# An Investigation on the Issues in Cloud Data Security

A. Mercy Gnana Rani,
Department of Information Technology, Dr. SNS Rajalakshmi College of Arts and Science (Autonomous)
Coimbatore-641 049, Tamil Nadu, India

A. Marimuthu, Ph.D
Department of Computer Science, Government Arts College (Autonomous)
Coimbatore-641 018, Tamil Nadu, India

## ABSTRACT
Cloud computing is one of the most fascinating technologies which attract the users to outsource their data from local to remote cloud servers using Internet. A large number of cryptographic schemes are available to encrypt the sensitive information and to protect data. Even though it protects the data but it limits the functionality of the cloud storage. This paper focuses on investigation of cloud data security and its issues. Cloud Computing is one of the most influential technology in the IT industry in recent years. In Cloud, the computing infrastructures (Hardware and Software) are provided as services over the internet in pay-as-you-use basis. The outsourced sensitive data an cloud servers are not within the same domain. For securing these sensitive user data in cloud server, at present many cryptographic solutions are available. However, these solutions have computation overhead, key distribution and data management for providing security and scalability in data access control of cloud computing. This paper presents the analysis on various cloud data security issues available.

## Keywords
Cloud Computing, Outsourcing data, Encryption

## 1. INTRODUCTION
Cloud computing is one of the most important next generation distributed computing systems which provides a services such as on-demand self service, pay-per-use service etc. The most important factors that attracts the business organizations to the cloud computing is reduction of hardware expenditure. Although the advantages of cloud computing attracts the organization, still it has lot of security problems [1].

The National Institute of Standard and Technology (NIST) define the following characteristics of the cloud computing [2, 3]

1. On demand self service: A consumer can unilaterally provision computing abilities.
2. Broad network access: Capabilities are accessed through the standard approaches and it facilitates the service by using the heterogeneous client platforms.
3. Resource polling: The organized resources are mainly used to serve the consumer by either assigned or reassigned resource dynamically based on their needs.
4. Rapid Elasticity: Abilities can be quickly and elastically provisioned automatically, in certain scenarios, to speedily scale out and rapidly released to quickly scale in [3].
5. Measured Service: Cloud systems automatically handle and optimize resource use via leveraging a metering capability at some level of abstraction appropriate to the nature of service.

In cloud computing, outsourcing is the one of the important services because it has the following characteristics such as rapid resource elasticity, usage based pricing, location independent resource pooling. Microsoft's Azure storage and Amazon's S3 are the best examples of cloud computing service providers. The data security is the important because of the rapid growth in the cloud computing [4].

The major benefits of the cloud computing are that it reduces cost and capital expenditures, increased operational efficiencies, scalability, flexibility, immediate time to market and so on. Cloud computing has three important service models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS). Commercial cloud computing systems are built at different levels. Table I shows the service models in cloud computing.

**Table 1.**

| IaaS | PaaS | SaaS |
|---|---|---|
| Amazon's Ec2 [2] | Google App Engine [5] | Google's Apps [6] |
| Amazon's S3 [3] | Yahoo Pig | Salesforce's |
| IBM's Blue Cloud [4] | | Customer Relation Management System |

With advanced growth and development of cloud computing, security implications of moving services or infrastructure to the cloud need serious consideration. Small and medium enterprises in general cannot afford to devote resources to address security issues can benefit from the security solution applied by cloud providers. In order that the cloud is well accepted by organizations, security concerns of both data owners and end users need to be taken into consideration. Moving into the cloud exposes both challenges and opportunities. Although the clouds centralized data model makes it suitable to monitor access to data, it also exposes the risk of a comprehensive data theft [5]. Further, organizations have to trust a third party vendor with their applications and data. This loss of control over data conventionally maintained in-house, introduces certain new security management challenges. Moreover, the notion of unlimited resources in the cloud is possible through resource sharing. This multitenant environment of the cloud in which the tenants share resources results in new privacy concerns as the conventional network firewalls and secure socket layers cannot be a security shield in the cloud [6]. In the cloud, a business's data is typically stored on a virtual machine, which is most likely running on a server with other virtual machines some of which could be malicious. Moreover, cloud data is accessed via the Internet, which guarantees security only to a certain level [6].

