2014 IEEE 6th International Conference on Cloud Computing Technology and Science

Security Challenges in Cloud Storage

F. Yahya[1], V. Chang[2], R.J. Walters[1], and G.B. Wills[1]

1. Electronics and Computer Science, University of Southampton, Southampton, UK
2. Computing and Creative Technologies, Leeds Metropolitan University, Leeds, UK

***Abstract*— As cloud becomes the tool of choice for more data storage services, the number of service providers has also increased. With these choices, organisations have a wide selection of services available to move their data to the cloud. However, the responsibility to maintain the security of sensitive data stored therein remains paramount. This paper will discuss some of the challenges of securing a cloud storage and putting it into context by reviewing relevant literature. The challenges associated with the three important security aspects (confidentiality, integrity and availability) are discussed together with the vulnerabilities linked to them. It is important to look into these challenges as cloud storage is not only about technological evolution but involves security considerations. We aim to provide insights of security challenges and its solutions to enhance cloud storage implementation.**

***Keywords*—Cloud storage, Cloud storage provider, Security**

I. Introduction

DISK storage is an essential computer component to retain data. Well-known as being the leading expenditure in any IT projects, the growth is projected to rise annually in most organisations. Therefore, more and more users and organisations have moved their data to the cloud to save cost, utilise resources and have worldwide access [1][2].

A cloud storage concept comes simultaneously with the rise of cloud computing. It has the facility to store data on the cloud, available anytime and anywhere at lower cost. In other words, it is the storage component of cloud computing. Yet, sharing the cloud with other users possess risks and concerns over security. Users raised concerns whether their data are accessed by unauthorised person since there are many user sharing the resources over the cloud. This has also been supported by the Cloud Security Alliance (CSA) in their statistical overview of vulnerabilities. It has been reported by CSA [3] that the major concerns on security issues are confidentiality, integrity and availability.

According to their report, the highest incident occurred from threats of insecure Application Programming Interface/s (APIs), followed closely by data loss and leakage and thirdly, hardware failure from twelve threats defined by CSA. In short, this paper discusses some security challenges in cloud storage and putting it into context by reviewing relevant literature.

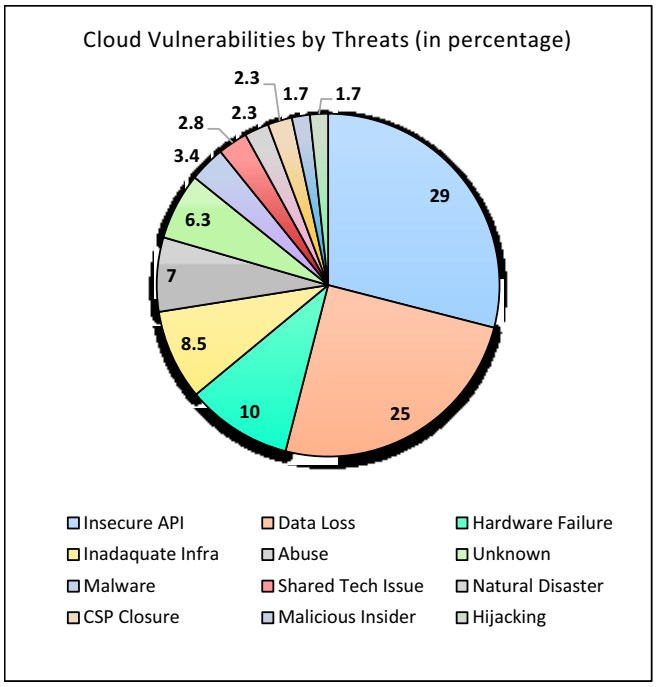

Figure 1 Cloud Vulnerabilities Incidents by Threats [3]

II. General Architecture

Cloud storage architectures are mainly about delivering storage on demand in a highly scalable and multi-tenant way. Basically, cloud storage architectures contain of a front end that exports an API to communicate with the backend storage.

