IJCTA, 10(03), 2017, pp. 149-158
© International Science Press

Trusted Computing Based Security Schemes for Cloud – A Survey

P.V. Samuel Blessed Nayagam* and A. Shajin Nargunam*

Abstract : Cloud computing is becoming a ubiquitous computing environment which enables the service providers to provide flexible service to the cloud users. Securing the computation and protecting the data of cloud users are two major concerns of trusted cloud computing. Recent literatures provide solutions to various security solutions to protect cloud data and computation. In cloud environment the security changeless is induced by both insiders and outsiders associated with the cloud. Tracking and protecting an open access shared computing environment is a challenge. Further building a Trustable dynamic computing resource provisioning scheme pose a number of access control limitations to the operating environment. From the cloud users point, selecting the best cloud environment which offers cost effective, secure and trustable computing platform is a dare. Providing a cost effective security solution to cloud computing require extensive multi-dimensional focus. Mechanism to prove the indirect mutual trust between the cloud service provider and the cloud users enables cloud users to select the trusted service provider. This paper gives the survey of different trusted computing based solutions and a qualitative analysis of security solutions available in recent literature.

Keywords: Cloud Computing, Trusted Computing, Virtual Machines, Security.

1. INTRODUCTION

Clouds are a large pool of virtualized resources such as hardware, development platforms and services which are easily accessible via internet. These resources can be configured dynamically to adjust to a variable load and for an optimum resource utilization. The available pool of resources is used by a pay-per-use model in which service guarantees are offered by the Infrastructure Provider by means of customized Service Level Agreements. Cloud paradigm is becoming popular among businesses as it reduces upfront infrastructure investments and maintenance costs. In a cloud environment the physical location of the data is independent of its representation and the data owner does not have control over the physical placement of data and integrity of virtual machine images loaded by the cloud provider remains an open issue. Important capabilities of cloud computing are its rapid elasticity that allows to scale the provided computational and storage resources in line with the demand, as well as the built-in capability to measure the service at an appropriate level of abstraction.

To ensure trust in a cloud environment, the organization makes a commitment and places trust into the control mechanisms and processes employed by the cloud provider. Trust through the use of cloud computing, the organization relinquishes control over significant parts of aspects of security and privacy. As a result of this, it makes easier for an insider to access the information provoking both intentional incidents leading to loss or corruption of data. Another risk is due to the lack of clarity over data ownership. There are fewer mechanisms for data protection when data is created through cloud services are maintained in cloud storage. The first scheme depends on the migration capabilities offered by the type of the cloud service provider. The second scheme depends on the visibility of the state of the system and the state of the data produced by the cloud.

* Assistant Professor, Professor, Noorul Islam Centre for Higher Education

One of the main issues in cloud environment is separation between a cloud providers and users. The users may be malicious nodes or hackers who intend to avoid inadvertent or intentional access to sensitive information. Cloud provider uses virtual machines (VMs) and a hypervisor to separate customers. Trusted cloud computing technologies can provide significant security improvements for Virtual Machine and virtual network separation. Hardware supported verification ensures verification of hypervisors and virtual machines.

User does not have control nor knowledge of the physical placement of the data in the cloud after scheduling. To ensure strong policies and practices that address cloud security issues, each user should have a legal and regulatory mechanism to inspect cloud provider policies and practices to ensure their adequacy. The trusted storage and trusted platform management and access techniques can play a key role in limiting access to data. An automated monitoring is the best solution for trusted cloud computing base which enables the integration of different security systems and provides real-time notification of incidents and of user misbehavior.

Cloud computing is becoming a ubiquitous computing platform in the recent years to cater to the overriding computational needs of the users. This enables the users to use computing capabilities as an ongoing service rather than building an internal capital infrastructure. In cloud computing, computing takes place over the Internet which enables Utility Computing and use of integrated and networked hardware, software and Internet infrastructure.

