J. Appl. Environ. Biol. Sci., 6(2S)102-108, 2016

© 2016, TextRoad Publication

ISSN: 2090-4274
Journal of Applied Environmental
and Biological Sciences
www.textroad.com

Secure Data in Cloud on the Basis of Sensitivity

Asif Iqbal[1], Haseeb Ur Rahman[2], Mazhar Ullah Khan[3], Muhammad Fayaz[4]

[1,2,4]Department of Computer Science & IT, University of Malakand, Pakistan
[3]Network Administrator, PakistanTelevision,Peshawar, KPK, Pakistan

Received: January7, 2016
Accepted: March 2, 2016

ABSTRACT

Cloud computing is an Internet based model, providing many advantages to its clients in the form of low cost, broad network access etc. On the other hand security is considered to be the biggest concern, which is a big hurdle in the wide adoption of cloud computing. With high rates of storage and high growth in data production, cloud data centers are becoming attractive places for the storage for both the individual users and organizations (both are called clients here). The security of data, especially of sensitive nature, is a matter of big concern and there is the need of providing protection to the data in the same manner, i.e. more security for sensitive data than ordinary. The focus of this paper is to discuss security for data on sensitivity bases.

KEYWORDS: Cloud Computing. Encryption algorithm.Data sensitivity. Data storage

1. INTRODUCTION

The storage of data in cloud data centers is increasing day-by-day due to its economic advantages. As the use of computer in our life is increasing, therefore the data generation of clients is increasing as well. The increase in amount of data generation can be problematic for small organizations or individual users as they would have to buy large storage devices which is a finanacial burden for them . Cloud providers provide enough large storage for this data on a meagre cost base and also keep multiple copies of the same data, which can be helpful in the process of recovery. Hence, there is a good chance for these users to store this large data with low cost in cloud data centers. The owners are relieved with the security of their data and they can access to it whenever they want.

Storing clients' data in the cloud means that it is now out of control of them giving rise to many security concerns. Therefore, integrity and privacy of data become very important for delivery of correct format to the concerned party. Encryption is a way to provide security to the data used in a cloud environment[1, 2].

This research work provide such a mechanism where clients can themselves provide extra security to their most important data on the basis of encryption. This scheme is not only helpful for cloud computing, but also used in other fields like long term archives, database system etc. The cloud client selects files and appropriate encryption level security for the data. Since cloud data center servers (storage) are not trusted [3], hence this scheme can provide a better source for the privacy and integrity to the untrusted storage like that the cloud has now. A better working condition for both cloud client and provider based on confidence can be expected from this scheme. On the bases of better cloud data protection, clients may be confident to store more sensitive data which they were reluctant to store it previously.

The rest of this paper is organized as: Section 2 explains the cloud computing background which consists of the basics of the cloud model, issues with cloud computing, data integrity and privacy. In Section 3, related work will be discussed which was found to be helpful to do this research work. In Section 4, the proposed model has been presented/discussed. The work has been concluded in Section 5.

2. Background

2.1 The Cloud Model

NIST definition of the cloud is largely used definition of cloud computing "*Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.*"[4]. According to NIST cloud computing has three service models, i.e. Software as a Service (SaaS), Platform as a service (PaaS) and

Corresponding Author: Asif Iqbal, Department of Computer Science & IT, University of Malakand, Pakistan
asifuom577@gmail.com

Infrastructure as a Service (IaaS), four deployment models Private cloud, community cloud, Hybrid Cloud and Public cloud[5]. According to [6] there are six characteristics of the cloud model, i.e. on-demand self-service, Broad network access, Resource pooling, Location independence, Rapid elasticity and Measured service.