In traditional storage systems, this API is the SCSI protocol; nonetheless in the cloud, these are evolving protocols. At this layer, there are Web service, file-based Internet SCSI or iSCSI front ends. This layer is the first communication point between the user and the service provider. Users access the services using their credentials. The midpoint component is a layer called storage controller that interconnects and communicates from the front API to the backend storages. This layer has a variety of features such as replication, traditional data-placement algorithms with geographical location. Finally, the back-end consist of physical storage for data. This may be a central protocol that runs dedicated programs or a traditional

F. Y. is with Electronics & Computer Science, University of Southampton, SO17 1BJ, United Kingdom (e-mail: fara.yahya@soton.ac.uk).

V. C. is with Computing and Creative Technologies, Leeds Metropolitan University, LS6 3QR, United Kingdom (email: v.i.chang@leedsmet.ac.uk).

R. J. W. is with Electronics & Computer Science, University of Southampton, SO17 1BJ, United Kingdom (e-mail: rjw1@ecs.soton.ac.uk).

G. B. W. is with Electronics & Computer Science, University of Southampton, SO17 1BJ, United Kingdom (e-mail: gbw@ecs.soton.ac.uk).

978-1-4799-4093-6/14 $31.00 © 2014 IEEE
DOI 10.1109/CloudCom.2014.171

back-end to the physical disks.

There are mainly three types of cloud storage; public, private and hybrid cloud storage. Public cloud storage is usually built for large-scale users and has shared resource infrastructure. A private cloud that is also known as an internal cloud storage serves a specific group of users. Unlike the public cloud storage, private cloud storage resides in a controlled

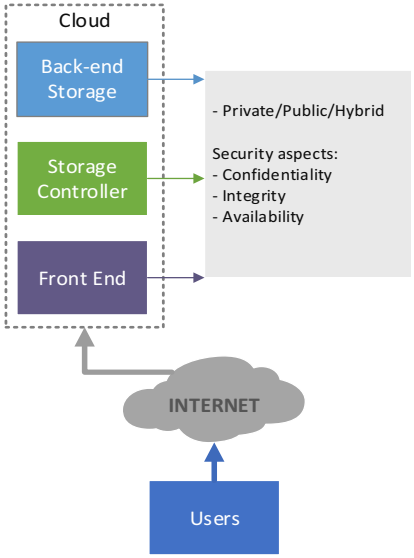

Figure 2 Generic cloud storage architecture

environment to meet safety and performance requirements. The final type is the hybrid cloud storage that is a combination of both public and private cloud storage.

The underlying reason for this segregation of cloud storage types is the fact that it serves a focused group of users. The biggest issue is security. Users are unlikely to entrust their data to a third party company without having a guarantee that they are able to access their data whenever they want and no one else is able to access it at all. This explains clearly why there are different deployment models in adopting cloud services.

III. SECURITY CHALLENGES

Cloud storage is a service that includes inherent vulnerabilities, but these have never disuaded users from taking advantage of its economies and flexibilities. With adoption of a cloud model, users lose control over physical security. In fact in a public cloud storage, users are sharing the computing resources with other users. Security overall covers mainly three aspects: confidentiality, integrity and availability (CIA). These aspects are the topmost considerations in designing a security measure to ensure maximum protection. This is reflected with the vulnerabilities incidents results from CSA as the figure 3. In short, confidentiality involves protecting data and information from disclosure to unauthorised person. Integrity refers to protecting data and information from being modified by unauthorised person. On the other hand, availability is ensuring the authorised people are able to access and use the data and information whenever required. In this paper, the challenges are

