Neural Parallel and Scientific Computations 29 (2021), No. 4, 185-198

IDENTITY-BASED AUDITING FOR SHARED CLOUD DATA WITH EFFICIENT AND SECURE SENSITIVE INFORMATION HIDING

A. P. PREETHI[1] AND R. VARATHARAJAN[2]

[1]Karpagam College of Engineering, Anna University, Chennai
Email: 3jsngl@gmail.com
[2]Bharath University, Chennai, India.
Email : varathu21@gmail.com

ABSTRACT

Recently, store and retrieve data in the cloud architecture is an attractive cloud computing research. In addition to these, the utilization of economic resources and security of data transmission by the company, additional constraints such as Google, Microsoft, Yahoo, IBM and Amazon in various internet services. Data and structure management is the biggest concern of cloud computing strategy, as they evolved into custody, and provide new service mode via the Internet. Cloud service provider (CSP), the owner To calculate the data of the resource pool, it is the main component of containing clouds. Maintenance of the data center of a large movement with the CSP application software. Cloud service, down scale-up, and has easy access performance. Consumers, the cloud computing model, you must have the integrity to ensure the confidentiality, privacy, availability and data access management. Cloud computing is promising as had been efficient, there are many challenges, because the user does not know the location of the data, there was a data security.Address security software industry is an important factor in cloud data processing applications. Therefore, this study focused create cloud security and vulnerability level constraint data transfer mode. In cloud computing, data maintenance CSP is thus used for data storage security and trust is dependent on third-party suppliers authorized person. The rise of password encryption and decryption mechanisms to ensure the privacy of cloud data protection deposition. An important process before the encryption mechanism is to understand the security, storage and data access vulnerability levels. Niubi The purpose of this article is to provide security and privacy challenges of analyzing significant cloud computing and create policy challenges derived from observation. Encryption and decryption mechanisms to cloud computing model provides a number of enhanced security attributes involved in lead-based encryption (ABE)

Received July 15, 2021
www.dynamicpublishers.org;
https://doi.org/10.46719/npsc20212942

of property-based development. The job analysis study and consider the behavior of the traditional ABE program spending measure.

1. INTRODUCTION

The study estimated that the relationship between the various encryption schemes based on the communication, computation and parameter storage of overhead. The proposed study shows the mechanism-based encryption key, how to strengthen and attributes, file size, and the number of key safety performance. The research work program consists of three phases. The initial stage of reviewing safety issues, challenges, threats, vulnerabilities, the corresponding encryption solutions to these problems. The state of the next phase of discussions about solutions to maintain the robustness of the data integrity of the cloud deployment model. Security and key integrity and verify the performance of the existing proposed DKP ABE program to export the final stages of discussions to generate a key strategy (DKP) to manage.

Cloud computing is a type of calculation, depending on the computing resource sharing between servers and applications, and has been hosting and providing services via the Internet in a new paradigm. Hosted applications, the cost and storage with cloud computing applications art designs significantly reduced. Cloud is located in a remote location, named network or the Internet. Users can access the application via the Internet tool. Users can configure the operation and use Internet applications at any time. Users can work from anywhere. Users are not restricted their hands which device. Users are not restricted their hands which device. There is no need for any software to access or manipulate cloud applications. Cloud computing provides a development and deployment tools, which are available on the Internet. It is maintenance free, saving time. Cloud computing resources on the network. It provides independent access to any type of client. Server capacity with extended vertically. It uses only the required energy is environmentally friendly, without leaving a large carbon footprint. Ideal growing bandwidth requirements and fluctuations. It provides on-demand self-service. These resources cannot interact with the cloud service provider to use. Cloud computing is highly cost effective because it has a higher work efficiency. These resources cannot interact with the cloud service provider to use. Because it has a high working efficiency, cloud computing is a very effective cost. To access the data in the store data and the

cloud is, only you will need to connect to the Internet. Cloud computing, improved the more reliable, and provides excellent load balancing.

