International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 22 (2017) pp. 11787-11795

A Novel Framework for Cloud Storage Security Using two way Verification

Rakesh Nag Dasari
Research Scholar, Department of computer science & Engineering,
Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur, Andhra Pradesh, India.
Orcid Id: 0000-0001-6504-650X

Dr. Y. Prasanth
Professor, Department of computer science & Engineering,
Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur, Andhra Pradesh, India.

Dr. O. NagaRaju
Head & Asst. Professor, Department of Computer Science & Engineering,
Sri Kasu Brahmananda Reddy Govt. Degree College, Macherla, Andhra Pradesh, India.
Orcid Id: 0000-0002-4906-529X

Abstract

With the rapid growth in the demand for HPC or high performance computing, the application or service providers are forced to provide application and services on cloud infrastructure. The major motivations are reducing cost of the on premises hosting of infrastructure, manageability of the application and variable demand of the application. Henceforth deploying the applications on the cloud can cater the benefits to the consumers of the applications. The management of the deployed applications can also bring three major challenges as network feasibility, computational feasibility and data security. After the application is pushed to the cloud infrastructure, the additional persuasion of security auditing must be integrated in order to protect the data. Various research attempts are made towards enabling the auditing features on the cloud based data by various researchers. Nevertheless, the complexity of the audit process proven to be the bottleneck in improving performance of the application as it consumes the computational resources of the same application. Thus the demand for the enhanced but low computational auditing process cannot be ignored. Henceforth, this work proposes a novel auditing framework in multiple levels in order to audit the access requests and upon validating the conditions of one level, the connection request will be moved to the further complex levels in order to reduce the computational loads. The proposed framework demonstrates a significant reduction in the computational load on the cloud server, thus improves the application performance leveraging the infrastructure use.

Keywords: Cloud Storage, Data Security, Two-Way Security, Consumer Security, Computation Cost Reduction

INTRODUCTION

Considering the recent growth in the space of computing with the introduction of cloud computing, Internet-of-Things, Grid Computing, Internet and information security, the newer dimensions are introduced for research. The notable work outcomes M. Armbrust et al on cloud computing [1], M. Whaiduzzaman et al. on vehicular cloud computing [2], P. M. Mell et al. on NIST [3], G. Han et al. on routing algorithms [4] and T. Qiu et al. on IoT [5] have motivated number of research enthusiast in the recent era.

With the introduction of cloud computing, the industry received a huge attention due to the benefits and advantages. Various companies, ranging from small to minimum to large enterprises migrated their applications on the cloud. Some companies migrated their data on the cloud due to the large size of the data and high cost of the dedicated storage facilities. The work by M. Ali et al. [6] has demonstrated the challenges of storing data on the cloud and security issues.

The practical approaches of the security implementations are discussed by T. A. Velte et al. [7], which enabled the research dentations for various researchers. The trend followed by Z. Xia et al. [8] by proposing rank based search scheme over encrypted data, Z. Fu et al.[9] by demonstrating personalized search operations over encrypted data and again with Z. Fu et al. [10] by secure searching operations on cloud data.

Nevertheless, the data owners demand for the continuous proof of the correctness of the data so that the consumers of the data can receive the secure and correct data from the services. A number of research attempts are been made to ensure the remote monitoring and auditing of the data. Few distinguished work established the thought to ensure the correctness with data integrity verification by Y. Ren et al [11] on provable auditing of data, B. Chen et al. [12] on remote verification of the data based on network coding and G. Ateniese et al. [13] on prevention of untrusted access of the data.

Henceforth, it is natural to understand that the challenges as,

Firstly, it is to allocate computational loads in optimal among the data processing and security features.

Secondly, as third party companies host the data, hence the protection is also the responsibility of that company and the data owner company need to decide upon the access of the data to the service provider.

Thus, building the public auditing system with the benefit of preserving the privacy of the data is the major goal of this work. Additionally, this work also proposes a method to collect and store the access history for further statistical analysis.

The rest of the work is furnished as in Section – II the recent outcomes from the parallel research is been proposed, in Section – III the problem is been formulated, in Section – IV the novel framework is provided, in Section – V the results are been compared and finally in Section – VI this work presents the conclusion with future directions.

