Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 92 (2016) 128 – 135

Procedia Computer Science

2nd International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2016)

Srikanta Patnaik, Editor in Chief

Conference Organized by Interscience Institute of Management and Technology

Bhubaneswar, Odisha, India

A Study on Data Storage Security Issues in Cloud Computing

Naresh vurukonda[1], B.Thirumala Rao[2]

[1,2]Department of CSE, KLUniversity, Vijayawada, A.P, INDIA

[1] naresh.vurukonda@gamil.com, [2] drbtrao@kluniversity.in

Abstract

Cloud computing is a revolutionary mechanism that changing way to enterprise hardware and software design and procurements. Because of cloud simplicity everyone is moving data and application software to cloud data centers. The Cloud service provider (CSP) should ensure integrity, availability, privacy and confidentiality but CSP is not providing reliable data services to customer and to stored customer data. This study identifies the issues related to the cloud data storage such as data breaches, data theft, and unavailability of cloud data. Finally, we are providing possible solutions to respective issues in cloud.

Peer-review under responsibility of the Organizing Committee of ICCC 2016

Keywords: Cloud service provider (CSP), cloud data storage, security issues, policies & protocols;

1. Introduction

Cloud computing is a revolutionary mechanism that changing way to enterprise hardware and software design and procurements. The cloud computing provides rich benefits to the cloud clients such as costless services, elasticity of resources, easy access through internet, etc. From small to large enterprises poignant towards cloud computing to increase their business and tie-ups with other enterprises [1]. Even though cloud computing has enormous benefits, cloud user are unwilling to place their confidential or sensitive data, it includes personal health records, emails and government sensitive files. Suppose once data are placed in cloud datacenter; the cloud client lost their direct control over their data sources. The Cloud Service Provider(CSPs) has promise to ensures the data

Peer-review under responsibility of the Organizing Committee of ICCC 2016

doi:10.1016/j.procs.2016.07.335

security over stored data of cloud clients by using methods like firewalls and virtualization. These mechanisms would not provide the complete data protection because of its vulnerabilities' over the network and CSPs have full command on cloud applications, hardware and client's data. Encrypting sensitive data before hosting can deserve data privacy and confidentiality against CSP. A typical problem with encryption scheme is that it is impractical because of huge amount communication overheads over the cloud access patterns. Therefore, cloud needs secure methods to storage and management to preserve the data confidentiality and privacy [2][5]. This paper mainly focuses on security vulnerabilities and issues in confidentiality and privacy over client data.