Figure 1: General Diagram of Cloud Computing

Figure 1. Control, cloud computing technical configuration and online access to process applications used, and provides data, online storage infrastructure and applications to complete. FIG total cloud computing infrastructure depicted in figure 1.

Public clouds are those available to the general public by the service provider. Application hosting service provider in the cloud infrastructure. Public cloud providers are listed in the following general types: These types of vendor's own public cloud, they run in the cloud infrastructure, but also provide access via the Internet. With these types of clouds, the visibility of the position of the user does not cloud. All public cloud users Infrastructure consists of a number of the cost of the infrastructure of the user, security, you can share the same limited pool of protection of public cloud customers to share. Public cloud users, at a low cost, will let you operate go the model as a paid. Private cloud infrastructure, specific to a particular organization, companies have been able to host the application in the cloud. Issues related to private these types of data security and control of the cloud, this is not a solution to deal with the public cloud environment. Not shared with other organizations inside or the outside of the private cloud.

Private cloud deployments within a single organization in the chair. These types of clouds commonly used applications, which require comprehensive infrastructure control and configurability in. In the externally hosted private cloud is a use of the organization, but by third-party hosted in the cloud infrastructure. Service providers to ensure the privacy of the whole cloud environment. This type of format is organized, do not like to use the public cloud infrastructure. Sharing of physical resources associated with the risk of a public cloud infrastructure. All clouds have a distinct identity, but together, offer the advantage of a variety of deployment models. Third-party provider may be controlled in any complete Or partially mixing method by increasing the flexibility of cloud computing. Hybrid cloud architecture of either of cloud-based computing infrastructure, will require the resources of the server and on-premises off-site. Community cloud is a multi-tenant cloud service models, which are shared between different organizations. Community cloud governance, all of the organizations involved in the management and assurance. Community cloud, to establish a form of a mixture of a specific target group, is a private cloud, it is to operate. It is that the purpose community cloud to cooperate in order to achieve business goals. Community cloud can be divided into open and off-premises cloud.

2. RELATED WORK

Cloud service providers by checking independent of user data (CSP), authorized user to view the details of the operation, to share the vulnerabilities of multiple users (multi-tenant) in the introduction of the same infrastructure security since it is not. Ran et al. (2012) it is, outlines the challenges for building a trusted cloud environment, the importance of appropriate solutions. They highlight the impact of the multi-tenant nature of the security and privacy in particular. In a multi-tenant is required to optimize the use of resources essential attribute. Typically, the principle of virtual hardware utilization in a CSP, wherein said physical characteristic is made hidden. While performing the burden caused by the same physical structure and examples of multi-user, CSP. Function between the virtual environment and cloud infrastructure shared a similar result in the exchange of software flaws and vulnerabilities. Therefore, higher security than non-virtualized cloud environment risk.

Deyan, Hong Kong (2012) safe, we discussed the impact of various multi-tenant property. Isolation particular physical resources, security measures, is a source of significant impact on cloud

security to process the data and the vast amount of information from unauthorized access, a user who is a unified deployment of the main thread. They are, integrated framework, in order to provide the data to be carried out in order to identify the user's privacy guarantee security solutions isolation, it was concluded with the need to support the national defense strategy.