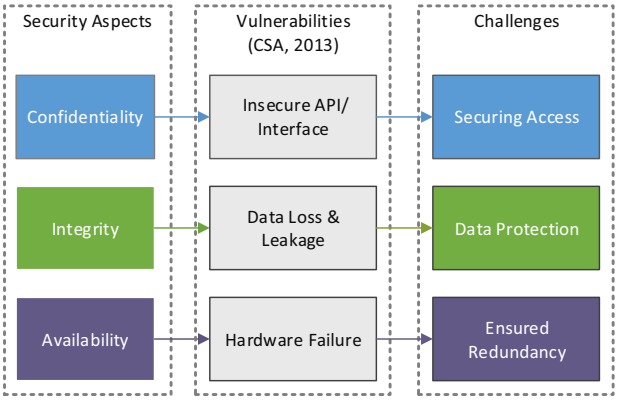

Figure 3 Cloud Storage Security Aspects, Vulnerabilities & Challenges

derived from the known vulnerabilities. Securing access to protected data and information is restricted to certain level of user authorised to access it. This requires mechanisms to be in place to control the access of protected data. The sophistication of the access control mechanisms should be in parity with the value of the information being protected; the more sensitive or valuable the information the stronger the control mechanisms need to be. The foundation on which access control mechanisms are built starts with authentication, authorisation and encryption. Secondly, protecting data from loss and leakage involves integrity of many parties involved in providing the resources. Some schemes and mechanism are needed to ensure the data and information kept on the cloud is unaltered or removed. It is suggested to practice auditing techniques such as proof-of-retrivebility and proof-of-data possession to enable verification. Subsequently, as access and data are getting secured, it is important to keep the hardware high-available. The hardware is the infrastructure hosting the services to store data and information. Without ensuring failover, the services are unable to meet the uptime and comply with service level managements. Discussions of each security challenge and related previous research is described below.

A. Securing Access

Data confidentiality remains one of the main concerns and the major barrier to the development of cloud services. It is vulnerable to conventional threats (injection attacks, cross-site scripting etc.) [4] but also to specific cloud computing threats (hypervisor flaws, management of the security perimeter within an organisation and confidence in the provider) [5].

Among the obvious dissimilarities between cloud storage and traditional storage is the way it is accessed as shown in figure 4. Web service APIs are the common ones although most providers have multiple access methods. These web service APIs are designed according to Representational State Transfer (REST) principles, which imply an object-based scheme running on top of HTTP i.e., using HTTP as a transport. REST APIs are stateless, thus making them simple to apply. Some cloud storage providers use REST APIs, mostly Amazon Simple Storage Service (Amazon S3) and Windows Azure™

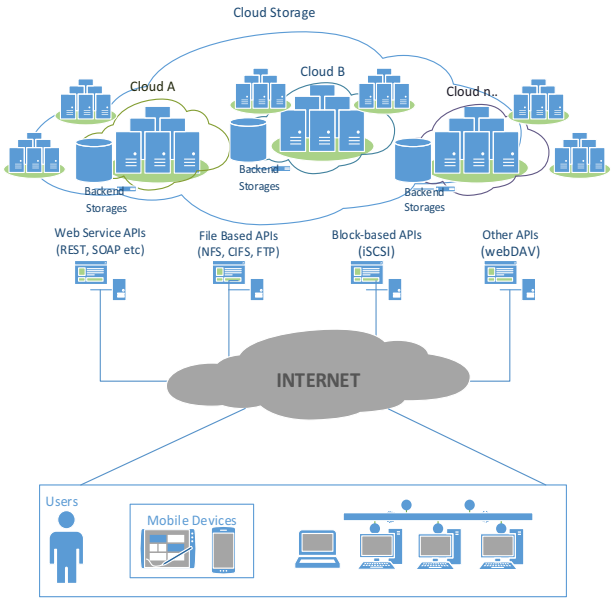

Figure 4 Cloud Storage Access Method

[6]. There is a major downfall of Web service APIs that is the requirement to do integration when being used with cloud storage. Consequently, other types of access methods are also implemented with cloud storage to fulfil instant integration requirement such as file-based protocol (NFS/CIFS, FTP or iSCSI). Cloud storage providers such as Six Degrees provide these types of access methods [6].

Though the protocols mentioned above are the most common, there are other protocols suitable for cloud storage. Web-based Distributed Authoring and Versioning (WebDAV) is an interesting protocol that is created on HTTP and allows the Web to be a readable and writable source. Prevalent providers of WebDAV include Zetta and Cleversafe [7]. Some solutions have also supported multi-protocol access for example, a cloud storage that enables both file-based (NFS and CIFS) and SAN-based protocols from the same storage-virtualization infrastructure.

Access security measures are generally considered in three steps: Identification & Authentication, Authorisation and Encryption.