The essential Cloud Computing Characteristics are

Massive Scale : Cloud computing provides unlimited computing capabilities by linking various servers and network storages.

Resilient Computing : Distributes redundant implementations of computing and storage resources across physical locations in which processing is automatically handed over to another redundant implementation.

Service Orientation : Service orientation is based on implementing computational processes as software services. These services consist of a set of loosely coupled resources designed to minimize dependencies and can be linked to support a well-defined computational task.

Virtualization : Helps to create a virtual version of computing resources, such as a server, storage device, network or even an operating system.

Rapid Elasticity : Controlled by the effective monitoring scheme, which gives rubber band effect by which more capacity shall be added within minutes with much ease.

Resource Pooling : Ability to serve multiple cloud users by using multitenancy models with different physical and virtual computing resources are dynamically assigned and reassigned according to cloud user demand.

Due to the rapid changes in technology, hybrid cloud environments are becoming popular in organizations. Use of hybrid cloud for performing secured computation and constantly reinventing themselves to respond to the dynamic changes is becoming a challenge in hybrid cloud environments. Cloud computing being the forefront of a business strategy, organizations understand that it’s hard to find one best computing environment to cater to the needs of all types of workloads.

2. RELATED WORKS

In [24], a widely known XML signatures attack was described in which the attacker intercepts a given Simple Object Access Protocol (SOAP) message being sent to the server by another client, replacing its content with some arbitrary request on behalf of the attacked client; Cloud providers are vulnerable to a variation of this signature wrapping attack [19]. To accurately maintain and instantiate VMs (in the case of IaaS) or modules (in the case of PaaS), the cloud provider needs to store metadata descriptions associated with each operation. These metadata descriptions shall be used by an intruder to determine the detailed functionality of a certain service. Jensen et.al. [20] states that spoofing attack can emerge by reengineering this metadata. Metadata spoofing attack [20] allows an adversary to modify metadata descriptions, potentially causing severe damage to the user's service. Another possible approach would be to ensure the establishment of trust relationships with users prior to accepting their requests, although this may not be applicable to some scenarios. Another virtualization-related security issue, raised by Christodorescu et. al. [17], is that vulnerabilities arise from the fact that in highly multiplexed cloud environments, providers often have no control over what types of VMs are being deployed by their clients. Conversely, users also have a very limited knowledge of the under lying physical infrastructure.

Wei et al. [30] explore the possible risks concerning how VM images are stored and managed in the cloud. In cloud environment an attacker can build and share images that are contaminated with malware and other types of threats. In [16] a practical example of how these risks can be exploited on Amazon EC2 and how they should be mitigated is presented. Assuming the attacker was able to place his VM on the same physical machine as the target instance, [26] shows that a malicious adversary may learn information about a co-resident VM via cache-based side channels (which could possibly be used to steal cryptographic keys), as well as other physical resources that are multiplexed among the co-resident instances. This work has been recently expanded by Xu et al. [31] who were able to create similar covert channels with noticeably higher bit rates than previously reported. To remedy this situation where a provider cannot offer appropriate security measures due to the unknown configuration and integrity of its clients' VMs, Christodorescu et al. [32] [17] propose a new architecture based on VM introspection. The concept of VM introspection was first introduced by Garfinkel et al. [18] and more recently formalized in [25].

Another work in the realm of virtualization security [28] proposed a system called NoHype, in which the need for hypervisors is eliminated. Wei et al. [30] were the first to expose the risks involved with the publishing and large scale usage of images. The authors emphasize that the sharing of VM images is of great importance since it largely simplifies administrative tasks and costs related to software installation. A recent work [16] presented practical examples of how these vulnerabilities can be exploited and argued that the increasing competition between cloud providers may become the driving force that will finally push for the security enhancement with regards to cloud VM images. With regard to the security of VMs, we point out the work of Schiffman et al. [27], which provides an architecture that allowed for the performance of runtime integrity proofs in general purpose distributed systems. Jensen et al. [21] describe how flooding attacks are a real threat to clouds. This issue rises in such environments when, for instance, all requests to a certain service need to be individually checked for validity, thereby causing service overloading.