2.2 Issues With Cloud Computing

Cloud computing has already gotten the attention of not only clients and developers, but also of the providers because they see the bright future of it from a business point of view. However, there are issues that keep the clients away to adopt this field to take advantages of it. These issues are aroused due to clients' data and applications are on the premise of providers as they have shifted them to the data centers of providers. Security, integrity and privacy are the main issues along with others [7]. According toV. S. K. Maddineni and S. Ragi[8], identified 43 security challenges e.g. DoS attack, Data leakage, data availiability etc in cloud computing. Moreover, the worries of these users are strengthened by events that happened in 2009 when Amazon's simple storage service stops to provide services in February and July. Similarly, in May 2009 Google Gmail also became victim of an attack and went silent for four hours, also Microsoft Azure remained suspended for 22 hours and there occureda lossof 45% of clients' data in this case when it was attacked by hackers [9]. Drop box which is a cloud storage provider sufferred when passwords were lost from their database and anyone could use their data [10]. According to Muna Paul[11] the seven security concerns in cloud computing based on survey that were found by (ISC)^2 are shown in Figure 1.

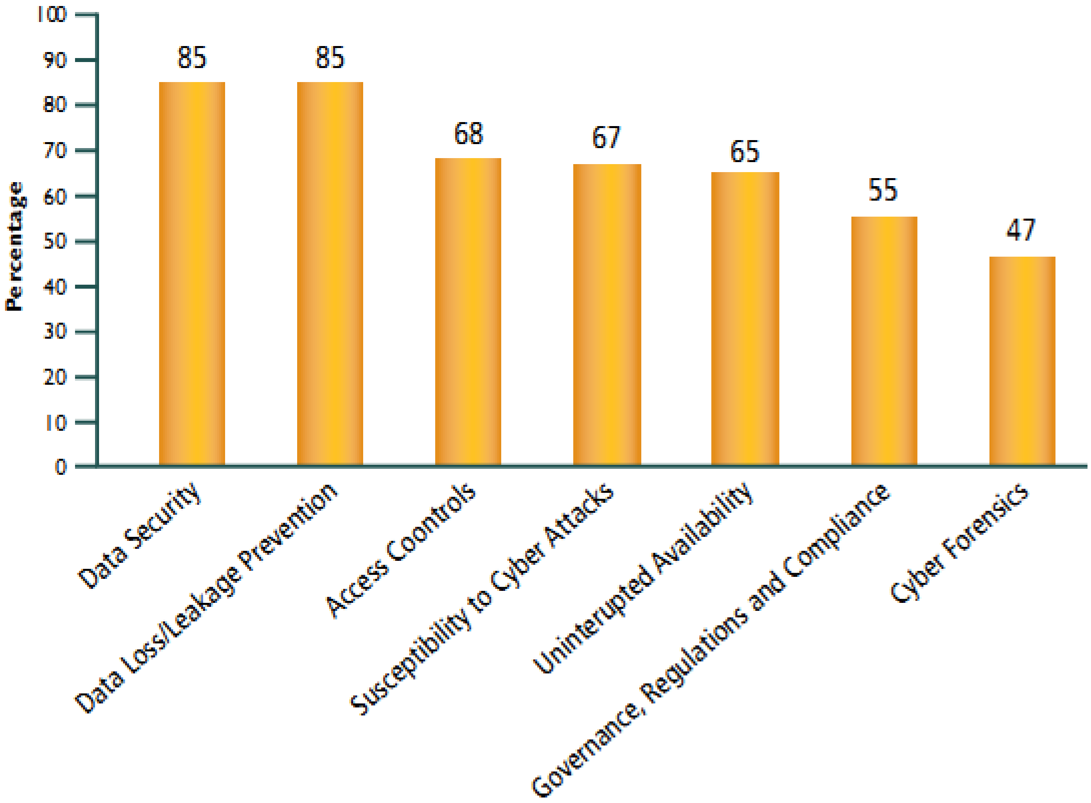

Figure 1. Cloud Security concerns

From Figure 1, it is clear that the security of data in the cloud data storage centers is very important and encryption can play a handy role in this regard. So, both data privacy and integrity become key points for the security of cloud computing and hence for the bright future of cloud computing.