Due to the importance of the cloud computing environment in the present decade, a number of research works have been carried out in the field to improve the overall performance [7]. With the increase of on-demand application usage, the potential of cyber attacks also increases. Individual users have to frequently provide online information about their identification, and these could be used by attackers for identity theft. In order to maintain various security and privacy issues like: confidentiality, operational integrity, disaster recovery and identity management,

following schemes should be deployed at least to ensure data security [8] to some extent like:

- An encryption approach to assure data security in a highly interfering environment maintaining security standards against popular threats and data storage security.
- The Service Providers should be given limited access to the data.
- Stringent access controls to prevent unauthorized and illegal access to the servers controlling the network.
- Data backup and redundant data storage to make data retrieval easy due to any type of loss unlike the recent breakdown issues with the Amazon cloud.
- Distributed identity management and user security is to be maintained by using either Lightweight Directory Access Protocol (LDAP), or published APIs (Application Programming Interfaces) to connect into identity systems [6].
- An essential characteristic feature of cloud computing is that it becomes an essential element in many organizations from the viewpoint of data security. This is mainly due to the fact that, the conventional techniques cannot be adopted as these have become quite outdated with respect to the ever evolving security threats and also to avoid data loss in a cloud computing environment. The second issue is that the data stored in the cloud is accessed a large number of times and is often subject to different types of changes [6].

# 2. LITERATURE SURVEY

## 2.1 Secure and dependable storage services in Cloud Computing (2011)

Cloud services also give up user's physical control of their outsourced data, which unavoidably poses new security threat towards the suitability of the data in cloud. This technique presented a distributed storage integrity auditing approach, which uses the homomorphism token and distributed erasure coded data [9]. This approach facilitates consumers to audit the cloud storage with very lightweight communication and computation cost. The auditing result guarantees both strong cloud storage correctness and achieves fast data error localization i.e., the detection of misbehaving server. The author showed that it has lightweight communication and computation cost.

## 2.2 Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing(2011)

This work facilitates the integrity of data storage in Cloud Computing. Specifically, the main purpose of Third Party Auditor (TPA) is to authenticate the integrity of the dynamic data stored in the cloud behalf of cloud clients. TPA removes the association of the client through auditing of whether his data stored in the cloud are indeed intact, which intern attains economies for Cloud Computing. This work investigated the issue of providing simultaneous public audit capability and data dynamics for remote data integrity check in Cloud Computing. The construction is purposefully developed to meet these two essential goals while attaining high efficiency [10]. For supporting efficient handling of multiple auditing works, the technique of bilinear aggregate signature is further investigated to extend main result into a multiuser setting. Performance analysis and extensive security shows that the proposed scheme is highly secure and efficient.

## 2.3 A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability(2011)

In this paper, a new remote data integrity checking protocol for cloud storage is proposed. The proposed protocol is suitable for offering integrity protection of customers' essential data. The proposed protocol supports data insertion, modification and deletion at the block level, and also supports public verifiability [11]. The proposed protocol is proved to be secure against an untrusted server. It is also private against third party verifiers. The experimental results illustrated that the proposed protocol has very good significance in communication, computation and storage costs.

## 2.4 A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding(2012)

A cloud storage system is considered here with storage servers and key servers. A threshold proxy re-encryption technique is introduced by the author to removal of codes above exponents. The threshold proxy re-encryption assistance with various processes like encoding, forwarding and fractional decryption functions in a distributed way. To decrypt a message of k blocks that are encrypted and encoded to n codeword symbols, each key server only has to partially decrypt two codeword symbols in the system [12]. The presented approach present a secure cloud storage system that gives secure data storage and secure data forwarding operation in a decentralized structure. Furthermore, every storage server independently done encoding and re-encryption and each key server separately carry out partial decryption. The storage servers take action as storage nodes in a satisfied addressable storage system for storing comfortable addressable blocks. At the same time as the key servers act as access nodes for giving a front-end layer such as a conventional file system interface.