Malicious insiders in the cloud cannot be trusted to steal users cause problems deployment model confidentiality of data in the cloud. Rocha and Correaia (2011 years), which consists of two processes, and mechanisms for reporting attacks failed to prevent the attack data to achieve the creation of trustworthy model. They discussed namely the following attack, plaintext passwords are Snapshot of memory, are stored in the generation of the secret key, extraction of transition sensitive data and virtual machines. They emphasized the protection of the attack, ie encryption, were distributed computing, trust and confidence. IAAS data manipulated by various applications running on the virtual machine. However, if there is no implementation of encryption. Application of fully homomorphic encryption (FHE) is the main solution to the above problem. However, to reduce the performance of the various types of data from the FHE client. In order to provide security, we can calculate reliable alternative strategies to address the challenges of the new security. But the problem is to maintain a reliable computing model, is caused by an external entity. This allows users without assumption is conflict between administrators and service provider of trust, although the malicious user, you can rest assured that no. Than a single cloud, such as Al Zain of clouds of sports-related security issues (2012) survey. They will focus on multi-promotion The use of the cloud, to reduce the risk of security. Security protocols such as this Byzantine agreement, for, to discuss the DepSky system cloudy environment. A large number of users, will be involved in causing a decrease in the level of availability of the service. We discussed a variety of research for they are in to reduce the risk of on process safety related to cloudy use.

Protection of sensitive data and comply with the law's achievements are the main focus point cloud model. Itani and so on. (2009) PAAS model focused These user-configurable software and data privacy two strategies as a protective mechanism, on. Completely trust the cloud service provider (CSP) based compliance, there is not trust the three levels of trust in the trust relationship support. They provide information about encryption coprocessor configuration and distribution, of the type described and encryption software use categories. They describe various protocols, namely the implementation of the process data transfer protocol, the software implementation of

the agreement and privacy feedback protocols. Privacy detailed study to provide a guarantee of future expansion, such as design choices and no TPA, alternative process models and supporting key management software to create a department of investigation of the development mode of PAAS PAAS mode. Data outsourcing and any computing cloud model is a difficult process unreliable. Bugiel, and so on. (2011) proposed structure, outsourcing and data to support any calculations. In this operation the following architecture: a communication, the application data encryption and authentication Between the cloud that can be trusted with the user. Encryption mechanism, in order to ensure the security and user privacy, we saw from the issues that arise in research. Words that have been hidden from the Greek means "password". The method of function of dividing the encrypted data transmitted to the intended recipient who has access to the information in the form of data and security. Encryption mechanisms, two processes, that is, the method comprising encrypting and decrypting. Original information (plaintext) was transformed into unreadable form (ciphertext), also known as reverse encryption process, so that the recovery information in its original form is called decryption. The rationale behind the substitution and transposition encryption mechanism. A plain-text elements to other Alternatively mapping plaintext elements and elements referred to in different order rearrangement called permutation. Encrypted encryption and decryption model. For other related works we refer Abraham, and so on (2013), Arora R, and so on (2013), Bamiah MA and so on (2011), Bhosale, and so on (2012), Bisong, and so on (2011), Feng J, and so on (2011), Fugkeaw S, and so on (2012), Graf S, and so on (2012), Grobauer B, and so on (2011), Jansen W (2011), Kalpana P and so on (2012).

3. RESULT AND DISCUSSION

Based access structures, policies divided into two types, namely keypolicy and ciphertext policy. The first defines the user's private key of the access structure and a second structure defined in the ciphertext. Access structure extends property change based encryption (the ABE) of various types. We begin in comparison, with regard to the access structure analysis between the ABE program. In this study considered more ABE programs are as follows:

- Policy-based ABE key (KP-ABE)
- Text Strategy ABE Ciper of (CP-ABE)

- ABE access structure with non-monotonic
- Grading ABE

KP-ABE generation process in the tree structure communication process in a disposable utilization in many private key. And real-time data encryption and support a minimum KP-ABE do not know who is a person of the data decryption. Isolation is provided between the private key and KP-ABE access attribute control structure leads to dissatisfaction. However, the CP-ABE conscious about the decrypted data results in real-time support. Most preferred the communication policy CP-ABE, since the set of access control structure and a private key from a group satisfying property. Although CP-ABE has several advantages, the negative restrictions are not considered for implementation. Seen from the analysis is the lack of provision of high security. Therefore, this study is defined as a better use of cloud resources to ensure the level of security derived key strategies. Cloud security model for the implementation of key export strategy (DKP), and is described in following Chapters.