SURVEY OF THE RECENT LITERATE

Motivated by the overwhelming responses by the industry and consumer, a number of research attempts are made towards the cloud computing and more specifically towards the security of cloud based application and the data produced or accessed by the applications. Notable work demonstrated in the early stages of cloud data security is by G. Ateniese et al. [13] by introducing PDP model based on enhanced RSA algorithm.

In the initial models presented by various researchers are restricted on the static nature of the application access on the data. Nevertheless, the consumer specific applications tend to have more dynamic access requests to the data. The existing protocols fail to address this problem. Henceforth, the novel outcome by C. Erway et al. [14] demonstrates the significant measures on data security in case of dynamic update requests. This creates a new trend in the research and further various enhancements were carried out in the space of cloud data security under dynamic access type requests. Few notables are to be named as C. Wang et al. in 2009 [15], Q.Wang et al. in 2011 [16] and K. Yang et al. in 2013 [17].

With the introduction of Big Data and relevant analytics load on the cloud services, few of the proposed methods tend to lose effectiveness due to complex nature of the proposed schemes. Thus the new trend of research was introduced by C. Wang et al. in the year of 2013 with a tag based solution to reduce the computing loads on the servers [18]. Also the concept of distributed security and the relevant challenges are been discussed by Y. Zhu et al. [19] for multiple instances of data. The multiple instances of the data, which is distributed and follow different scheme of signature are usually usages different signatures. Thus managing different signatures and verifying those can create a newer challenge for auditing. D. Boneh et al. proposed a novel signature aggregation method [20] for reducing the computational cost of the auditing and application.

In order to address the distributed and big data security challenges M. Sookhak et al [21] proposed a notable scheme of divide-and-conquer for effective management of dynamic auditing processes.

However, the security of the data on cloud and in case of any distributed architecture of storage relies on the security of the secure encryption keys. This disbelieve can cause a serious damage of the data. Henceforth, yet another challenge is to audit and trace the unnecessary exposing of the private secure key during the data access request. The notable work proposed by Y. Jia et al. [22] with a binary tree and generation or update of the key by traversing the tree in pre-order technique.

Henceforth, in the light of the recent enhancements of the researches, this work formulates the problem in the next section.

Problem Formulation

The cloud based data is generally accessed by the data owner, data consumers or the customers of the data owner, third party auditors and finally the cloud service provider. The owner is fully trusted in this scenario and it is the responsibility of the cloud service provider to ensure the security of the data while being accessed by the consumers. Nevertheless, the third party auditor and the cloud service providers can also access the data, while being partially trusted by the data owner. In such scenarios the challenge of data being accessed by any attacker in terms of audit information and statistical information of the cloud service provider is non-valuable. Thus making this model challenged by the researchers and demands improvements.

Secondly, the prime disrupt of these models are to consume the computational capacity of the cloud servers. The cloud server are configured to cater the consumer and data owner demands for higher loads, but the added computational processing for the security and auditing always tend to reduce the performance.

A. Evaluation of Generic Model

The above discussed model is the most popular existing framework [Fig – 1] in spite of the arguments for security.

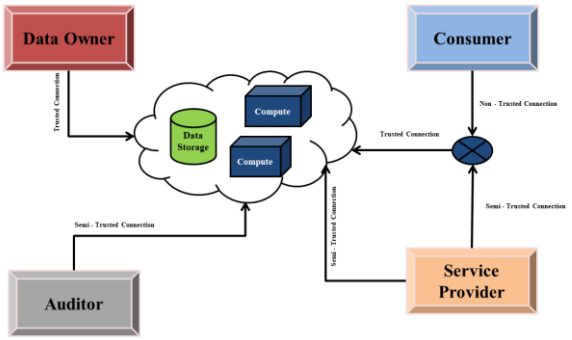

Figure 1: Three Party Verification and Cloud Data Security Model

The generic model is an association of the data owner, third party auditor and service provider. Along with these three parties, the consumer of the data is also to be considered. The first party, being the data owner, always can establish the secure and trusted connection to the data. In the other side, Auditor and Service Provider can also establish the connection to the data but those connections and access requests are considered to be the semi-trusted connections.