In the attack proposed in [23], the adversary gains control of a few hosts in a certain subnet (i.e., set of nodes connected via a common router) and then simply transmits enough traffic to hosts located elsewhere. In [29], accountability in both cloud and distributed systems are presented. Juels and Kaliski [22] proposed a solution to this problem by implementing the basic functionality of proofs of retrievability. Zhang et al. [33] considered a slightly different scenario, in which a given entity wishes to outsource a large computation where only a portion of the data is sensitive and needs to be processed by a private cloud, whereas the remaining information can be safely outsourced to a public cloud.

3. TRUSTED COMPUTING

Cloud security systems are building extensive efforts to secure the computing systems from the threats of attacks, and trying to strengthen the trustworthiness of the cloud among the customers. Several protection such as access restriction limits to hardware facilities, rigorous accountability and auditing procedures, and restricted number of access to critical components of the infrastructure. But the kernel system resources and administer still possess the technical means to access customers' VMs. Trusted Computing enables the system to enhance the solution that guarantees the confidentiality and integrity of computation, in a way that is verifiable by the cloud users. Trusted computing platforms like Terra [1] take a captivating methodology to this problem. This scheme prevents the owner of a physical host from examining and interfering with a computation. The remote attestation ability enables the cloud user to remotely monitor whether the host can securely run the computation. This scheme can secure a VM running on a single host. But in a public cloud, many providers use hundreds of machines, to run VMs' and can be dynamically scheduled to run on any one of them. This intricacy and the opaqueness of the provider produces vulnerabilities that conventional trusted platforms cannot address.

With root privileges at each machine, the misbehaving sysadmin can mount or execute malicious software to perform an attack. In case of Xen backend, it [2] allows the sysadmin to run a user level process in Dom0 by which the VM's memory content can be accessed at run time.

The trustworthiness can handle with the happening of events such as adding or removing nodes from a cloud, or shutting down nodes temporarily for maintenance. Trusted computing enables the user to verify whether the IaaS service secures its computation or not. To secure the computation of VMs, each node cooperates with the cloud controller in order to restrict the execution of a VM to a trusted node, and to safeguard the VM state against intrusion or modification during transit. In live migration [3], the current state of an executing VM is transferred from the source Ns to a destination Nd. Trusted computing enables safe transfer of VM state and ensure integrity while it is in transit over the network.

In the case that a trusted node reboots, the cloud controller must guarantee that the node's internal configuration remains unchanged, otherwise it could compromise the security. To further ensure security, the node only keeps time specific keys in the temporary memory, causing the key to be lost once the machine reboots. Thus the node is barred from the trusted cloud platform and it will not be able to decrypt messages encrypted with the previous key, and must initiate the registration process.

In order to safeguard the trusted computing in the cloud computing system, it should have the mechanism to monitor the user execution process and also have tracking scheme. The monitoring scheme integrated with the cloud computing system enables supervision of the participants' behavior. This is an extension of reference monitors, which is used in conventional operation systems and be beneficial in cloud computing too.

4. CLOUD SECURITY SCHEMES

Cloud security schemes enforce the system to behave consistently in expected ways with hardware and software support. There are different areas of cloud computing environment where it requires substantial security solutions. The major areas that requires security are cloud data at rest, cloud data in transit, cloud user/application authentication, cloud virtual machine migration and cloud memory sharing among virtual machines. The prime way [4] of integrity checking during remote code execution is called as remote attestation, which generates a hardware certificate to represent what software is running. This certificate can be used by the verifier to prove that the software is unaltered during computation. The prime focus of trusted computing is to ensure that component like the virtual hardware and other codes are not physically altered by the intruder.