2.3 Data Privacy And Integrity

The data that is to be communicated from sender to receiver must not be modified between these points[12].The term integrity means that the clients' stored data can't get corrupt. On the other hand the term privacy is used in the sense that private data won't be leaked to any unauthorized entity [13]. Therefore it is possible to say that integrity of data largely depends on privacy of the data. Without privacy, the integrity of data is not an easy task. Since organizations heavily depend on this data (in the case of cloud data is out of users control), it is considered as a matter of life and death for organizations. So, it must be handled properly, otherwise it will be a total disaster for organizations whose data is compromised. It is very important for cloud clients to keep their data secure, because finally its responsibility in case of any mishap will fall on their shoulders [14]. So the clients should also take the responsibility of securing their data because it can play good role in securing own data. This is also the aim of this research.

As we know that the privacy and integrity of data is very important when it is going to be sent or received from the providers. At the same time it is also very important to keep the integrity and privacy of data when it is stored at the data centers with providers. Data in cloud computing can be divided into three types, i.e. data in transit, data at rest, data in processing [15]. Each type of data requires a separate way to provide protection for that particular data. For example Secure Socket Layer (SSL) is used to provide protection to the data when it is in transit[16]. Protocols like AES, RSA, and SHA-256 are used when data is at rest[17].

2.4 Data Classification

If we closely analyze the data that is stored in the cloud, we will come to know that it is itself of different sensitivity nature. For example, most people generally hide their age (highly sensitive) but certainly like to announce their good educational record (less or non sensitive) and in the same way cloud clients wish to provide protection for their data.Also it is a general practice that attackers are more interested in sensitive data as compared to non-sensitive. In other words, it means security risk of data in cloud computing varies according to the sensitivity level of data [18]. Therefore, there is the need of such a scheme which handles sensitive data on priority basis, i.e. more sensitive data should provide better security as compared to less sensitive data. In this regard, too much work has not been done to the best of our knowledge and requires more to be done.

How data can be classified is a big question. There are various processes that can do this work for us e.g. manual processes that decides the sensitivity of data on case to case basis, location-based processes classify data based on client's or system's location. Similarly, application-based processes like database-specific classification, and on the other hand automated processes used by various technologies.

Application-based software by itself provides classification level. For instance Human Resource (HR) management, health record management and Customer relation management (CRM) tools can be confidential by itself. In **Data location-based** classification the location of clients or system becomes very important and decides about the data sensitivity e.g. data that is used or stored by the finance department or HR departments in various organizations are likely to be of a very sensitive nature.

Problem statement: Every individual's data have different privacy levels. Currently, to the best of our knowledge, CSPs do not consider sensitivity behavior of data and hence store it in the same manner as less sensitive data. It is important for both clients and cloud service providers (CSPs) to consider the following two questions.

Q1. Why not privacy and integrity should be provided to the data on the bases of its sensitivity by CSPs to achieve higher security level?

Q2. Why should not users pay to CSP on the bases of data security provided to their data?

These will be further helpful to explain our proposed model.

3. Related Work

"Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures"[19], is presented by Wassim Itani et al, and proposed Privacy as Security Service (PasS) through a set of protocols. They use Cryptographic Coprocessor(a small hardware card interfacing with main computer or server) for secure processing, storage and auiditing of user's data in the cloud. They applied trust based policy by dividing the data of a user on sensitivity bases i.e. No privacy, Privacy with Trusted provider, Privacy with Non trusted provider.

"Using encryption algorithm to enhance the data security in cloud computing"[1], is presented by Mandee Kaur et al, they have presented their theoretical model to make cloud data more secure and stated every bit of the data must pass to encryption framework, which is directed to / from the cloud. Encryption keys should not be stored in cloud cipher for the sake of security. According to their model the clientis given a choice to select an algorithm from many to encrypt the data for protection.

"3D security cloud computing using Graphical password "[20], proposed by MS SnehaVasant et al, they have presented 3D security technique to make cloud computing more secure. It divides the file or data and provides security in the form of graphical password for the three divided sections. There are three protection rings, in ring-1 the user interfaces with various objects. The user actions and interactions make 3D password. In ring-2 password is selected based on the icon. Ring-3 works on five points of images.

Jijo.S. Nair et al [2] proposed that encryption is not enough for it, but also steganography can fruitful in this regard. According to them data message is not only encrypted, but also hidden behind image to provide security to the data. Then this secure file (data) is uploaded to the data centers of the cloud and to maximize the availability of data, it is placed redundantly.