3.1 Security Performance

The number of subsets derived key policy recommendations (DKP), and participate in key attributes of the coverage optimization of high-level access control security analysis of vector-based group key management. For each number of key attributes, security, performance estimate is a percentage value. Optimized subset cover based on the tree structure. Increasing safety performance is the property of each number up to eight properties observed. Is 8,9,10 property, safety performance is significantly reduced. Due to the presence of the safety performance of the non-linear relationship between the number of security attributes and a significant Key Export Strategy (DKP) also followed gradually improve the safety performance of even larger number compared to a subset of the coverage optimization properties. For the maximum number of key attributes, security 98% performance due to less time and timely delivery of the encrypted cipher text to the appropriate user. Safety performance (%) presented in the graphical representation of the performance of DKP are shown higher than 38%Optimization subset cover.

The non-monotonic access structure uses the policy that includes the negative constraints. Due to the involvement of negative constraints to the policy, the overhead is increased considerably. To limit the overhead, hierarchical structure of key generation is evolved in HABE

mechanism. The descriptive analysis of all the schemes for various parameters such as efficiency, collision resistant, computational overhead, and access control are discussed in following chapters.

Table 1.

Number of key attributes in %	Subset Cover	DKP
1	21	39
2	42	50
3	58	61
4	62	80
5	78	80
6	80	82
7	90	91
8	65	94
9	77	97
10	60	98

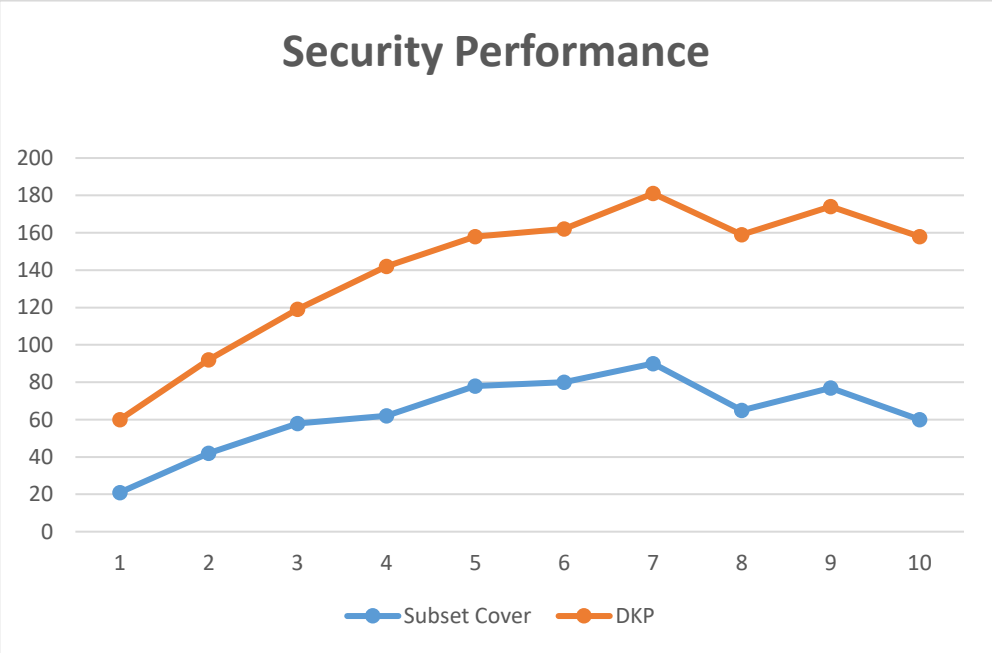

Figure 2: Performance of sensitivity analysis

When the AP - real good, FN - false negative. Viewed from a different fundus image data set to a different pattern.

Table 2.