A. Trustworthy Distributed Computing

Normally trustworthiness has no direct influence or control over the execution environment, processes, and other services. The trust building is in the hand of the verifier who verifies the trust by assessing and analyzing certain attributes. In a cloud service provider environment, workflow composed of several distributed services that requires the support of the External Service Provision Trust. Trustworthy computing, the trustor commonly coordinates multiple services to create a new trustable service. But the trust verifier has no knowledge of how these services are implemented or executed. In [5] distributed computing constant weight and variable weight tasks are created and these tasks are divided into smaller shares and are distributed to different nodes in the computing system. Initial trust value is assigned based on the similarity-based metric. Based on the cardinality, every node v_x computes its similarity with the neighboring nodes and assign the initial trust according to that. Further, based on the volume of interaction between the nodes, the node trust values are updated. Weighted Distributed Scheduling Scheme is used by the scheduler to schedule the jobs. Node weights are assigned based on the pre-computed trust. It is challenging for an intruder to gain meaningful interaction with other nodes. The nature of outliers in this system fails to differentiate attacker nodes with legitimate resource constrained nodes.

B. Secured Multi-community Clouds

Community cloud uses the pool of sparse resources to cater to the computing needs of cloud users. The proper collaboration among the cloud resources provides a powerful computing environment for performing complex tasks in a multi-community environment. Identifying the optimal community cloud that is secure and trusted to perform a high computational task challenging. In community cloud trust factor plays a key role in task scheduling. As a common point user prefers to choose a community cloud which have been chosen by other known/trusted users for task offloading. The trust relationship between the users and trust between users and clouds are used as the key metric for task offloading. If a direct trust relationship does not exist between any users, then transitive trust relationships are used to infer the trust relationships. The problem of identifying a set of community cloud which maximizes the security based trust enabled is given in [6]. High Security-Level Agreement clouds are selected from the community cloud for executing task. A group of community cloud maximizes the security-based trust-enabled performance price ratio improves the security level, but optimal usage of resources are not effectively considered by the scheduler. The trust values between the cloud and the new user is calculated in transitive route with the help of other nodes which are associated with the cloud and trustable to the new user.

C. Secure Group Sharing Public Cloud

In public cloud computing group data sharing, confidentiality and data protection are two major concerns. In [7] a secure group sharing mechanism for public cloud is proposed which segregate sensitive data and non-sensitive data. It exposes only non-sensitive data to the public cloud. Dynamic secure group sharing framework enables the effective management of access level control to different group members. Management of privilege granted to other selected group members is handled via proxy signature scheme. Group key pairs are updated dynamically when new members join/leave the group. Delegating most of the computing overhead to cloud servers without disclosing the security information improves the overall efficiency. Digital envelopes are updated based on proxy re-encryption, which in turn dilute the security boundary. To avoid single point overhead in managing the group members, group leader authorize some group members to manage the group.

D. Indirect Mutual Trust for Cloud Computing

Building indirect trust enables the cloud users to outsource the sensitive data to the cloud service provider. The block level dynamic operation presented in [8], ensures that it allows only the authorized users to add, delete or modify the outsourced data. The cloud service provider also ensures that authorized users receive the updated version of the outsourced data. It also allows the data owner to dynamically change the access control list of the outsourced data as per the changing needs. The authorized user sends data access request to cloud service provider and trusted third party, which in turn receives two signatures (one from CSP and another from TTP). Users holding the valid signatures are allowed to access the outsourced data from CSP. Data owner attach a tag with each block before outsourcing, which will be verified by the CSP for integrity and freshness of Data. Dual signature generation and verification process increases the computational overhead.