## 2.5 Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing(2010)

The paper deals with the services for data security and access control when users share sensitive data on cloud for sharing. The issue is handled by defining and enforcing access policies through data attributes and facilitating the data owner to allocate most of the computation works involved in fine grained data access control to entrusted cloud servers without disclosing the underlying data contents [13]. The paper presents an approach to attain this goal by utilizing KPABE and uniquely integrating it with approaches of proxy re-encryption and lazy re-encryption. Moreover, this approach can facilitate the data owner to allot most of computation overhead to powerful cloud servers. Privacy of user access privilege and user secret key accountability can be achieved. The simulation proof shows that the approach is secure under standard cryptographic models.

## 2.6 Cloud Security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks

The most serious threats to cloud computing is through HTTP Denial of Service or XML-Based Denial of Service attacks. In this paper, recreate some of the present attacks that attackers may start as HTTP and XML. The HTTP-DoS (H-DoS) attack is potentially lethal to cloud computing as it depends on HTTP to communicate with itself and other cloud systems. This paper explains that how such an attack can take place through the same scenario that brought down the pro-Iranian websites and how it can be done within a cloud or outside of the cloud system [14].

Moreover, another attack called Xml-Based Denial of Service (X-DoS), which is another lethal attack aimed at the services the cloud provides. In order to defend next to such attacks, brought forward the SOTA model and implemented it on a cloud system, which is called a Cloud TraceBack (CTB). The CTB demonstrated that it can be used in an actual X-DoS attack so the cloud victim could trace the attack back to the source.

## 2.7 Collaboration-Based Cloud Computing Security Management Framework

Though the cloud computing formulation is a capable internet-based computing platform, it results in a loss of security control over the cloud-hosted assets. It is because of the outsourcing of enterprise IT assets hosted on third-party cloud computing platforms. In addition, the lack of security constraints in the Service Level Agreements between the cloud providers and consumers results in a loss of trust as well. Attaining a security certificate such as ISO 27000 or NIST-FISMA would help cloud providers improve consumers trust in their cloud platforms' security. Still, such standards are still far from covering the full complexity of the cloud computing model [15]. A collaboration-based security management framework is introduced for the cloud computing formulation. This model introduces an alignment of the NISTFISMA standard to fit with the cloud computing model. The proposed model is formulated by using it to model and secure a multitenant SaaS application with two different tenants. It can be used by cloud providers to manage their cloud platforms, by cloud consumers to manage their cloud hosted assets, and as a security-as-a-service to help cloud consumers in outsourcing their internal SMP to the cloud.

## 2.8 The Security of Cloud Computing System enabled by Trusted Computing Technology

Cloud computing facilitates sharing distributed resources and services that belong to different organizations. Since, cloud computing share distributed resources through the network in the open environment; it would lead to various security problems to develop the cloud computing application. Advantages of the proposed approach are to extend the trusted computing technology into the cloud computing environment to attain the trusted computing needs for the cloud computing and then fulfill the trusted cloud computing [16]. Transfer Control Protocol (TCP) is used as the hardware base for the cloud computing system. The TCP offers cloud computing system certain essential security functions, such as authentication, communication security and data protection. The related approaches for these implementations are presented. The TCP provides cloud computing a secure base for achieve trusted computing. However, integrating these hardware modules with cloud computing system is a challenging task and needs more advanced research. At present, a new model system of trusted cloud computing which is based on the trusted computing platform and can provide flexible security services for users.

## 2.9 Data Outsourcing in Cloud Environments a Privacy Preserving Approach

By increasing cost of maintaining IT centers, organizations are looking into outsourcing their storage and computational requirements to a cloud server. However, such outsourcing has also increased more serious issue of data privacy. Sayi et al [17] concluded their work in privacy-preserving data outsourcing. Specially, the author talked about the issue of employing vertical fragmentation to a relation so that the fragment that is assigned to the cloud server contains maximum data without violating privacy. At this time, privacy is spoken in terms of a set of confidentiality constraints. The author represented the confidentiality constraints as a graph where the nodes are the attributes and links represent paired confidentiality. The graph coloring problem is applied by the author with two colors for the cyclic portion of the graph. Some heuristic are used by the author to eliminate the cycles, and complete the coloring of all nodes. At present the author extending the work to multiple relations and constraints with multiple attributes in a constraint (i.e., triplet, quadruplet, etc.) instead of just pairs.