No. of Attributes in %	**ACV-BGKM**	**DKP**
2	58.50	68.99
4	67.00	69.74
6	73.25	78.92
8	78.45	82.53
10	76.97	87.14
12	83.41	92.42
14	83.18	92.91

DR specifically shown in Figure 2, which generates a higher efficiency than other methods than the above-described embodiments true positives accuracy. In 98% of the accuracy of the result of this proposed method, as well as non-conventional systems microaneurysms prognosis - proliferative diabetic retinopathy (PMNPDR), provided 72% and 88% of the collection system (EBC) based.

3.2 Specificity Analysis

Specificity, positive predictive value of a properly rated positive or negative rating was rated appropriate part of the rating, the true negative rate ratio.

When AN- actual negative, FN- false negative. Analysis using different specific fundus image 5 in FIG. Generating different test values in the database in different ways. The proposed system is greater than the specificity of other methods, and gives an QCD review of the proposed method for analyzing the specificity ratio of 98%. Similarly, conventional methods are PMNPDR EBC and provide 76%, 89% results.

3.3 Encryption time

File size and analysis of the proposed DKP and role-based access control and encryption time varying comparisons. An increase in the file size will gradually longer the encryption time. In the existing role-based access control, at the time of encryption, it is for more of the maximum file size. As shown in Table 2, however, it proposed DKP has provided the minimum time requirement. Visualization of the comparison of the proposed DKP and role-based access control is shown in Figure 6.3. 17 ms encryption time for 30 milliseconds proposed DKP for role-based access control low file size (one B). Similarly, the maximum file size, will be respectively encrypted time 93 ms and 65 ms (100 MB).The comparative analysis shows that the reduction of 43.33 % and 30.11 % for low and high file sizes compared to role based access control is achieved by proposed DKP.

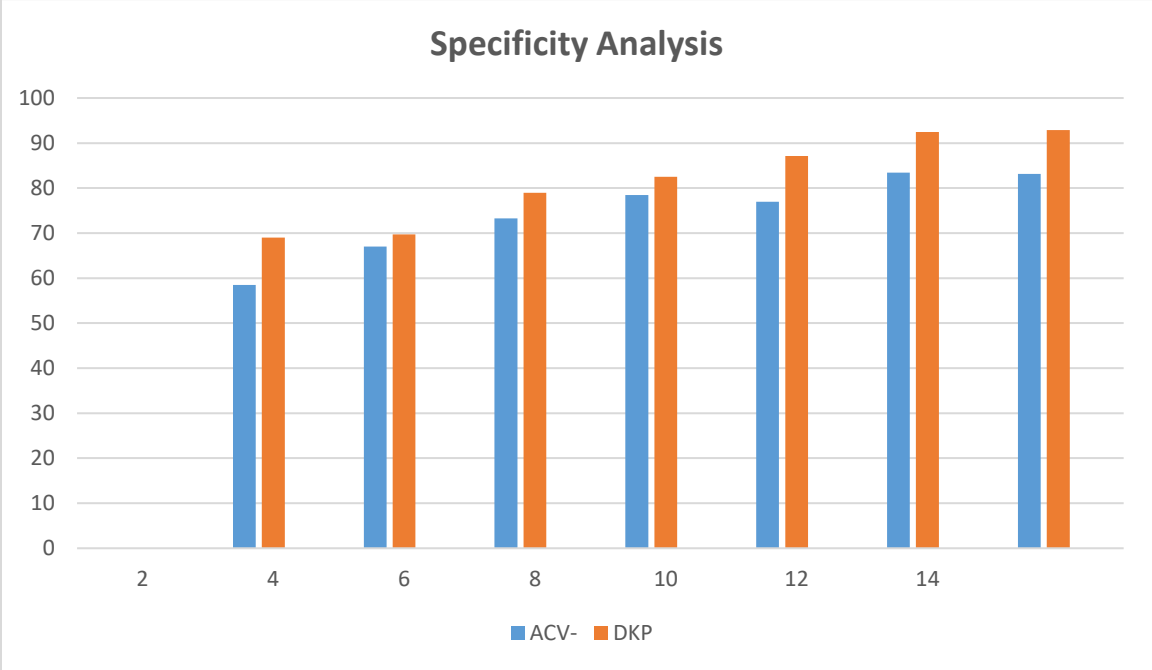

Figure 2: Performance of specificity analysis

Besides subset cover, the comparative analysis of proposed DKP and the existing methodologies of ACV-BGKM for the maximum file sizes as depicted in Table 3.