Saranya Eswaran and Dr.SunithaAbburu[21] presented their work based on TPA. They claim that their work will make cloud client able to check the integrity of data without accessing total file. Hence it will decrease network traffic and computation in a cloud environment. Here authorize users will store file(s) in cloud storage and will get secret key from the system. This secret key will be needed by the TPA for verification of that particular user data (file).

4. Proposed Model

As for Q1 is concerned, a user prioritize his data based on its sensitivity level. Accordingly the protection will be provided and the user will be charged by CSP (As there will be an agreement between client and CSP based on protection level to his / her data). For this purpose CSP provides an interface to the client, mentioning high sensitive, medium sensitive and non-sensitive data fields or options. The client data is protected according to the preference security level based on selections made by the client. A sample is shown in the Figure 2.

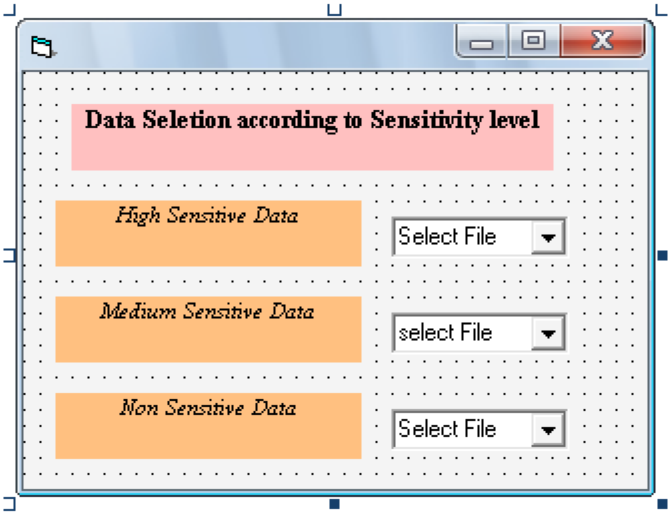

Figure2.A sample of user interface of the scheme

For simplicity here only three levels of data security are considered, namely they are high sensitive data, medium level sensitive data and non-sensitive. The number of levels can be increased or decreased according to need. Here high sensitive data requires more protection as compared to medium and non-sensitive data. Medium protection level data needs protection between high sensitive data and non-sensitive data. Nonsensitive data needs the least level of protection. Here data protectionis in the form of encrypting data using encryption algorithms. It can be of one of the eight modern encryption techniques, namely RC4 (RC stand for Rivest Cipher), RC6, MARS, Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple-DES (3DES)[15]. To reduce the transmission of huge data, non-sensitivity data may be sent to the cloud provider without encrypting it and then encrypted by the CSP with least secure structure.

Regarding Q2, the user may have to,comparatively pay higher charges to CSP due to the consumption of more resources of CSP in terms of encryption algorithm and some other facility. These facilities may be in the form of data availability such as having multiple copies of same data file for rapid provision and guarantee of data in case of loss. New Service Level Agreement (SLA) will be required between the clients and cloud service providers, as there will be different rates for different data security levels. In this way,aclient is given the opportunity to mention a part of his data as less-sensitive hence reducing the cost. Similarly, a CSP's resources will not be wasted on data that requires no security and will be utilized to improve its services by making the sensitive data more secure according to the expectation of clients.

4.1 Algorithm For The Proposed Model

The algorithm for the proposed model is
Switch(I)

```
{
        case 1:
                Apply lowest level of protection to the user mentioned part of his data.
        case 2:
                Apply the next protection level.
        ………………………………………………………………
        ………………………………………………………………
        ………………………………………………………………
        case n:
                Apply most powerfulprotection level to the user mentioned part of the data.
}}
```

Where "I" represents the type of security level that client wants for protecting certain part / file of his data. It takes values ranging from 0 to n. 'n' means highest level of security and '0' lowest security level of user data.

4.2 Implementation And Discussion

In this section the process of implementation has been discussed. This scheme is tested locally and experiments have been conducted in a local file setting which provide evidence that this approach may provide efficient data security in a Cloud environment.