E. Proof-Carrying Cloud Computing

Without sufficient trust, it is difficult for the cloud users to completely hand over the control of computation to the cloud service provider. In [9] a client side integrity verification mechanism for outsourcing computation is presented. In order to reduce the complexity of the verification process, it uses the inherent structure of the optimization mechanism for integrity verification. Optimization based proof-carrying verification ensures significant computational saving at client side and introduces minimal overhead on the cloud. Even though the integrity verification scheme ensures less computational overhead, it can be applied only to engineering optimization solutions.

F. Dynamic Trusted Scheduling

Building trusted computing in a highly dynamic heterogeneous distributed open system is a key challenge. To ensure secure execution of jobs in a dynamic computing environment, trusted dynamic level security scheme is presented in [10]. The cooperation based probability scheme is used to represent the trust level of each node in the cloud. A static scheduling heuristics which creates a DAG-structure facilitate the scheduler to select the trustable nodes for computation. Trust analyzer monitors the trust level of local nodes and communicate the trust factor of each node. This enables the scheduler to schedule the task on the most trustworthy node in the cloud. Different types of QoS requirements create challenges in large dynamic cloud systems.

G. Secure Data Self-Destructing Scheme

Extended lifecycle of sensitive data in the cloud is becoming increasingly vulnerable to cloud users. A time specific attribute based encryption is presented in [11] for automatic self-destruction of data from the cloud immediately after its lifetime. In this scheme, it allows to decrypt the cypher only if data time label matches with the time attribute associated with the private key. During memory paging time expired cyphers are removed from the memory. This scheme securely delete the outsourced data in the cloud servers after the specified usage period. Secure data-self destructing scheme helps to deactivate the outsourced data after the usage period. But the communication overhead increases because of time specified key exchange process. Time and attribute based encryption and decryption process increases the computational overhead also.

H. Trust-Aware Service Brokering Scheme

Understanding the trust degree of users and identifying the trustable cloud environment based on the users demand is a crucial issue in the multi cloud environment. In [12] a trust aware service brokering scheme is used to match the cloud services for various user requests. A trusted third party based brokering architecture is used for trust matching. In this the T-Broker acts as a middleware for cloud trust management and service users. The trust is measured in terms of directly monitored evidence and feedback received from other resource. Dynamic changing cloud nature in a multi cloud environment increases the communication and computational overhead.

I. Secure Data Access Control

Data owner publishes sensitive data in the cloud and fine-grained access control scheme ensures which data consumer has the access privilege to the data. Cipher-text policy attribute based encryption scheme in [13] uses fine-grained access control mechanism which enforces policy based user attributes for encryption. In order to provide access permission to new cloud users, data owner assigns new sets of attributes and the secret key associated with these attributes is generated. The version number associated with the secret key helps to ensure the freshness and validity of the secret key. In this scheme policies are enforced based on user attributes. Data owner delegates most of the laborious user revocation task to cloud services. The data set attributes are removed by the data owner, if necessary and a new set of attributes is assigned. Cloud servers update the new attributes in the access control list, re-encrypt the data and update the secret key if necessary. Re-encryption and attribute updates at the server side reduces computation overhead brought to the data owner. It is resistant to collusion attacks and protects user access privilege information. Attribute policy based scheduling scheme needs to be identified and the performance of the system degrades as the number of cloud users increases.

J. Authentication Scheme for Mobile Cloud

For mobile users, it is tedious to register different user accounts on each service provider and maintaining different private keys for authentication. In [14] a security scheme which provides access to different cloud computing services from multiple service providers using single private key is presented. It uses bilinear pairing and dynamic nonce generation to generation of a single private key which can be used by the mobile users for authentication. An anonymous user authentication scheme based on bilinear pairing is used to support mutual authentication. It uses an identity-based cryptosystem which uses identities of mobile users and service providers for generating public key. The system is stable for most of the authentication threats imposed on mobile cloud users. No verification table is required at the service providers' side for authentication and it reduces authentication processing time, communication and computation time.