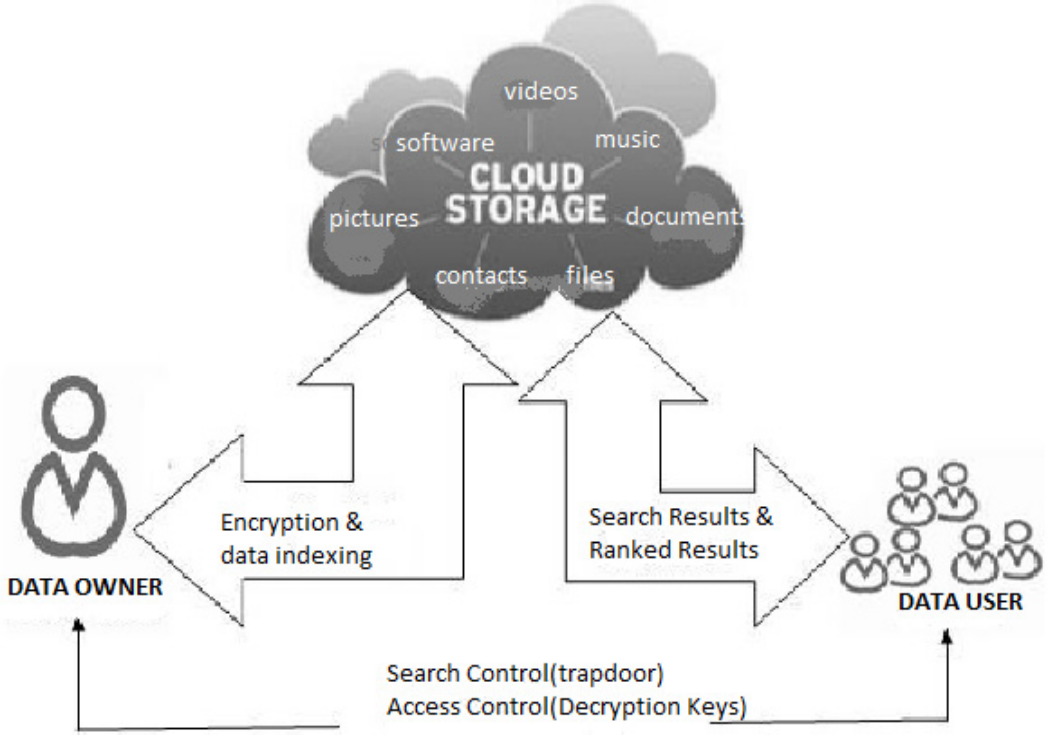

Figure 1: Cloud data storage model.

2. Cloud Data Storage Challenges & Issues

The cloud computing does not provide control over the stored data in cloud data centers. The cloud service providers have full of control over the data, they can perform any malicious tasks such as copy, destroying, modifying, etc. The cloud computing ensures certain level of control over the virtual machines. Due to this lack of control over the data leads in greater security issues than the generic cloud computing model as shown in figure 1. The only encryption doesn't give full control over the stored data but it gives somewhat better than plain data. The characteristics of cloud computing are virtualization and multi tenancy also has various possibilities of attacks than in the generic cloud model. The figure 2 has various issues those are discussed below in clearly.