1) Identification and Authentication

Password security heavily depends on creating strong passwords and protecting them from getting stolen. Researchers have established that strong passwords are necessarily long, random and hard to crack but often difficult to remember. Bang *et al*. suggests that security is not just a technical issue but also a behavioural issue involving users, mostly untrained ones [8]. It was also presented that humans have limited memory capacity therefore the use of long random passwords is almost impossible. In their study, a new vulnerability measure from a network perspective is suggested that captures the structural characteristics of the Identification–Password (ID-PW) usage network. Public awareness and support from the country's government is said to be the backbone in ensuring overall security. On the other hand, Zhao *et al*. built a Cloud-based storage free BPM designed to achieve a high level of security with desired CIA [9]. The password manager is integrated with web browsers but this technique possesses risks of keystroke logger if the user log-in from an anti-malware program. Generation of password structure at highest probabilistic order to make password-cracking harder using the right word-mangling rule [10] is said to be able to assist users in selecting their own memorable password even though it is argued that as long users are able to choose their own passwords, the attacks can break password more easily than through a brute-force attack. A password strength evaluation of password-guessing algorithm results in effectiveness of a dictionary-check that depends heavily on the choice of dictionary. There is a strong relationship of both password-composition policies and metrics for quantifying password security [11].

2) Authorisation

An authorisation process ensures that a person has the right to assess a certain resources and limits of the access unknowing of other user's information. Users may have access but have a specific role or authority to do something within their scope. A privacy protecting authorisation infrastructure that provides a web service interface for cloud providers to use and application developers may then use this to further develop privacy preserving applications. The authorisation infrastructure does not obviate the need for trust but rather is built on the assumption that cloud providers can be trusted to the extent that they wish to provide an automated infrastructure that can easily enforce each other's policies reliably and automatically [12].

A paper suggested an authorisation model suitable for cloud services that supports hierarchical role-based access control (RBAC), path-based object hierarchies and federation [13] in multi-tenancy environment. These features provide a convenient authorisation service for cloud, especially those using path-based patterns such as REST APIs.

Although authorisation usually supports high scalability, it is believed to improve scalability and this would hopefully enable more fine-grained control on the authorisation information.

3) Encryption

It is a standard approach to apply encryption techniques into sensitive data to secure it. Encryption has always been seen as the ultimate security measure but it also comes with a set of difficulties. Traditional encryption is done by transferring the data files locally and decrypting it. Today, encryption is done in many ways. Table 1 shows the review of encryption methods and approaches. Previous literature shows [14] extensive research on encoding and decoding information in order to guarantee privacy.

A cryptographic cloud storage system called CS2 was amongst early research done on applying symmetric encryption techniques that ensures confidentiality, integrity and verifiability without being resource hungry [15]. Recently, a Cloud storage encryption (CSE) framework was proposed also

using a symmetric, searchable encryption with policy and access methods [14].

An Attribute-based encryption (ABE) with verification and recovery technique was proposed to effectively secure the data and provide recovery mechanism [16]. A different paper suggested ABE encryption was an efficient data retrieval scheme best suited for cloud storage systems with massive amount of data [17].

Table 1 Review of Encryption Methods and Approaches

Encryption methods	Approach		Limitation
Symmetric cryptography (Private-key)	Searchable symmetric encryption [15] [14]		The key used to encrypt and decrypt data must remain secure because anyone with access to it can read the coded messages.
Asymmetric cryptography (Public key)	Attribute-based Encryption (ABE)	Attribute-based Encryption (ABE) [16]	Encryption are more complex compared to symmetric encryption and takes longer to encrypt and decrypt. Needs verification of the public key authenticity.
		Searchable ABE [17]	
		Cipher text-policy Attribute-based Encryption (CP-ABE) [18]	
		Hierarchical Identity-Based Encryption and Key-Policy Attribute-Based Encryption [19]	

A fine-grained and cryptographic access control for cloud storage services called CS-CACS uses CP-ABE which is implemented based on the Hadoop Distributed File System (HDFS) environment [18] to efficiently secure user data. An approach was introduced [19] using user-centric privacy preserving cryptographic access control protocol, K2C (Key To Cloud) that enables end-users to store and share sensitive data securely in untrusted cloud storage for hierarchically organised data. It uses two cryptographic libraries, Hierarchical Identity-Based Encryption and Key-Policy Attribute-Based Encryption.