Table 1
Scalability Rates of Existing Cloud Security Schemes

Reference	*Basic Theory*	*Security Features*	*Scalability*
[5]	Weighted Distributed Scheduling.	Trust Based Weight Assignment	Low
[6]	Manage trust level between user and cloud	Trust-enabled performance price ratio.	Medium
[7]	Group Key Sharing Scheme	Session Keys and Digital Envelops	Medium
[8]	Access Control Tag	Data Access is restricted	Low
[9]	Optimization based Outsourcing	Client side verification	High (Optimization)
[10]	Static scheduling with DAG	Trust based scheduling	High (Limited QoS)
[11]	Time-specified attribute based encryption	Secure data-self destructing scheme	High
[12]	Trusted Third party based brokering	Indirect Trust Monitoring	Medium
[13]	Policy attribute based Encryption	Resist collusion attacks and protects ACL	High
[14]	Bilinear pairing is used to support mutual authentication	Identity-based cryptosystem	High
[15]	Service-oriented workflow in scheduling	Trust Based Scheduling	High/Medium

K. Trust Based Service Oriented Scheduling

Assigning complex tasks to unknown service providers may cause failure to the execution. So trust between the service provider and services is essential for collaborative process in the cloud. Work flow based scheduling algorithms normally focus on execution time and computational cost. But in a dynamic cloud environment work flow based scheduling faces uncertainty and unreliability. A trust service based scheduling scheme is presented in [15]. A trust metric with the combination of direct trust and recommended trust is used for service workflow scheduling. The scheduling algorithm uses the trust factor and service-oriented workflow in scheduling the jobs. The policy balancing scheme enables the user to balance the different requirements such as time, cost and trust. This scheduling scheme finds the optimal solution within the deadline constraint. The performance of the system is not stable under uncertain and unreliable environments. Dynamic runtime changes affect the statically predetermined schedule.

5. CONCLUSION

The purpose of this survey is to describe the present day issues in trusted cloud computing, trusted scheduling and their relevant contexts. Trustworthy computing and trust based scheduling is used for comprehension and comparison to trust in different usages. The different types of trust properties, service differentiation based on sensitive data, authentication and access control limitations are presented, mainly relevant to enhance trustworthiness of a cloud computing environment. The discussion of the strengths and weaknesses of different cloud computing security schemes with the directions of future research along the way is provided. Table 1 shows the different cloud security schemes available in the literature and their scalability measures.

Based on this, it is observed that the trust relationship between the cloud users and the cloud service providers are used as the key metric for task offloading and trust building mechanisms provides a way for scaling a trustable cloud computing environment. Indirect mutual trust and dynamic integrity verification process also help to create a trustworthy computing platform in a multi cloud environment. Trust matching and trust based scheduling schemes also supports trusted computing. But providing a cost effective, efficient trust based computing solution and building formal system trust need more study because of the dynamic nature of the distributed computing environments. Investigating secured cloud computing and trusted computing based cloud solutions would yield a great research contribution. Because providing flexible, scalable, open cloud computing system impose, much more security challenges. In a distributed cloud computing environment, malicious VM co-resided with the victim VM and shares physical resources like as data cache, network access, processor, memory and CPU pipelines. To protect the system from such types of attacks, complete access protection and process monitoring schemes are required. The computational and communication overhead incurred by such protection schemes drastically degrades the overall performance of the computing environment. Integrating several cloud services to build a composite trustable cloud computing platform is still a research challenge.