This scheme is tested for two categories of data, i.e. CuricullumVitae (CV) and health record of a person. Health record has been given the highest protection priority and lowest protection provided to CV. Because AES provides better security in comparison to DES [22], that's why AES is applied to Healthrec.txt and DES is applied to CV.txt.

In **Comparison** to normal adopted procedure in which all the data is stored with the single encryption scheme this scheme may provide more security as shown in the Figure 3.

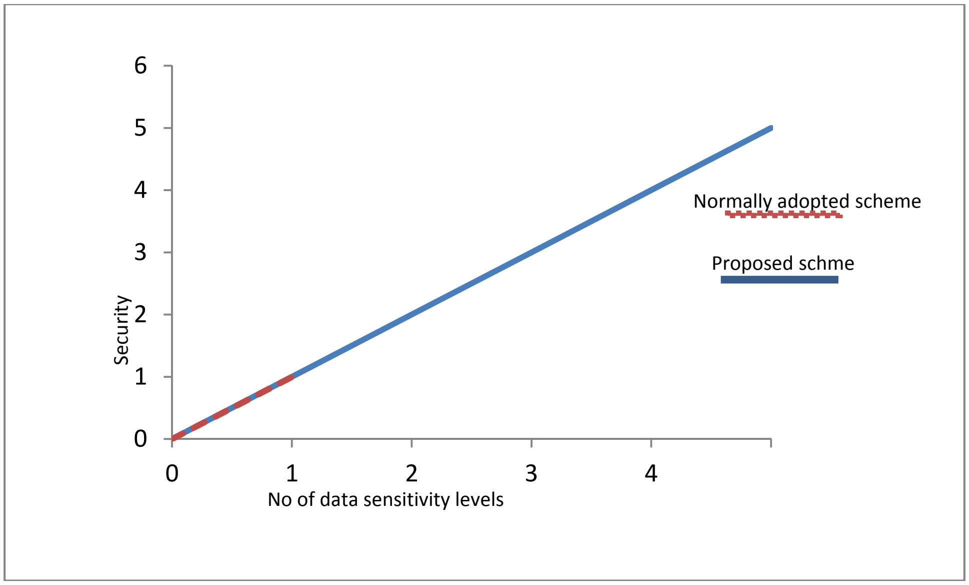

Figure 3. Comparison of proposed scheme with normally adopted schemes

Also this scheme will make data more and more secure as the attackers have to break the security of each category as we have divided the data into different categories and encrypted each one with different encryption algorithms, as compared to a single type of data. Therefore, the attacker will have to come with different schemes to decrypted different categories of data, which is never an easy task. For example, after a single breach an attacker is able to gain control of whole data of a client, when data is not categorized. The attacker will have to break the security of both categories if the client data is categorized into two types. In case when data is divided into three categories, it will require three different schemes for attackers to decrypt all the three categories of data and so on. This means that there is a direct relationship between Security of data and no. of levels (categories) of data.

Let ‘X’ represents the number of categories i.e. sensitivity levels of user’s data and ‘Y’ represent the number of required security breaches for decryption of all sensitivity levels of data of clients’. The relationship between ‘X’ and ‘Y’ can be shown mathematically as

$$Y=X$$

From the Figure 4 it is clear that when there is no data no data breach is needed. When data is not categories, only one breach will be required and for two categories two breaches will be needed and this direct relationship is shown in the above graph. As for n levels of security, according to the above given relation, will require n attemps to get access to the data but we believe that 3-5 levels will be more practical.

