presented under this topic. 3) About large datasets in cloud, privacy protection and preservation have to consider dealing with this condition, from the perspective of efficiency and economic.

D. Privacy protection and preservation in cloud management platform level

At the cloud management platform level, privacy protection and preservation are important issues for the novel cloud environments, too. But, there are still two main points in terms of privacy protection and preservation: 1) cloud management platforms are key components in cloud. For cloud service providers, cloud management platforms are the basis to build cloud systems. 2) In current cloud management platforms, privacy protection and preservation just start to be discussed specially to match the key role of cloud operation platforms in cloud systems. So, the bridging function of this level between the application platform level and the VM management platform level makes privacy protection and preservation at this level to be an effectiveness multiplier for cloud privacy protection.

In the future, we believe that cloud privacy protection and preservation at cloud operating platform level have some aspects that should get adequate attentions: 1) for specific cloud operating service platforms, types of particular privacy protection and preservation approaches have to be considered. For example, Hadoop has been utilised in cloud environments widely, and different data distribution strategies could influence privacy protection and preservation approaches. 2) Open-source cloud service management platforms can obtain a lot of attentions for their openness and be analysed in terms of privacy leakage, especially from privacy attackers. So, it is important to investigate this kind of cloud management platforms from the perspective of privacy protection, such as Openstack [32]. 3) In general, everything in cloud should be charged for usage. So, in cloud management platforms, cost should be considered to get a better efficiency in privacy protection [43].

E. Privacy protection and preservation in VM management platform level

At the VM management platform level, privacy protection and preservation are important research issues, too. Obviously, there are two main reasons: 1) VMs are key issues in cloud services. For cloud service providers, VMs are the basis to manage all kinds of cloud resources together to serve upper cloud service levels at cloud service sides. 2) Currently, VMs have been utilised widely. So they already get enough attentions from malicious attackers, and their privacy vulnerabilities have been investigated. In cloud environments with the openness feature, privacy protection and preservation at this level should be investigated carefully to support whole cloud privacy protection and preservation. Besides, privacy protection and preservation approaches applied at VM management platform level could focus on improving at two aspects: the effectiveness and efficiency of privacy protection with deployments.

In the future, we believe that about cloud privacy protection and preservation at VM management platform level, there are some aspects that should be emphasised: 1) for the combination of different VMs sources in cloud, it is predictable that some 'malicious' ones can be a privacy risk in this kind of environments. So, some approaches have to be presented to build a safe and secure cloud environment with several VMs, just like [44]. 2) For privacy-stealing attacks focusing on VMs, identity managements in VMs could be analysed by attackers to obtain privacy vulnerabilities, so it is necessary to keep eyes on this area [45]. 3) Just like at the former level, cost on privacy protection is a valuable topic at this level [46].

F. Privacy protection and preservation in physical computing, storage and network level

At the physical computing, storage and network level, just like introduced before, privacy protection and preservation consider some basic approaches to be executed. In cloud environments, complex and unknown service conditions require these basic approaches to keep private information safe at this level. In general, privacy protection and preservation at physical computing, storage and network level are to make sure privacy safe in the view of basic OSs in cloud.

In the future, we believe that about cloud privacy protection and preservation at physical computing, storage and network level, there are some aspects should obtain adequate attentions: 1) for cloud data, a cloud environment means a great challenge for privacy protection and preservation to withstand serious attacks, especially side channel attacks [7, 47]. 2) For network anonymity, cloud computing has to utilise it into one kind of environments with various types of privacy attacks in this opaque condition [48].

In summary, cloud privacy protection and preservation deserve more and more attentions from different angles, including system design, build and maintenance. Besides, as one of the most complex computing environments, cloud computing will certainly involve unforeseeable challenges in privacy protection and preservation. Hence, it is necessary to analyse cloud privacy risks, and design cloud privacy protection and preservation approaches. For example, 1) for cloud customers, before they join in cloud environments, some actions and measures applied at client sides can give them confidence to use cloud services. 2) For cloud service providers, just like other service providers in existing computing environments, malicious customers or attackers are the major concerned target in privacy protection and preservation. 3) For most service providers, living in the cloud 'ecological' environment, it is necessary to communicate or cooperate with each other. So, other 'malicious' service providers may be privacy attackers or thieves. 4) For service providers, internal control and management in privacy protection and preservation are necessary to avoid some unintentional privacy leakages, and so on.

In NIST's guideline on security and privacy in public cloud computing [49], governance, compliance, trust, architecture, identity and access management, software isolation, data protection, availability and incident response are various important views to enhance security and privacy in cloud. They are general principles which have to be utilised in whole cloud service levels, from the perspective of the cloud system integration and architecture. On the basis of that, cloud privacy protection and preservation approaches have to be analysed to realise some of these views at different cloud service levels. In other words, cloud privacy protection and preservation pursue reasonable efforts from these views and give confidence to cloud customers, services and other related roles, like legislations. So, cloud privacy protection and preservation are promising research areas in cloud computing, and deep investigation in these views can enhance the development of cloud computing.