## 2.10 Privacy Enhanced Data Outsourcing in the Cloud

In cloud computing, outsourcing data security is more tedious task. The situation becomes even tougher when outsourced data sources in a cloud environment are handling by multiple outsourcers who hold diverse access rights. Miao Zhou et al, [18] presented an improved and new tree-based key management approach that permit a data source to be accessed by multiple parties who hold different rights. Make sure that the database that are present already are secure, while some selected data sources can be securely common with other certified parties.

This approach is more efficient and different from other approaches since it is based on novel tree-based key management scheme that allows a data source to be accessed by multiple parties.

# 3. PROBLEMS AND DIRECTIONS

It is obvious from the above discussion that cloud data security has always been an important feature of quality of service in the cloud environment. A number of cryptographic techniques have been used for the purpose of cloud data security.

Traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the user's loss control of data under cloud computing. Therefore verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of the data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging.

The main problems in the existing approaches are that

1. The communication traffic between the user and storage servers is high.
2. The user has to manage their cryptographic keys. If the user's cryptographic keys is lost or compromised, security problem will arise.
3. It is very hard for storage servers to directly support other functions excluding data storing and retrieving.

Storage servers cannot directly forward a user's messages from one person to another person. However the owner of the message is responsible for message decryption and also forwarding the same.

Data security required in cloud environment is data confidentiality to outsiders, including the cloud providers and their competitors. Data confidentiality alone is not the security requirement. Flexible and fine-grained access control is also desired in the service-oriented cloud computing model. Hence the outsourced data are generally encrypted so that only authorized users can access them. Generally, these outsourced data consist of many data blocks, hence the management of encryption keys is a major challenge.

Tree-based key management schemes are observed to provide better results for managing the encryption key. Compared with the other cryptographic techniques, this key management provides better security for the outsourced data.

Novel encryption algorithms with reduced encryption time utilized for cloud data security are required to protect outsourced data in a cloud in a more efficient way.

## 4. COMPARATIVE ANALYSIS OF THE EXISTING APPROACHES

The performance evaluation of the above discussed approaches is based on certain performance metrics. The security of the data outsourcing in the cloud is evaluated using three metrics like Decryption and Re-Encryption time, Time cost and the Space cost.

**Table 2: Methods to Secure Data Outsourcing in the Cloud**

| APPROACHES | DECRYPTION &RE-ENCRYPTION TIME | TIME COST | SPACE COST |
|---|---|---|---|
| WALLNER ET AL., (1999) | 0.2485 | 10.125 | 4.185 |
| WANG ET AL.(2009) | 0.1200 | 8.465 | 3.325 |
| ZHIDONG SHEN,ET AL., (2010) | 0.0915 | 8.125 | 3.195 |
| SAYI, T., ET AL., (2012) | 0.0855 | 8.015 | 3.141 |
| MIAO ZHOU ET AL., (2012) | 0.0540 | 7.119 | 2.154 |

### 4.1 Performance Comparison

Figure 2 shows the comparison of the Decryption and Re-Encryption time values of various approaches.