Finally, the connections from the data consumers are completely untrusted and it is the responsibility of the cloud service provider to reduce the risk of unauthorized access by verifying the connections.

B. Identification of Problems

In this part of the work, with the detail understanding of the existing framework, the core part of the problems are to be identified.

Firstly, the auditing and the data access requests from the third party auditor and the consumer of the data are to be verified. Considering the additional load on the computing capabilities of the cloud server, the reduced mechanism for verification is to be enabled without compromising the security challenges.

Secondly, the auditing and statistical data collection process is to be enabled for enhancements of the research and improvement of the performance.

Henceforward, this work proposes a novel two way verification framework in the next section of this work considering the problems identified in this section.

PROPOSED FRAMEWORK

The major identified drawbacks of the existing systems are semi-trusted access by the third party auditors and upon introducing the security measures for the auditor access to the data, the increase in the computing load on the cloud servers. Hence, this work proposes a two way security mechanism for cloud based data separately for data consumers and auditors based on different key based accessed. In this section, this work elaborates the two ways key based mechanism and also furnishes the comparative study in order to demonstrate the performance improvements [Fig – 2].

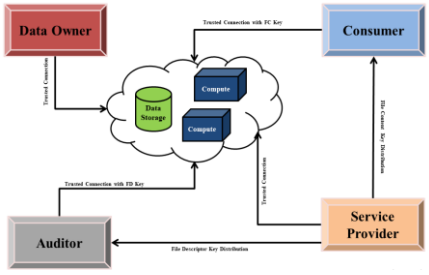

Figure. 2: Proposed Two Way Cloud Data Security Model

C. The Proposed Model

The proposed model algorithm is divided into four parts as generate the keys, upload the files with key based encryption, access request validation and finally the data decryption.

Step -1. Generation of the keys

Algorithm Part – 1: KeyGeneration

1. Randomize two prime number selection as A & B, where A is greater than B
2. Calculate the product of two prime numbers as K = A * B
3. Consider a random polynomial of order N as $\gamma(N)$
4. Calculate the intermediator of the key as $\gamma(N) = (A-1) * (B-1)$
5. Calculate the public prime component as E such that GCD (E, $\gamma(N)$) == 1
6. Generate the Public Key PK as PK = (E, $\gamma(N)$)
7. Generate the File Descriptor Private Key as FDPvK = (D1, $\gamma(N)$), where $D1 = E^{\gamma(N)} / |\gamma(N)|$
8. Generate the File Content Private Key as FCPvK = (D2, $\gamma(N)$), where $D2 = \gamma(N)^{E} / |\gamma(N)|$

Nevertheless, the key generation algorithm can be replaced by any proprietary encryption and decryption algorithm in general and the modified algorithm will not change the performance improvements of this proposed framework.

Step -2. Encryption of the file data and uploading of the file

Algorithm Part – 2: Encrypt and Merge for Upload

1. Segregate the file descriptor and the file content as consider as FD and FC respectively
2. If FD is not encrypted, then encrypt with PK & FDPvK, else continue to the next part
3. If FC is not encrypted, then encrypt with PK & FCPvK, else continue to the next part
4. If FD & FC both are encrypted, then merge the encrypted FD & FC and upload the file to the cloud storage

Once the files are uploaded on to the cloud, then the access requests can be accepted and process for the validation

Step -3. Access request validation

Algorithm Part – 3: Access Request Validation

1. If the access request is been made for the auditing access, then verify the request with the key combination of PK & FDPvK.
2. Once, the verification is valid, and label the request as FDR. Else terminate the request.
3. Else If the access request is been made for the data access, then verify the request with the key combination of PK & PCPvK
4. Once, the verification is valid, and label the request as FCR. Else terminate the request.

This step will significantly reduce the computational overload of the security process and also ensure semi-trusted access to the core components of the cloud data.

Step -4. Decryption of the file

Algorithm Part – 4: Decryption of the Content

1. If the requester label is FDR, then process the file descriptor and decrypt.
2. Else If the requester label is FCR, then process the file content and decrypt file descriptor and content both.