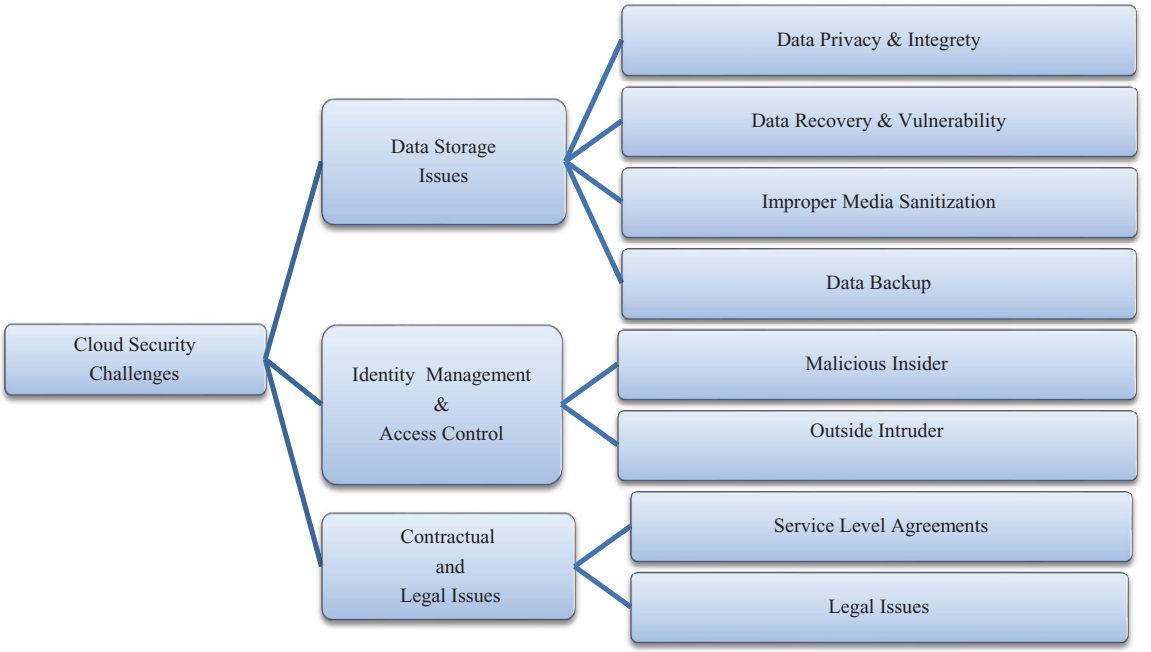

Figure 2. Cloud security Challenges

2.1 Cloud Storage issues

2.1.1 Data privacy and Integrity

Even though cloud computing provide less cost and less resource management, it has some security threats. As we discussed earlier cloud computing has to ensure integrity, confidentiality, privacy and availability of data in generic cloud computing model but the cloud computing model is more vulnerable to security threats in terms of above conditions. Because of simplicity cloud users are increasing exponentially and applications are hosted in cloud is very high. These situations lead to greater security threats to cloud clients. If any attack is successful on data entity will leads to data breach and takes an unauthorized access to data of all cloud users. Because of this integrity violation cloud data lost multi-tenant nature. Especially SaaS providers may also lost their technical data and they have great risk over data storage. Apart from these risks, data processing also has great risk while data being transformed among multiple tenants. Because of virtualization multiple physical resources are shared among the users. This leads to launch attacks by malicious insiders of the CSP and/or organization. These situations may allow the malicious user to perform attacks on stored data of other customer while processing their data. Other major risk is when data is outsourced to third party storage by the CSP [5]. The key generation and key management in cryptography for cloud computing is not standardized up to the mark. But without standard and secure key management for the cloud doesn't allow the standard cryptography algorithms to perform well in generic cloud computing model. Such that cryptography may also ensures the potential risks to cloud computing.

2.1.2 Data recoverability and vulnerability

Due to resource pooling and elasticity characteristics, the cloud ensures dynamic and on-demand Resource provisioning to the users. The resource allocated to a particular user may be assigned to the other user at some later point of time. In case of memory and storage resources, a malicious user can employ data recovery techniques to

obtain the data of previous users [13]. The authors in [13] were able to recover Amazon machine images files 98 % of the times. The data recovery vulnerability can pose major threats to the sensitive user data.

2.1.3 Improper media refinement.

The storage medias are sanitize because of following reasons (i) the disk may needs to replace with other disk (ii) No need to maintain the disk or no longer to maintain (iii) massacre of services. Improper refinement ensures great risk to stored data. In multi-tenant cloud it is not possible to refine as it is earlier tenant.

2.1.4 Data backup

The data backup is an important when accidental and/or intentional disasters. The CSP has to perform regular backups of stored to ensure the data availability. In fact, the backup data should be keeping with security guidelines to prevent malicious activities such as tampering and unauthorized access.

2.2. Identity Management and Access Control

The integrity and confidentiality of data and services are related with access control and identity management. It is important to maintain track record for user identity for avoiding unauthorized access to the stored data. The identity and access controls are complex in cloud computing because of that data owner and stored data are at different executive platforms. In cloud environment, different organizations use variety of authentication authorization agenda. By using different approaches for authentication and authorization gives a compound situation over a period of time. The cloud resources are dynamic and are elastic for cloud user and IP addresses are continuously changed when services are started or restarted in pay per usage model. That allows the cloud users to join and leave feature to cloud resources when they required i.e., on-demand access policy. All these features need efficient and effective access control and identity management. The cloud has to maintain quickly updating and managing identity management for joining and leaving users over cloud resources. There are many issues in access control and identity management, for example weak credentials may reset easily, denial of service attack to lock the account for a period of time, Weak logging and monitoring abilities, and XML wrapping attacks on web pages.

2.2.1 Malicious Insiders

An insider threat can be posed by employees, contractors and /or third party business partners of an organization. In cloud environment i.e., at Cloud Service Provider (CSP) side attacks leads to loss of user's information integrity, confidentiality, and security. This leads to information loss or breaches at both environments.. This attack is precious and it is well known to most of the organization [7].There is variety of attack patterns performed by insiders because of sophistication about internal structure of an organization data storage structure. Most organizations ignoring this attack because it is very hard to defend and impossible to find the complete solution for this attack. This attack ensures great risk in terms of data breaches and loss confidentiality at both organization and cloud level [8].