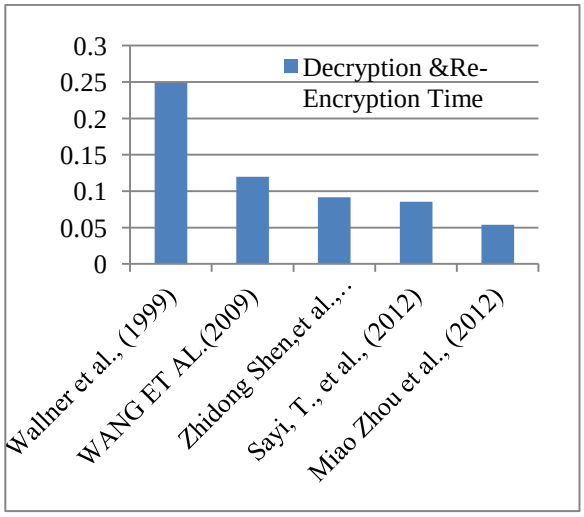


Figure 1: Comparison of Decryption and Re-Encryption time values

It is observed from the figure that the approach by Miao Zhou, et al., (2011) and Sayi, T., et al., (2012) outperformed the other approaches in terms of Decryption and Re-Encryption time values. For instance, the Decryption and Re-Encryption time obtained by the Miao Zhou, et al., (2012) is 0.0540, Sayi, T., et al., (2012) is 0.0855, Zhidong shen, et al., (2010) is 0.0915, where as it is very high for the other approaches taken for consideration.

Figure 2 shows the comparison of Time cost values for various existing approaches. It is observed from the graph that the Miao Zhou, et al., (2011), Sayi, T., et al., (2012) and Zhidong shen, et al., (2010) approach outperformed the other approaches in terms of Time cost.

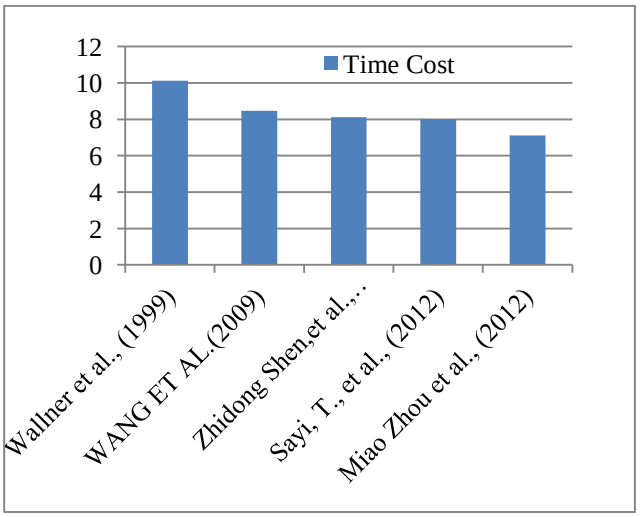


Figure 2: Comparison of Time Cost Values

Figure 3 shows the space cost of various existing approaches. The space cost of the Miao Zhou, et al., (2011), Sayi, T., et al., (2012) and Zhidong shen, et al., (2010) approach outperformed the other approaches in terms of Time cost, where as the other approaches is observed to provide high space cost.

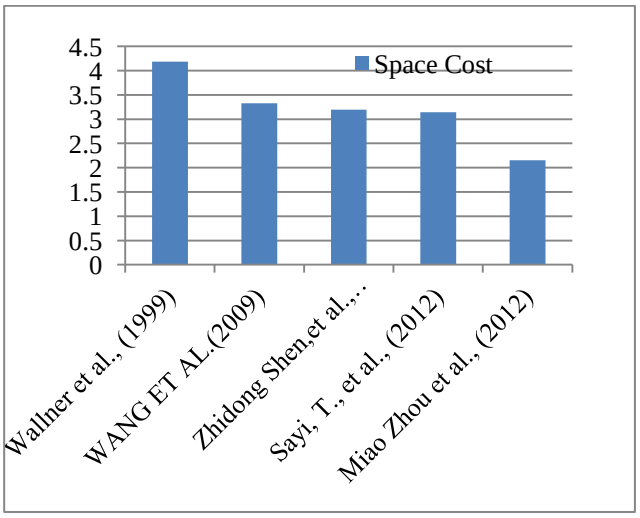


Figure 3: Comparison of Space Cost Values

It is inferred from the above results that the Miao Zhou, et al., (2011), Sayi, T., et al., (2012) and Zhidong shen, et al., (2010) approach outperformed the other approaches and gives significant results. Thus, also to increase the security of the data several other key management schemes and the new encryption algorithms should be developed.