Hence with this separation of the validation, encryption and decryption based on labels will significantly reduce the time complexity of the framework and thus will reduce the computing load challenges.

D. Comparative Analysis with Existing Model

After the formulation of the algorithm in the framework, this work compares the proposed framework with the existing model.

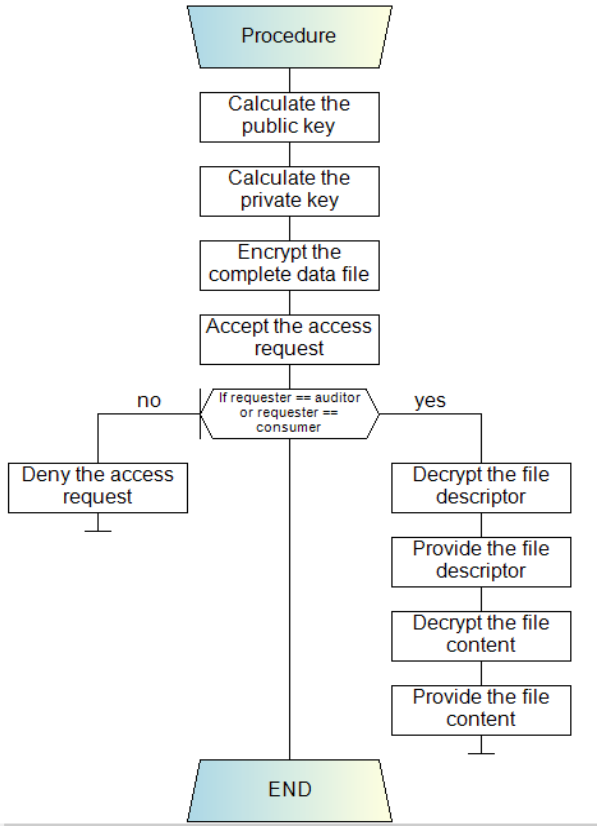

Figure 3: Existing Data Security Process

Firstly, the existing model is to be considered [Fig – 3]. It is natural to understand that, in spite of the variation of the access request types; this process cannot differentiate the requester types. Hence the complete content i.e. files descriptor for the auditing purpose and the content for the consumer purposes are exposed to the auditor and consumer both. Hence, making the model time efficient, but at the same time making the model security compromised.