B. Data Protection

Cloud storage that holds data and information on the cloud is obligated on data integrity. Data integrity depends on the assurance pursued by the user that data are unaltered on the provider infrastructure. Data integrity threats involve both malicious third party occurrences and hosting infrastructure weaknesses.

This issue is well studied in the literature with the introduction of Proof-of-Retrievability (POR) and Proof-of-Data Possession (PDP) protocols [20][21]. These techniques allow detecting data integrity damages without requiring a copy of the user local data. The idea was to encode the protocol with the data before storing it.

Some improved versions were developed to make it compact [22] and high-available, HAIL [23]. Nevertheless, these techniques involve pre-processing the data before storing it externally to the provider. With the aim of making it more dynamic, new approaches were introduced using algebraic signatures and making it more flexible [24], [25].

There has also been research that looks into auditing the security of cloud storage. A publicly auditable cloud data storage (TPA) suggested that an interface layer can help user assess risks [26, 27, 28].

Another issue was also raised as users found that even if they accidentally deleted their data, the provider can restore a backup file. This means the data is still kept by the provider. In FADE [29], a secure overlay with file assured deletion is presented. It is a policy-based scheme that reliably removes files and withdraw file-access policies on it. Thus, even if a data is restored by a provider, the file is restricted from read/write as the file-access policies are revoked.

On the other hand, accountability is known as one of the preventive controls to protect data privacy in the cloud. It enhance trusts and manage risks. A research done by Pearson *et al.* [30] provides a solution called A4Cloud that ensure trusts are not breached. It supports CSPs by enabling techniques such as audited policy enforcement, assessment of possible policy violations effects, violations detection and incidents management.

C. Ensured Redundancy

Data availability is critical. Cloud storage providers must guarantee that the data will always be available autonomously regardless of hardware failures, corrupted physical disks or downtime. Hardware failures can happen at any time. This includes failures caused by environmental failures such as a natural disaster, flood or even fire.

A hardware design should be built on a basis of having redundancy and a minimum single points of failure. At the design phase, the analyst creates a physical hardware map that shows all the connection points for server, storage, network and software. CloudSim was introduced for modelling Cloud environments and performance testing application services. Among components that can be modelled are virtualization (VMs), clustered configurations, multi data centres points (used for disaster recovery centres) and backups which are known to have high-availability and fault-tolerance [31].

Calder *et al*. presented the case of a cloud storage provider, Windows Azure (WAS) on the combination of strong consistency, global partitioned namespace and disaster recovery has been the important features in ensuring availability of the multi-tenancy environment [32]. This has reduced the storage cost significantly than the cost of running all workloads on a dedicated hardware. Therefore, it is said that having redundant resources is essential to prevent downtime from happening in cloud environments.

Table 2 Evaluation of Existing Approaches

Approach		Password	Policy	Access control	Federation	Encryption	Verification	Recovery	Auditing	Compact	High Available	Dynamic	Fault Tolerant
Secured Access	[8]	√											
	[9]	√											
	[10]	√											
	[11]	√	√										
	[12]		√	√									
	[13]		√	√	√								
	[14]		√			√							
	[15]					√	√					√	
	[16]					√	√	√					
	[17]					√		√					
	[18]			√		√		√					
	[19]			√		√							
Data Protection	[20]					√			√				
	[21]					√			√				
	[22]									√			
	[23]										√		
	[24]											√	
	[25]											√	
	[26]								√				
	[27]								√				
	[28]								√				
	[29]		√						√				
	[30]		√						√				
Ensured Redundancy	[31]							√			√		√
	[32]							√					

IV. CONCLUSION

The cloud is a multi-tenant environment, where resources are shared. Threats can happen from anywhere; inside the shared environment or from outside of it. However, placing sensitive data in a shared cloud storage is apparently risky. Whether accidental or due to a malicious hacker attack, data privacy, loss or leakage and unavailable for access would be a major security violation involving confidentiality, integrity and availability. The best strategy is to practice all security measures such as access control, encryption, auditing and redundancy to ensure the data are protected from every angle and gaining overall security.