6. REFERENCES

1. T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh. Terra: A Virtual Machine-Based Platform for Trusted Computing. In Proc. of SOSP’03, 2003.
2. B. D. Payne, M. Carbone, and W. Lee. Secure and Flexible Monitoring of Virtual Machines. In Proc. of ACSAC’07, 2007.
3. C. Clark, K. Fraser, S. Hand, J. G. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield. Live migration of virtual machines. In Proc. of NSDI’05, pages 273–286, Berkeley, CA, USA, 2005. USENIX Association
4. N. Santos, K.P. Gummadi, and R. Rodrigues, “Towards trusted cloud computing,” Proc. 2009 conference on Hot topics in cloud computing, 2009.
5. Aziz Mohaisen, Abhishek Chandra and Yongdae Kim, “Trutworthy Distributed Computing on Social Networks”, IEEE Transactions on Services Computing, Vol. 7, No. 3, July-September 2014.
6. Fei Hao, Geyong Min, Jinjun Chen, Fei Wang, Man Lin, Changqing Luo and Laurence T. Yang, “An Optimized Computational Model for Multi-Community-Cloud Social Collaboration”, IEEE Transactions on Services Computing, Vol. 7, No. 3, July-September 2014.
7. Kaiping Xue and Peilin Hong “A Dynamic Secure Group Sharing Framework in Public Cloud Computing”, IEEE Transactions on Cloud Computing, Vol .2, No.4, October-December 2014.
8. Ayad Barsoun and Anwar Hasan “Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems”, IEEE Trans. On Parallel and Distributed Systems. Vol.24, No.12, December 2013.
9. Zhen Xu, Cong Wang, Kui Ren, Lingyu Wang, and Bingsheng Zhang, “Proof-Carrying Cloud Computation: The Case of Convex Optimization”, IEEE Trans On Information Forensics and Security, Vol.9, No. 11, November 2014.
10. Wei Wang, Guosun, Daizhong Tang, Jing Jao , “Cloud-DLS: Dynamic Trusted Scheduling for Cloud computing”, Expert Systems with Applications 39(2012) 2321-2329.

11. Jinbo Xiong, Ximeng Liu, Zhiqiang Yao, Jianfeng Ma, Qi Li, Kui Geng, and Patrick S.Chen, "A Secure Data Self Destructing Scheme in Cloud Computing", IEEE Transactions on Cloud Computing , Vol . 2, No. 4. October-December 2014.

12. Xiaoyong Li, Huadong Ma, Feng Zhou, and Wenbin Yao, "T-Broker: A Trust-Aware Service Brokering Scheme for Multiple Cloud Collaborative Services", IEEE Transactions on Information Forensics and Security, Vol.10, No. 7, July 2015.

13. Heng He, Ruixuan Li, Xinhua Dong and Zhao Zhang, "Secure, Efficient and Fine –Grained Data Access Control Mechanism for P2P Storage Cloud", IEEE Transactions on Cloud Computing, Vol. 2, No. 4, October- December 2014.

14. Jia-Lun Tsai and Nai-Wei Lo, "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services", IEEE Systems Journal, Vol. 9, No. 3, September 2015.

15. WenAn Tan, Yong Sun, Ling Xia Li, GuangZhen Lu, and Tong Wang, "A Trust Service –Oriented Scheduling Model for Workflow Applications in Cloud Computing", IEEE Systems Journal, Vol. 8, No. 3, September 2014.

16. Bugiel, S., Nurnberger, S., Poppelmann, T., Sadeghi, A.R., Schneider, T.: AmazonIA: When elasticity snaps back. In: Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS'11, pp. 389–400. ACM, New York, NY, USA (2011). DOI 10.1145/2046707.2046753

17. Christodorescu, M., Sailer, R., Schales, D., Sgandurra, D. , Zamboni, D. : Cloud security is not (just) virtualization security. In: Proceedings of the ACM Cloud Computing Security Workshop, CCSW'09, pp. 97–102. ACM, New York, NY, USA (2009). DOI 10.1145/1655008. 1655022

18. Garfinkel, T., Rosenblum, M.: A virtual machine introspection based architecture for intrusion detection. In: Proceedings of Network and Distributed Systems Security Symposium, NDSS'03, pp. 191–206 (2003)

19. Gruschka, N., Iacono, L.: Vulnerable cloud: SOAP message security validation revisited. In: Proceedings of the IEEE International Conference on Web Services, ICWS'09, pp. 625–631. IEEE Computer Society, Washington, DC, USA (2009). DOI 10.1109/ICWS.2009.70