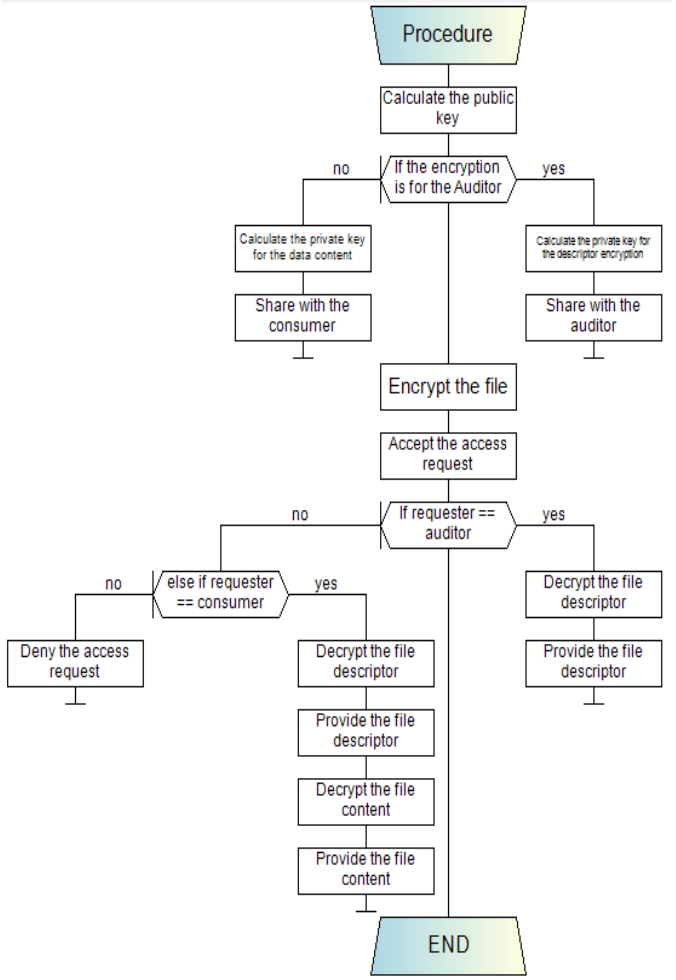

Figure 4: Proposed Data Security Process

Secondly, the proposed model is to be considered [Fig – 4]. It is natural to understand that, this process is sufficient enough to categorize the access requests and provide only designated access to the required data. The time complexity of this algorithm is moderate as the descriptor of the file will be much lesser than the size of the content, thus encryption of the parts of the file can be justified. In the other hand, this process restricts the exposing of private contents to the auditors.

RESULTS AND DISCUSSION

The result evaluation of this work is been simulated and performed in controlled simulation environment. The simulation setup is identical for existing and proposed framework [Table – 1].

TABLE I: EXPERIMENTAL SETUP

SNO	Component	Records
1	Physical Host	3
2	Virtual Machines	105
3	Simulation Time	1000 Seconds
4	Cloudlets	110

The simulation results are been considered for existing method [Table – 2] and proposed method [Table – 3].

Table II: Existing Framework – Access Time

Cloudlet ID	STATUS	Data center ID	VM ID	Time (msec)	Request time (msec)	Response Time (msec)
0	SUCCESS	3	0	400	0.1	400.1
5	SUCCESS	3	0	400	0.1	400.1
1	SUCCESS	3	1	400	0.1	400.1
6	SUCCESS	3	1	400	0.1	400.1
2	SUCCESS	3	2	400	0.1	400.1
7	SUCCESS	3	2	400	0.1	400.1
4	SUCCESS	3	4	400	0.1	400.1
9	SUCCESS	3	4	400	0.1	400.1
3	SUCCESS	3	3	400	0.1	400.1
8	SUCCESS	3	3	400	0.1	400.1
101	SUCCESS	3	101	400	200.1	600.1
106	SUCCESS	3	101	400	200.1	600.1
103	SUCCESS	3	103	400	200.1	600.1
108	SUCCESS	3	103	400	200.1	600.1
100	SUCCESS	3	100	400	200.1	600.1
105	SUCCESS	3	100	400	200.1	600.1
102	SUCCESS	3	102	400	200.1	600.1
107	SUCCESS	3	102	400	200.1	600.1
104	SUCCESS	3	104	400	200.1	600.1
109	SUCCESS	3	104	400	200.1	600.1

Table III: Proposed Framework – Access Time

Cloudlet ID	STATUS	Data center ID	VM ID	Time (msec)	Request time (msec)	Response Time (msec)
0	SUCCESS	3	0	320	0.1	320.1
5	SUCCESS	3	0	320	0.1	320.1
1	SUCCESS	3	1	320	0.1	320.1
6	SUCCESS	3	1	320	0.1	320.1
2	SUCCESS	3	2	320	0.1	320.1
7	SUCCESS	3	2	320	0.1	320.1
4	SUCCESS	3	4	320	0.1	320.1
9	SUCCESS	3	4	320	0.1	320.1
3	SUCCESS	3	3	320	0.1	320.1
8	SUCCESS	3	3	320	0.1	320.1
101	SUCCESS	3	101	320	200.1	520.1
106	SUCCESS	3	101	320	200.1	520.1
103	SUCCESS	3	103	320	200.1	520.1
108	SUCCESS	3	103	320	200.1	520.1
100	SUCCESS	3	100	320	200.1	520.1
105	SUCCESS	3	100	320	200.1	520.1
102	SUCCESS	3	102	320	200.1	520.1
107	SUCCESS	3	102	320	200.1	520.1
104	SUCCESS	3	104	320	200.1	520.1
109	SUCCESS	3	104	320	200.1	520.1

The results are also analysed graphically for existing method [Fig – 5] & proposed method [Fig – 6].