2.2.2 outside Intruder

Attacks that come from external origins are called outsider attacks [30]. Data security is one of the important issue in cloud computing. Since service providers does not have permission for access to the physical security system of data centers. But they must depend on the infrastructure provider to get full data security. In a virtual private cloud environment, the service provider can only specify the security setting remotely, and we don't know exactly those are fully implemented. In this Process, the infrastructure provider must reach the following objectives: (1) confidentiality, for secure data transfer and access, and (2) audit ability [31]. So that outside intruders can't access sensitive data which is stored in cloud.

2.3 Contractual and Legal issues

After moving to cloud computing environment, there are many issues in geographic jurisdictions, regulatory law, performance assurance, contract enforcements, etc. The above mentioned issues are comes under the legalities, Service Level Agreements and data location in data centers [9].

2.3.1. Service level agreements

The Service Level Agreement (SLA) can be described as a protocol, it specifies set of conditions and terms among user and Cloud service provider. The SLA should specify the following: Actions that CSP will taken when data breach happened, remedial actions and performance level at minimum level [5]. The users should have clear view on security for their resources and all other requirements should be agreed upon the SLA. The contract enforcement becoming issues because statistics provided by CSP are totally unproven. Finally, the contracts are non-negotiable and pre-defined that has to be in friendly manner between CSP and user. The regulatory laws such as Sarbanes- Oxley and HIPAA become an open issue [10].

2.3.2. Legal issues

The legal issues arise because that the presence CSP resources in geographically conflicting various legal jurisdictions [11]. If the user is migrated to one geographical to other, an issue will occur because of different legal jurisdictions. For a movement data is distributed over a various data centers, those are owned by CSP those have different laws and security guidelines. This scenario may takes into the serious issue in cloud computing.

3. Literature Solutions

In this section, we explained the research work solutions and at the same time it also given the comprehensive discussion. Results presented in tables that make the reader understand easily The discussion can be made in several sub-chapters.

3.1 Data storage issues solutions

The SecCloud is presented by Wei et al. [12], it provides a storage security protocol for cloud customer's data and it not only secures the stored data but also provides security on computational data. The SecCloud protocol uses encryption for storing data in secure mode. The multiplicative groups and cyclic additive pairing is used for key generation for cloud customers, CSP, and other business partners or trusted third party. The encrypted data along with the verifiable signature is sent to cloud data center along with session key. The Diffie-Hellman algorithm is used for generation of session key for both bilinear groups. By receiving encrypted data the cloud decrypts the data, verifies the digital signature and stores the original data in specified location in cloud. The SecCloud verifies whether data is stored at specified location or not. The Merkle hash tree is used for computation security in SecCloud protocol. The verifying agency will verify the computational results that are building by using Merkle hash tree. The File Assured Deletion (FADE) protocol provides a key management with data integrity and privacy in [15].

The key management along with the data integrity and privacy are assured by File Assured Deletion protocol (FADE) proposed in [18].Because of FADE simplicity; it is a light weight protocol and uses both asymmetric and symmetric key encryption of data. The Shamir scheme protects symmetric and asymmetric keys to generous the trust in the key management. A group of key managers are used by FADE protocol, those acts as a trusted third party. The key k is used as encryption key for file F of the client and another key used for encryption of data key ($k.$). The policy file maintains the details that which files are accessible. So that, to upload data the user requests the key pair from the third party by sending policy file p. The key manager sends public and private keys to the user by using the policy file. The upload file encrypts with randomly generated k and k is encrypted with symmetric key. That encrypted file is decrypted with the public key of generated key pair and MAC is also generated for integrity check. The reverse process will be taken by the receiver to get back original data.