20. Jensen, M., Gruschka, N., Herkenhoner, R.: A survey of attacks on web services. Computer Science – Research and Development 24(4), 185–197 (2009)

21. Jensen, M., Schwenk, J., Gruschka, N., Iacono, L.: On technical security issues in cloud computing. In: Proceedings of the IEEE International Conference on Cloud Computing, CLOUD'09, pp. 109–116. IEEE Computer Society, Washington, DC, USA (2009). DOI 10.1109/CLOUD.2009.60

22. Juels, A., Kaliski, B.: PORs: Proofs of retrievability for large files. In: Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS'07, pp. 584–597. ACM, New York, NY, USA (2007). DOI 10.1145/1315245.1315317

23. Liu, H.: A new form of DOS attack in a cloud and its avoidance mechanism. In: Proceedings of the ACM Cloud Computing Security Workshop, CCSW'10, pp. 65–76. ACM, New York, NY, USA (2010). DOI 10.1145/1866835.1866849

24. McIntosh, M., Austel, P.: XML signature element wrapping attacks and countermeasures. In Proceedings of the Workshop on Secure Web Services, SWS'05, pp. 20–27. ACM, New York, NY, USA (2005). DOI 10.1145/1103022.1103026

25. Prof. J., Schneider, C., Eckert, C.: A formal model for virtual machine introspection. In: Proceedings of the 1st ACM Workshop on Virtual Machine Security, VMSec'09, pp. 1–10. ACM, New York, NY, USA (2009).DOI 10.1145/1655148.1655150

26. Ristenpart, T., Tromer, E., Shacham, H., Savage, S.: Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS'09, pp. 199–212. ACM, New York, NY, USA (2009). DOI 10.1145/1653662.1653687

27. Schiffman, J., Moyer, T., Shal, C., Jaeger, T., McDaniel, P Justifying integrity using a virtual achine verifier. In: Proceedings of the Computer Security Applications Conference, ACSAC'09, pp. 83–92. IEEE Computer Society, Washington, DC, U S A (10.1109/ACSAC.2009.18

28. Szefer, J., Keller, E., Lee, R., Rexford, J.: Eliminating the hypervisor attack surface for a more secure cloud. In: Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS'11, pp. 401–412. ACM, New York, NY, USA (2011). DOI 10.1145/2046707. 2046754

29. Wang, C., Zhou, Y.: A collaborative monitoring mechanism for making a multitenant platform accountable. In: Proceedings of the 2nd USENIX Conference on Hot Topics in Cloud Computing, HotCloud'10. USENIX Association, Berkeley, CA, USA (2010)

30. Wei, J., Zhang, X., Ammons, G., Bala, V., Ning, P.: Managing security of virtual machine images in a cloud environment. In: Proceedings of the ACM Cloud Computing Security Workshop, CCSW'09, pp. 91–96. ACM, New York, NY, USA (2009). DOI 10.1145/1655008. 1655021

31. Xu, Y., Bailey, M., Jahanian, F., Joshi, K., Hiltunen, M., Schlichting, An exploration of L2 cache covert channels in virtualized environments. In: Proceedings of the 3rd ACM Cloud Computing Security Workshop, CCSW'11, pp. 29–40. ACM, New York, NY, USA (2011). DOI 10.1145/2046660.2046670.

32. Yumerefendi, A., Chase, J.: Strong accountability for network storage. Transactions on Storage 3(3), 11:1–11:33 (2007). DOI 10.1145/1288783.1288786

33. Zhang, K., Zhou, X., Chen, Y., Wang, X., Ruan, Y.: Sedic: Privacy-aware data intensive computing on hybrid clouds. In: Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS'11, pp. 515–526. ACM, New York, NY, USA (2011). DOI 10.1145/2046707.2046767