We have presented a review of challenges in enhancing cloud storage security. As shown in Table 2, the evaluation of existing approaches covers many aspects of security measures such as password protection, policy enforcement, access control etc. Recent advances on security measures indicate security is a continuously interesting aspect in the cloud. Each security challenges are discussed specifically in section III with its recent advances. These advances can be used as a reference in exploring new security researches in cloud storage.

This paper provides a brief explanation on cloud storage. Mainly, it describes the security challenges together with the recent advances for each challenges. This is done by reviewing previous literature and putting it into context. We are also looking into emerging approaches and technologies that may be potentially continued and improved for future research. Therefore, in our next stage of research, a thorough work will be introduced. An overview of future work is described in the last section.

V. FUTURE WORK

In this research, a comprehensive framework focusing on the integrated security layers of a cloud storage architecture is being evaluated. This framework is aimed to be more dynamic and localised in nature and intended to emphasis on security methodology that varies dynamically from many layers. The framework will also focus on providing security on demand to the cloud storage and its security measure depends on the value of data stored by the user.

One size may not necessarily fit all. There are diverse systems and varied resources in the cloud, a single security framework would be excessively rigid for certain applications and if there is less security, vulnerability threats are apparent for some applications like financial applications. On the other hand, if the cloud has a common security methodology in place, it will be easily targeted for hackers because such threats makes the whole cloud vulnerable to attacks.

Therefore, in such a scenario, if customised security is designed, it would make sense. Though there are many practical concerns regarding to dynamic security the future work is much concentrated to derive a framework which targets these concepts and provide a practical solution for cloud storage.

ACKNOWLEDGMENT

We acknowledge the award of Malaysian Public Service Department Training (HLP) scholarship to Fara Yahya allowing the research to be undertaken. We would like to thank the anonymous reviewers for their valuable comments.

REFERENCES

[1] J. JU, J. WU, J. FU, and Z. LIN, "A Survey on Cloud Storage," *Journal of Computers*, vol. 6. 2011.

[2] J. Wu, L. Ping, X. Ge, W. Ya, and J. Fu, "Cloud storage as the infrastructure of Cloud Computing," in *Proceedings - 2010 International Conference on Intelligent Computing and Cognitive Informatics, ICICCI 2010*, 2010, pp. 380–383.

[3] CSA, "Cloud Computing Vulnerability Incidents : A Statistical Overview," 2013.

[4] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, Jan. 2011.

[5] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, Mar. 2012.

[6] M. T. Jones, "Anatomy of a cloud storage infrastructure Models , features , and internals," no. November, pp. 1–11, 2010.

[7] V. S. Suntharam, K. V Reddy, and N. Puspalatha, "Data Storage Security in Cloud Computing and Verification of Metadata by Encryption," *Int. J. Comput. Sci. Electron. Eng.*, vol. 2, no. 3, 2013.

[8] Y. Bang, D.-J. Lee, Y.-S. Bae, and J.-H. Ahn, "Improving information security management: An analysis of ID–password usage and a new login vulnerability measure," *Int. J. Inf. Manage.*, vol. 32, no. 5, pp. 409–418, Oct. 2012.

[9] R. Zhao and C. Yue, "Toward a secure and usable cloud-based password manager for web browsers," *Comput. Secur.*, vol. 46, pp. 32–47, Oct. 2014.

[10] M. Weir, S. Aggarwal, B. De Medeiros, and B. Glodek, "Password cracking using probabilistic context-free grammars," in *Proceedings - IEEE Symposium on Security and Privacy*, 2009, pp. 391–405.

[11] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. López, "Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms," in *Proceedings - IEEE Symposium on Security and Privacy*, 2012, pp. 523–537.

[12] D. W. Chadwick and K. Fatema, "A privacy preserving authorisation system for the cloud," in *Journal of Computer and System Sciences*, 2012, vol. 78, pp. 1359–1373.

[13] J. M. A. Calero, N. Edwards, J. Kirschnik, L. Wilcock, and M. Wray, "Toward a Multi-Tenancy Authorization System for Cloud Services," no. December, 2010.