Liu et al.[15] proposed a scheme that has a time based re-encryption with ABE algorithm to support secure data

sharing among the group with access control. This scheme ensures that forwarded data safely reached to the group users and it maintains the user revocation. In this scheme, the time period is associated with every user and by expiration the revocation automatically by Cloud Service Provider (CSP). This time based encryption scheme allows users to share keys in prior with CSP and CSP generate re-encryption keys by taking request from user. The ABE protocol ensures an access control by examining the set of attributes rather than identity. This scheme ensures the privacy and availability of data among the group peoples but doesn't concentrate on data integrity.

The probabilistic sampling is used to reduce the computational redundancy instead of rebuilding the whole tree again. The below list are key recommendations by the Computer Security Alliances (CSA) [18] for the data security and effective key management. The scope of key should be maintained by group or individual. The standard encryption algorithms should be used and weak algorithms should discard.

The best guidelines for key management and encryption software products should be used, it is better to use legitimate software technology to ensure security on storage. The customer or organizations and/or trusted third party should maintain effective key management. If the improper auditing protocol is designed, encryption process may control the data flow to external parties during the auditing. But encryption itself does not prevent data flow to external parties but instead it can reduce it some minimal level. But it requires great range of key management process and overheads for key generation while storing data. But exposure of encryption key leads to data leakage and it still a problem in cloud environment. This problem is addressed by combining the homomorphic authenticator along with the random masking process [19]. Illustrated in the following Table 1.

Table 1. The Possible Solutions of Data storage issues

Authors	**Proposed Scheme**	**Services**	**Privacy**	**Integrity**	**Availability**	**Confidentiality**
L. Wei, H. Zhu[12]	SecCloud,for Securing cloud data	Encryption Bilinear pairing Signature verification Trusted third party	✓	✓	×	✓
Y. Tang, P.P. Lee, J.C.S. Lui[15]	FADE, a protocol for data privacy and integrity	Encryption Trusted third party Assured deletion Threshold secret sharing	✓	✓	×	✓
Q.Liu,G.Wang[16]	TimePRE, a scheme for secure data sharing in cloud	Proxy re-encryption Attribute based encryption	✓	×	×	✓
Z. Tari[17]	A methodology for security of resident data	Erasure correcting Code Data redundancy	×	✓	✓	✓

3.2 Identity management and Access control solutions

The authors proposed Simple Privacy preserving Identity Management for Cloud Environments (SPICE) in [20] for identity management systems. The SPICE ensures group signature for providing the unidentified authentication, access control, accountability, unlink ability, and user centric authorization. The SPICE provides above mentioned properties with only a single registration. After user registration with trusted third party they obtain unique credentials for all the services provided by CSP. By using the credentials, user generates authentication certificate. Different CSPs expecting variety attributes for authentication and user has to generate their required form of authentication certificate with same credentials.

The Role Based Multi-Tenancy Access Control (RB_MTAC) been proposed in [21]. The RB_MTAC merges the role based access control scheme along with identity management. This requires user registration with CSP and obtains single credential that should be unique. The user has to choose the password while registration with CSP portal. By using these credentials the user can enter into the cloud environment by passing through identity module that uniquely identifies the user and after that it will be redirected to role assignment module that establish a connection to the RB_MTAC database and assigns the roles to registered user based on enrolled information.

Dhungana et al. [22] proposed a scheme for the cloud networking infrastructure as identity management framework and it is maintained by User managed Access (UMA) protocol. Here CSP acts as a host, while the authorized used acts as service owner. The authorization manager handles the service management and service requesting users also managed by authorization manager. This scheme ensures the identity management and access control across multiple Cloud providers with the help of authorization management. Illustrated in the following Table 2.