Table 3.

File Size (Mb) sec	ACV-BGKM	DKP
5	14.24	11.23
10	17.57	13.36
15	19.56	14.27
20	22.45	15.98
25	25.12	17.50
30	27.78	19.01
35	30.44	20.53

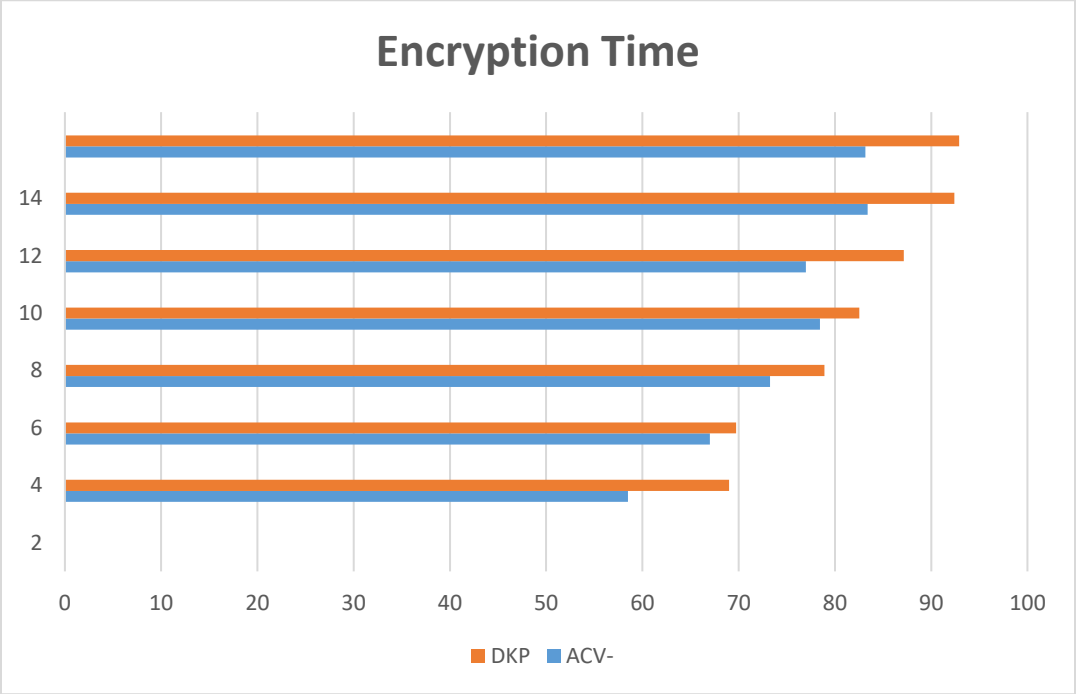

Figure 3. Encryption time in terms of the small file sizes for proposed DKP and

The graphical representation of comparative analysis between the encryption time and number of attributes is illustrated in Figure 6.4. The proposed DKP offered the low time consumption for encryption process compared to the existing methodologies for the maximum file sizes. For the maximum size of 35 MB, the encryption time for DKP is 20.53 ms which is less compared to other methods of ACVBGKM by a percentage of 36.73, 32.91, 25.13, and 32.56 respectively.