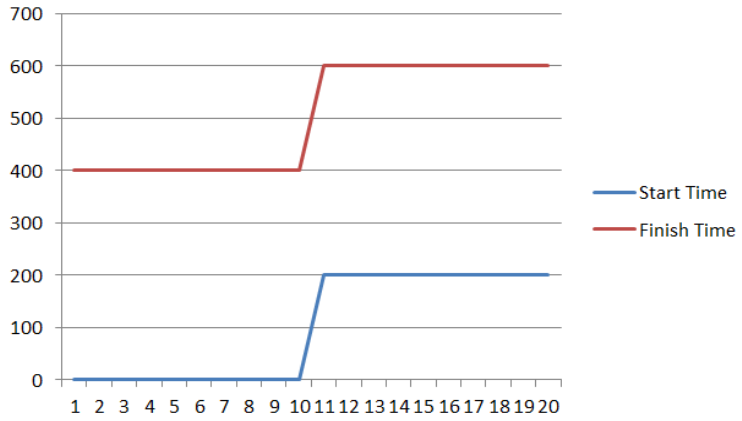

Figure 5: Existing Data Security Process Request Start & Finish Time

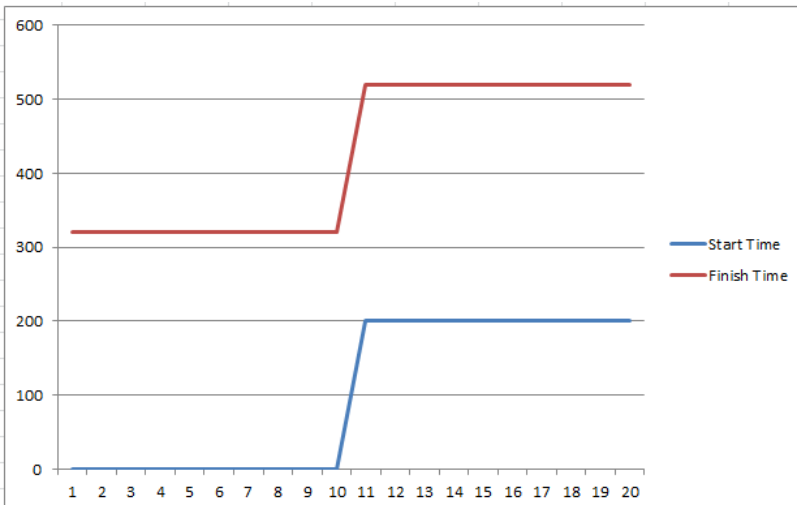

Figure 6: Proposed Data Security Process Request Start & Finish Time

Hence, the comparative analyses for both the methods are carried out [Table – 4].

TABLE IV: AVERAGE RESPONSE TIME

Model Name	**Average Time (msec)**
Existing Model	400
Proposed Model	320
Improvements	**25%**

The graphical analysis demonstrates the reduction in time complexity significantly along with the security enhancements [Fig – 7]

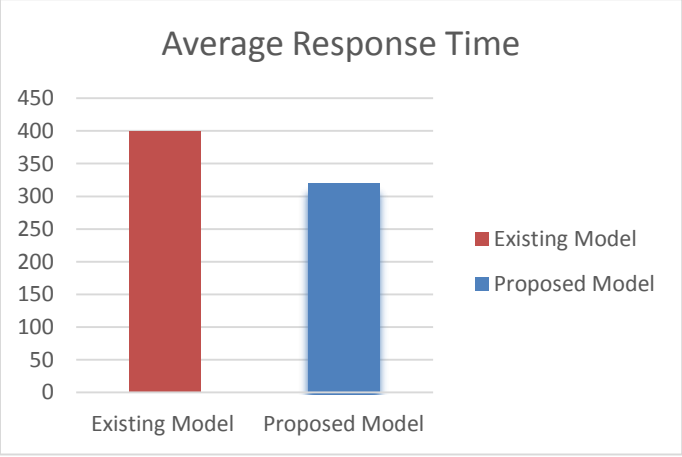

Figure. 7: Response Time Analysis

Henceforth, in the light of the results obtained and the comparative analysis of both the models, this work presents the conclusion in the next section.