[14] H. M. Al-sabri and S. M. Al-saleem, "Building a Cloud Storage Encryption (CSE) Architecture for Enhancing Cloud Security," vol. 10, no. 2, pp. 259–266, 2013.

[15] S. Kamara, C. Papamanthou, and T. Roeder, "CS2 : A Searchable Cryptographic Cloud Storage System," pp. 1–25, 2011.

[16] R. V Agalya and K. K. Lekshmi, "A Verifiable Cloud Storage using Attribute Based Encryption and Outsourced Decryption with Recoverability," vol. 3, no. 10, 2014.

[17] D. Koo, J. Hur, and H. Yoon, "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage," *Comput. Electr. Eng.*, vol. 39, no. 1, pp. 34–46, Jan. 2013.

[18] R. Zhang and P. Chen, "A dynamic cryptographic access control scheme in cloud storage services," in *Proceedings - 2012 8th International Conference on Computing and Networking Technology (INC, ICCIS and ICMIC), ICCNT 2012*, 2012, pp. 50–55.

[19] S. Zarandioon, D. Yao, and V. Ganapathy, "K2C: Cryptographic cloud storage with lazy revocation and anonymous access," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, 2012, vol. 96 LNICST, pp. 59–76.

[20] A. Juels and B. S. K. Jr, "PORs : Proofs of Retrievability for Large Files," *CCS '07, Alexandra, Virginia, USA*, pp. 584–597, 2007.

[21] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," *Proc. 14th ACM Conf. Comput. Commun. Secur. - CCS '07*, no. 1, p. 598, 2007.

[22] H. Shacham, "Compact Proofs of Retrievability," *Adv. Cryptology-ASIACRYPT 2008, Springer Berlin Heidelberg.*, pp. 90–107, 2006.

[23] K. D. Bowers, A. Juels, and A. Oprea, "HAIL : A High-Availability and Integrity Layer for Cloud Storage," in *CCS*, 2009, vol. 489, pp. 187–198.

[24] L. Chen, "Using algebraic signatures to check data possession in cloud storage," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1709–1715, Sep. 2013.

[25] Y. Yu, J. Ni, M. H. Au, H. Liu, H. Wang, and C. Xu, "Improved security of a dynamic remote data possession checking protocol for cloud storage," *Expert Syst. Appl.*, vol. 41, no. 17, pp. 7789–7796, Dec. 2014.

[26] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, pp. 847–859, 2011.

[27] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic audit services for integrity verification of outsourced storages in clouds," *Proc. 2011 ACM Symp. Appl. Comput. - SAC '11*, p. 1550, 2011.

[28] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing," *Inf. Sci. (Ny).*, vol. 258, pp. 371–386, Feb. 2014.

[29] Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, "Secure overlay cloud storage with access control and assured deletion," *IEEE Trans. Dependable Secur. Comput.*, vol. 9, pp. 903–916, 2012.

[30] S. Pearson, V. Tountopoulos, D. Catteddu, M. Sudholt, R. Molva, C. Reich, S. Fischer-Hubner, C. Millard, V. Lotz, M. G. Jaatun, R. Leenes, C. Rong, and J. Lopez, "Accountability for cloud and other future Internet services," *4th IEEE Int. Conf. Cloud Comput. Technol. Sci. Proc.*, pp. 629–632, Dec. 2012.

[31] R. N. Calheiros, R. Ranjan, A. Beloglazov, and A. F. De Rose, "CloudSim : a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," no. August 2010, pp. 23–50, 2011.

[32] B. Calder, J. Wang, A. Ogus, N. Nilakantan, A. Skjolsvold, S. Mckelvie, Y. Xu, S. Srivastav, J. Wu, H. Simitci, J. Haridas, C. Uddaraju, H. Khatri, A. Edwards, V. Bedekar, S. Mainali, R. Abbasi, A. Agarwal, M. Fahim, M. Ikram, D. Bhardwaj, S. Dayanand, A. Adusumilli, M. Mcnett, S. Sankaran, K. Manivannan, and L. Rigas, "Windows Azure Storage : A Highly Available Cloud Storage Service with Strong Consistency," *SOSP*, vol. 20, pp. 143–157, 2011.