4. CONCLUSION

And data stored in the cloud architecture, retrieving data transmission efficiency and security of economic resources is to limit the variety of Internet services offered by companies such as Google, Microsoft, Yahoo, IBM and Amazon compute an attractive Research in the field of cloud. Research focused on the following concerns - cloud computing strategy and management structure. Cloud service provider (CSP), the owner of the data is a major component in cloud computing and containing the resource pool. The CSP maintenance of application software to move large data centers. Simple access to various properties of the study involved scaling down cloud model. Integrity under the cloud computing model using the consumer should have the following characteristics, confidentiality, privacy, data availability, and their identity. We have reviewed this study challenges the cloud security model. In addition, this model guarantees data transmission research focused on creation, regardless of data location. Integrity verification to ensure the privacy and security of data and storage requirements. But still some challenges proposed to provide security. In order to ensure the protection, encryption mechanisms under investigation evolved. Knowledge about security vulnerabilities and security levels of data access is regarded as the initial stage of encryption mechanisms.

REFERENCES

[1]. Abraham SE & Gokulavanan R 2013, ‘Ensuring Privacy and Security in Data Sharing under Cloud Environment’, International Journal of Computer Applications Technology and Research, vol. 2, no. 2, pp. 188-194.

[2]. Al Zain M, Pardede E, Soh B & Thom J 2012, 'Cloud computing security: from single to multi-clouds', 45th Hawaii International Conference on System Science (HICSS), 2012 pp. 5490-5499.

[3]. Arora R, Parashar A & Transforming CCI 2013, 'Secure user data in cloud computing using encryption algorithms', International Journal of Engineering Research and Applications, vol. 3, no. 4, pp. 1922-1926.

[4]. Bamiah MA & Brohi SN 2011, 'Seven deadly threats and vulnerabilities in cloud computing', International Journal of Advanced Engineering Sciences and Technologies (IJAEST), vol. 9, no. 1, pp. 87-90.

[5]. Bhosale P, Deshmukh P, Dimbar G & Deshpande A 2012, 'Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption', International Journal of Engineering Research and Technology.

[6]. Bisong A & Rahman M 2011, 'An overview of the security concerns in enterprise cloud computing', International Journal of Network and its applications (IJNSA), vol. 3, no. 1, pp. 30-45.

[7]. Bugiel S, Nurnberger S, Sadeghi A & Schneider T 2011, 'Twin clouds: An architecture for secure cloud computing', Workshop on Cryptography and Security in Clouds (WCSC 2011).

[8]. Deyan C & Hong Z 2012, 'Data Security and Privacy Protection Issues in Cloud Computing', International Conference on Computer Science and Electronics Engineering (ICCSEE), 2012 pp. 647-651.

[9]. Feng J, Chen Y, Summerville D, Ku W-S & Su Z 2011, 'Enhancing cloud storage security against roll-back attacks with a new fair multi-party nonrepudiation protocol', Consumer Communications and Networking Conference (CCNC), 2011 IEEE, pp. 521-522.

[10]. Fugkeaw S 2012, 'Achieving privacy and security in multi-owner data outsourcing', Digital Information Management (ICDIM), 2012 Seventh International Conference on, pp. 239-244.

[11]. Graf S, Lang P, Hohenadel SA & Waldvogel M 2012, 'Versatile key management for secure cloud storage', Reliable Distributed Systems (SRDS), 2012 IEEE 31st Symposium on, pp. 469-474.

[12]. Grobauer B, Walloschek T & Stocker E 2011, 'Understanding Cloud Computing Vulnerabilities', Security & Privacy, IEEE, vol. 9, no. 2, pp. 50-57.

[13]. Itani W, Kayssi A & Chehab A 2009, 'Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures', Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009. DASC '09., pp. 711-716.

[14]. Jansen W 2011, 'Cloud hooks: Security and privacy issues in cloud computing', System Sciences (HICSS), 2011 44th Hawaii International Conference on, pp. 1-10.

[15]. Kalpana P & Singaraju S 2012, 'Data security in cloud computing using RSA algorithm', IJRCCT, vol. 1, no. 4, pp. 143-146.