IV. CONCLUSIONS AND FUTURE WORK

In this paper, we have systematically analysed open research problems in the field of cloud privacy protection and preservation, and classified their key research issues. The paper depicts a comprehensive picture and provides some insights into further potential research points for cloud privacy protection and preservation. Our ongoing and future work is to investigate such issues, by developing new and evaluating existing privacy protection and preservation approaches.

ACKNOWLEDGEMENT

The research work reported in this paper is partly supported by Australian Research Council under LP0990393 and LP110100228.

REFERENCE:

[1] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as The 5th Utility," *Future Generation Computer Systems,* 25(6): 599-616, 2009.

[2] Aaron Weiss, "Computing in The Clouds," *ACM Networker,* 11(4): 16-25, 2007.

[3] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H.Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, and Z. Matei, "Above the Clouds: A Berkeley View of Cloud Computing," *Communications of the ACM,* 53(6): 50-58, 2010.

[4] Siani Pearson, Yun Shen, and Miranda Mowbray, "A Privacy Manager for Cloud Computing," 1st International Conference on Cloud Computing (CloudCom 2009), pp. 90–106, Beijing, China, December 1-4, 2009.

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

[6] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, and Jesus Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control," 2009 ACM Workshop on Cloud Computing Security (CCSW 2009), pp. 85-90, Chicago, Illinois, USA, November 9-13, 2009.

[7] Martin Mulazzani, Sebastian Schrittwieser, Manuel Leithner, Markus Huber, and Edgar Weippl, "Dark Clouds on the Horizon: Using Cloud Storage as Attacks Vector and Online Slack Space," 20th USENIX Security Symposium, pp. 11, San Francisco, California, USA, August 8–12, 2011.

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

[9] Stephen McLaughlin, Patrick McDaniel, and William Aiello, "Protecting Consumer Privacy from Electric Load Monitoring," 18th ACM Conference on Computer and Communications Security (CCS' 11), pp. 87-98, Chicago, Illinois, USA, 17-21 October, 2011.

[10] Andrew Chi-Chih Yao, "Protocols for Secure Computations," 23rd Annual Symposium on Foundations of Computer Science (SFCS' 82), pp. 160-164, Chicago, Illinois, USA, Novenmber 3-5, 1982.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

[16] 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.

[17] 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.

[18] 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.

[19] 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.

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

[21] 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.

[22] 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.

[23] Amos Beimel, Yuval Ishai, and Eyal Kushilevitz, "General Constructions for Information-Theoretic Private Information Retrieval," *Journal of Computer System Science,* 71(2): 213-247, 2005.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] Openstack. (2012, August 22). Available: http://openstack.org/

[33] 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.

[34] 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.

[35] Ahmed M. Azab, Peng Ning, and Xiaolan Zhang, "SICE: A Hardware-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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou, "Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data," 30th IEEE International Conference on Computer Communications (IEEE INFOCOM 2011), pp. 829-837, Shanghai, China, April 10-15 2011.

[41] Gaofeng Zhang, Yun Yang, Dong Yuan, and Jinjun Chen, "A Trust-based Noise Injection Strategy for Privacy Protection in Cloud Computing," *Software: Practice and Experience,* 42(4): 431-445, 2012.

[42] Wassim Itani, Ayman Kayssi, and Ali Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC '09), pp. 711-716, Chengdu, China, December 12-14 2009.

[43] Xuyun Zhang, Chang Liu, Jinjun Chen, and Wanchun Dou, "An Upper-Bound Control Approach for Cost-Effective Privacy Protection of Intermediate Dataset Storage in Cloud," 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC' 11), pp. 518-525, Sydney, Australia, December 12-14, 2011.

[44] Qian Liu, Chuliang Weng, Minglu Li, and Yuan Luo, "An In-VM Measuring Framework for Increasing Virtual Machine Security in Clouds," *Security & Privacy, IEEE,* 8(6): 56-62, 2010.

[45] Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," 16th ACM Conference on Computer and Communications Security (CCS' 09), pp. 199-212, Chicago, Illinois, USA, November 9-13, 2009.

[46] Chang Liu, Xuyun Zhang, Jinjun Chen, and Chi Yang, "An Authenticated Key Exchange Scheme for Efficient Security-Aware Scheduling of Scientific Applications in Cloud Computing," 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC' 11), pp. 372-379, December 12-14, 2011.

[47] Danny Harnik, Benny Pinkas, and Alexandra Shulman-Peleg, "Side Channels in Cloud Services: Deduplication in Cloud Storage," *Security & Privacy, IEEE,* 8(6): 40-47, 2010.

[48] Prateek Mittal, Ahmed Khurshid, Joshua Juen, Matthew Caesar, and Nikita Borisov, "Stealthy Traffic Analysis of Low-Latency Anonymous Communication Using Throughput Fingerprinting," 18th ACM Conference on Computer and Communications Security (CCS' 11), pp. 215-226, Chicago, Illinois, USA, October 17-21, 2011.

[49] Wayne Jansen and Grance Timothy, "Guidelines on Security and Privacy in Public Cloud Computing," National Institute of Standard and Technology , Special Publication 800-144, http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf , Accessed in August 10th, 2012.December 2011.