CONCLUSION

The acceptance of the cloud computing is due to the nature of the applications and services to be scalable during the fluctuation of the demands. This characteristic alone gained a lot of popularity and acceptance of cloud computing. The acceptance motivated number of legacy applications to be migrated on to the cloud. Henceforth, the deployed applications and services generates a lot of data, thus the data needs security. In this work, a novel two way security framework is proposed and compared with the existing frameworks. This proposed method not only enhances the security measures, also demonstrates the reduction in response time as far as the encryption and decryption is concerned. This improvement will certainly help the researcher community to rethink on the security protocols those are used and predict the newer research dimensions. This work also proposes further study on the security factors during transmission over the network.

REFERENCES

[1] M. Armbrust et al., ``A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 5058, 2010.

[2] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, ``A survey on vehicular cloud computing," J. Netw. Comput. Appl., vol. 40, pp. 325344, Apr. 2014.

[3] P. M. Mell and T. Grance, ``The NIST denition of cloud computing,"Commun. ACM, vol. 53. no. 6, p. 50, 2011.

[4] G. Han, A. Qian, J. Jiang, N. Sun, and L. Liu, ``A grid-based joint routing and charging algorithm for industrial wireless rechargeable sensor networks," Comput. Netw., vol. 101, no. 6, pp. 1928, 2016.

[5] T. Qiu, D. Luo, F. Xia, N. Deonauth,W. Si, and A. Tolba, ``A greedy model with small world for improving the robustness of heterogeneous Internet of Things," Comput. Netw., vol. 101, no. 6, pp. 127143, 2016.

[6] M. Ali, S. U. Khan, and A. V. Vasilakos, ``Security in cloud computing: Opportunities and challenges," Inf. Sci., vol. 305, pp. 357383, Jun. 2015.

[7] T. A. Velte and R. Elsenpeter, ``Cloud computing, a practical approach,"Spatial Sci., vol. 60, no. 1, pp. 197198, 2015.

[8] Z. Xia, X. Wang, X. Sun, and Q. Wang, ``A secure and dynamic multikeyword ranked search scheme over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 340352, Feb. 2016.

[9] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, ``Enabling personalized search over encrypted outsourced data with efciency improvement," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 9, pp. 25462559, Sep. 2016, doi: 10.1109/TPDS.2015.2506573.2015.

[10] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, ``Achieving efcient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Trans. Commun., vol. E98-B, no. 1, pp. 190200, 2015.

[11] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, ``Mutual veriable provable data auditing in public cloud storage," J. Internet Technol., vol. 16, no. 2, pp. 317323, 2015.

[12] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, ``Remote data checking for network coding-based distributed storage systems," in Proc. ACM Workshop Cloud Comput. Secur. Workshop, 2010, pp. 3142.

[13] G. Ateniese et al., ``Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Security (CCS), 2007, pp. 598609.

[14] C. Erway, C. Papamanthou, and R. Tamassia, ``Dynamic provable data possession," ACM Trans. Inf. Syst. Secur., vol. 17, no. 4, pp. 213222, 2009.

[15] C. Wang et al., ``Ensuring data storage security in cloud computing," in Proc. 17th Int. Workshop Quality Service (IWQoS), 2009, pp. 19.

[16] 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, no. 5, pp. 847859, May 2011.

[17] K. Yang and X. Jia, ``An efcient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel Distrib. Syst.,vol. 24, no. 9, pp. 17171726, Sep. 2013.

[18] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, ``Privacypreserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362375, Feb. 2013.

[19] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, ``Cooperative provable data possession for integrity verication in multicloud storage," IEEE Trans. ParallelDistrib. Syst., vol. 23, no. 12, pp. 22312244, Dec. 2012.

[20] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, ``Aggregate and veriably encrypted signatures from bilinear maps," in Proc. Adv. Cryptograph.(Eurocrypt) Int. Conf. Theory Appl. Cryptograph. Techn., pp. 416432, 2003.

[21] M. Sookhak, A. Gania, M. K. Khanb, and R. Buyyac, ``Dynamic remote data auditing for securing big data storage in cloud computing," Inf. Sci., 2015. [Online]. Available: http://dx.doi.org/10.1016/j.ins.2015.09.004

[22] Y. Jia, R. Kui, W. Cong, and V. Varadharajan, ``Enabling cloud storage auditing with key-exposure resistance," IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 11671179, Jun. 2015.