Table 2. The Solutions of Identity management and Access control

Authors	Proposed Scheme	Services	Access control	Authentication	Identity management
S.M.S. Chow, et al.[23]	SPICE, identity management framework	Anonymous and delegatable Authentication Access control Accountability	✓	✓	×
Z.Yan,P. Zhang[24]	Role based access control scheme	Access control	✓	✓	×
R.D.Dhungana, A.Mohammad[22]	Identity management framework	Identity management Authentication Access control	✓	×	✓
S. Ruj, M. Stojmenovic[25]	Decentralized access control for cloud storage	Attribute based encryption Attribute based signature	×	✓	✓
Z. Wan, J. Liu[26]	HASBE	Access control for cloud Re-encryption Privacy	✓	✓	×

3.3 Contractual and legal Issue solutions

In cloud computing environment, the users have great benefits because of simplicity and poses great risk in case of violation of service level agreements. The authors in [27] proposed a scheme that reacts on Service Level Agreements (SLA) violations in order to reduce the security risks in cancellation / violation environment. This scheme concentrates on algorithm that performs renegotiation of risk awareness. The algorithm uses the scheme of [28] to determine a minimum risk service among levels of service to fulfill the users need. The algorithm performs the scrutinizes and renegotiation of services at runtime environment for the replacement or cancellation of services. Finally it updates the risk factors according to the SLA.

Table 3. The Possible Solutions for Contractual and legal Issues

Authors	Proposed Scheme	Services	Negotiation	Enforcement	Monitoring
M.L. Hale, R. Gamble[28]	SecAgreement	Embedding security parameters into SLA ws-agreement	✓	×	×
M. Rak, N. Suri[29]	SPECS, SLA-based	Embedding security Matchmaking	✓	✓	✓

Rak et al. [29] proposed a SPECS method that ensures architecture to provide a services termed as SLA-based security as a service. The proposed architecture mainly focused three aspects namely negotiation, enforcement, and monitoring. The SPEC recommends the enforcement activating factors by monitoring and reporting or system startup.

4. Conclusion

The cloud computing architecture stores data and application software with minimal management effort and provides on demand services to customers through internet. But with cloud management customer don't have trust worthy commitments or policies. This will lead to many security issues with data storage such as privacy, confidentiality, integrity and availability. In this study we focused on data storage security issues in cloud computing and we first provided service models of cloud, deployment models and variety of security issues in data storage in

cloud environment. In the final section, we addressed possible solutions for the data storage issues that provide privacy and confidentiality in cloud environment.