## 5. CONCLUSION

This paper clearly discusses the various available cloud data security techniques and also analysis various security issues, characteristics features and working of the existing techniques. This investigation would be a motivation for research scholars to carry out their research work in cloud data security. It has been observed that, a number of cryptographic techniques have been presented to provide security and authentication to the cloud data. But, still there is space available for improvement. Key

management system is observed to provide significant performance in the cloud data security. Novel encryption algorithms have to be utilized for providing cloud security. Thus, more efficient encryption techniques have to be developed which reduce the time needed for encryption and decryption.

## 6. REFERENCES

[1] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono, Ninja Marnau, "Security and Privacy Enhancing Multi-Cloud Architectures" ISSN: 1545-5971,2013.

[2] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal "A Survey on Security Issues in Cloud Computing"2011.

[3] The NIST Definition of Cloud Computing, version 15, by Peter Mell and Tim Grance, October 7, 2009, National Institute of Standards and Technology (NIST), Information Technology Laboratory (www.csrc.nist.gov).

[4] Cong Wang ; Kui Ren ; Wenjing Lou ; Jin Li, "Toward publicly auditable secure cloud data storage services", IEEE Network, Volume: 24 , Issue: 4, Page(s): 19 – 24, 2010.

[5] Balding, C. (2008). Assessing the Security Benefits of Cloud Computing. Retrieved from http://cloudsecurity.org/blog/2008/07/21/assessing-the-security-benefits-of-cloud-computing.html

[6] Abhinay B.Angadi, Akshata B.Angadi, Karuna C.Gull, "Security Issues with Possible Solutions in Cloud Computing-A Survey", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 2, February 2013.

[7] Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Edition on Risks and Compliance (Theory in Practice)," O'Reilly Media, Sep. 2009; ISBN: 978-0596802769. http://oreilly.com/catalog/9780596802776.

[8] Lori M. Kaufman, "Data security in the world of cloud computing," IEEE Security and Privacy Journal, vol. 7, issue. 4, pp. 61-64, July- Aug 2009, ISSN: 1540-7993.

[9] Cong Wang, Kui Ren, Qian Wang and Wenjing Lou "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE transactions on Services Computing, vol 5, no. 3, pp 220-232, 2011.

[10] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No 5 May 2011.

[11] Sheng Zhong and Zhuo Hao. "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability," IEEE Internet Computing, 2010.

[12] Hsiao-Ying Lin, Wen-Guey Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding" IEEE transactions on parallel and distributed systems, Vol. 23, No. 6, June 2012

[13] Shucheng Yu, Cong Wang, Kui Ren, Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing" Technical Program at IEEE INFOCOM 2010

[14] Ashley Chonka, Yang Xiang n, Wanlei Zhou, Alessio Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks" Journal of Network and Computer Applications 2010

[15] Mohemed Almorsy, John Grundy and Amani S. Ibrahim "Collaboration-Based Cloud Computing Security Management Framework" IEEE International Conference on Cloud Computing (CLOUD 2011).

[16] Zhidong Shen, Qiang Tong "The Security of Cloud Computing System enabled by Trusted Computing Technology" 2nd International Conference on Signal Processing Systems (ICSPS), 2010.

[17] Sayi, T.J.V.R.K. ; Krishna, R.K.N.S. ; Mukkamala, R. ; Baruah, P.K., "Data Outsourcing in Cloud Environments: A Privacy Preserving Approach", Ninth International Conference on Information Technology: New Generations (ITNG), Page(s): 361 – 366, 2012.

[18] Miao Zhou , Yimu, Willy Susilo , Junyan , Lijudong "privacy enhanced data outsourcing in the cloud" Journal of Network and Computer Applications, 2012.

[19] Wallner, HarderE.Agee,Rfc2627: key management for multicast: issues and architectures; 1999.

[20] Wang W, LiZ, Owens R, BhargavaB. Secure and efficient access to outsourced data. In: Proceedings of the 2009 ACM workshop on cloud computing security, CCSW '09.NewYork, NY, USA: ACM;2009.p.55–66.