References

[1] A. Abbas, K. Bilal, L. Zhang, S.U. Khan, A cloud based health insurance plan recommendation system: a user centered approach, Future Gener. Comput. Syst. (2014)
[2] P. Mell, T. Grance, The NIST definition of cloud computing (draft), NIST Special Publ. 800 (145) (2011) 7.
[3] J. Che, Y. Duan, T. Zhang, J. Fan, Study on the security models and strategies of cloud computing, Proc. Eng. 23 (2011) 586–593.
[4] R. Chandramouli, M. Iorga, S. Chokhani, Cryptographic key management issues and challenges in cloud services, in: Secure Cloud Computing, Springer, New York, 2014, pp. 1–30.
[5] C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, Toward secure and dependable storage services in cloud computing, IEEE Trans. Services Comput. 5 (2)(2012) 220–232.
[6] M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, S. Loureiro, A security analysis of amazon's elastic compute cloud service, in: Proceedings of the 27th Annual ACM Symposium on Applied Computing, 2012, pp. 1427–1434.
[7] Duncan, Adrian, Sadie Creese, and Michael Goldsmith. "Insider attacks in cloud computing." Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012.
[8] Khorshed, Md Tanzim, ABM Shawkat Ali, and Saleh A. Wasimi. "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing." Future Generation computer systems 28.6 (2012): 833-851.
[9] A. Andrieux, K. Czajkowski, A. Dan, K. Keahey, H. Ludwig, T. Nakata, J. Pruyne, J. Rofrano, S. Tuecke, M. Xu, Web services agreement specification.
[10] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, A. Ghalsasi, Cloud computing the business perspective, Decis. Support Syst. 51 (1) (2011) 176–189.
[11] B. Hay, K. Nance, M. Bishop, Storm clouds rising: security challenges for IaaS cloud computing, in: 44th Hawaii International Conference on System Sciences (HICSS), IEEE, 2011, pp. 1–7.
[12] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A.V. Vasilakos, Security and privacy for storage and computation in cloud computing, Inform. Sci. 258 (2014) 371–386.
[13] O.D. Alowolodu, B.K. Alese, A.O. Adetunmbi, O.S. Adewale, O.S. Ogundele, Elliptic curve cryptography for securing cloud computing applications, Int. J.Comput. Appl. 66 (2013).
[14] M. Aslam, C. Gehrmann, M. Bjorkman, Security and trust preserving VM migrations in public clouds, in: IEEE 11th International Conference on Trust,Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 869–876.
[15] Y. Tang, P.P. Lee, J.C.S. Lui, R. Perlman, Secure overlay cloud storage with access control and assured deletion, IEEE Trans. Dependable Secure Comput.9 (6) (2012) 903–916.
[16] Q. Liu, G. Wang, J. Wu, Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Inform. Sci. 258 (2014) 355–370.
[17] Z. Tari, Security and privacy in cloud computing, IEEE Cloud Comput. 1 (1) (2014) 54–57.
[18] Cloud security alliance, security guidelines for critical areas of focus in cloud computing v3.0, 2011.
[19] Y. Fu, Z. Lin, Exterior: using a dual-vm based external shell for guest-os introspection, configuration, and recovery, in: Proceedings of the 9th ACMSIGPLAN/SIGOPS International Conference on Virtual Execution Environments, 2013, pp. 97–110.
[20] S.M.S. Chow, Y. He, L.C.K. Hui, S.M. Yiu, Spicesimple privacy-preserving identity-management for cloud environment, in: Applied Cryptography and Network Security, Springer, Berlin, Heidelberg, 2012, pp. 526–543.
[21] S. Yang, P. Lai, J. Lin, Design role-based multi-tenancy access control scheme for cloud services, in: IEEE International Symposium on Biometrics and Security Technologies (ISBAST), 2013, pp. 273–279.
[22] R.D. Dhungana, A. Mohammad, A. Sharma, I. Schoen, Identity management framework for cloud networking infrastructure, in: IEEE International Conference on Innovations in Information Technology (IIT), 2013, pp. 13–17.
[23] Boneh, Dan, and Matthew Franklin. "Identity-based encryption from the Weil pairing." SIAM Journal on Computing 32.3 (2003): 586-615.
[24] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for Internet of things, J. Netw. Comput. Appl. 42 (2014) 120–134.
[25] S. Ruj, M. Stojmenovic, A. Nayak, Decentralized access control with anonymous authentication of data stored in clouds, IEEE Trans. Parallel Distrib. Syst. 25 (2) (2014) 384–394
[26] Z. Wan, J. Liu, R.H. Deng, HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing, IEEE Trans. Inform. Forensics Sec. 7 (2) (2012) 743–754.
[27] M.L. Hale, R. Gamble, Risk propagation of security SLAs in the cloud, in: IEEE Globecom Workshops (GC Wkshps), 2012, pp. 730–735.
[28] M.L. Hale, R. Gamble, Secagreement: advancing security risk calculations in cloud services, in: IEEE Eighth World Congress on Services (SERVICES), 2012, pp. 133–140.
[29] M. Rak, N. Suri, J. Luna, D. Petcu, V. Casola, U. Villano, Security as a service using an SLA-based approach via SPECS, in: IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), vol. 2, 2013, pp. 1–6.
[30] Patel, Ahmed, et al. "An intrusion detection and prevention system in cloud computing: A systematic review." *Journal of Network and Computer Applications* 36.1 (2013): 25-41.
[31] Reddy, V. Krishna, B. Thirumala Rao, and L. S. S. Reddy. "Research issues in cloud computing." *Global Journal of Computer Science and Technology* 11.11 (2011).