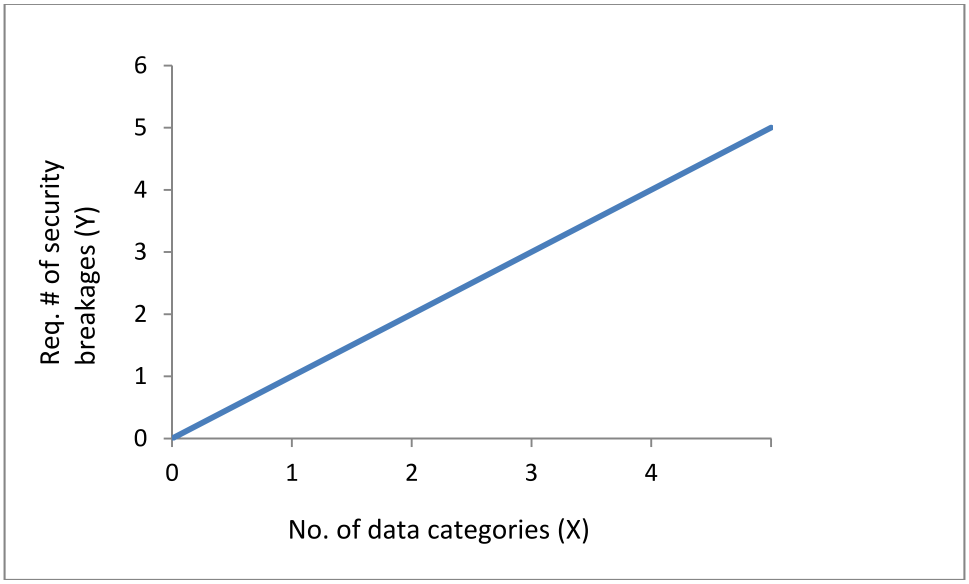

Figure 4.No. of data categories Vs Security breakages required for attacker

4.3 Benefits Of the Proposed System

- One of the benefits of this approach that client is also taking an active part in giving protection to his own data according to the need and the same is also mentioned by [6].
- Organization will give more time to secure sensitive nature data. Therefore the security of important data will improve.
- More clients will join the cloud as they now see that their sensitive data is now more secure.
- Clients have now a range of security levels in front of them and know the cost of it after a particular level of security is selected by the client for its data.

5. Conclusion

Although cloud computing provides many advantages to its clients, there are still many challenges to be addressed especially security, privacy and data integrity. Data security is one of the most important issue in cloud computing. Most of the approaches currently used, to the best of our knowledge, have not considered data categorization on the basis of its sensitivity to the user. Our proposed scheme categorize data on the basis of its sensitivity and then applies a suitable encryption algorithm. This scheme will make the job of the attacker more and more difficult as he / she has to break the security of each category of data to fully understand the whole data, thus helping the users to save their sensitive data more effectively. Similarly, CSPs can utilize their resources efficiently instead of applying security techniques on data that requires no security. Currently, our proposed scheme takes sensitivity levels manually from a user. In future, we will be focusing on developing a system where the sensitivity level of data will be captured automatically.

REFERENCES

[1] Kaur, M., & Mahajan, M. (2013). Using Encryption Algorithms to enhance the data security in Cloud Computing. *International Journal of Communication and Computer Technologies*, *1*(12).

[2] Nair, J. S., & Roy, B. Data Security in Cloud Jijo. S. Nair, BholaNath Roy.

[3] Sravan Kumar, R., &Saxena, A. (2011, January). Data integrity proofs in cloud storage. In *Communication Systems and Networks (COMSNETS), 2011 Third International Conference on* (pp. 1-4). IEEE.

[4] " http://www.nist.gov/itl/csd/cloud-102511.cfm," 10-01-2015.

[5] A. Iqbal, H. U. Rashid, and M. Khattak (2015). Enhanced Secure Model for Single Sign-On Across Open Cloud Federation, *International Journal of Computer Science and Telecommunications,* pp. 22-26.

[6] R. A. Lumley (2010). Cyber Security and Privacy in Cloud Computing: Multidisciplinary Research Problems in Business.

[7] Reddy, G. R., & Raju, M. B. Augmentation Data Security Aspects of Cloud Computing.

[8] Maddineni, V. S. K., &Ragi, S. (2011). Security Techniques for Protecting Data in Cloud Computing. Electrical Engineering.

[9] Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on* (Vol. 1, pp. 647-651).IEEE.

[10] F. Sharif and A. Hafeez (2012). The Analysis of Cloud Computing Major Security Concerns & their Solutions, *Journal of Information & Communication Technology,* pp. 48-53.

[11] M. Paul.Security in the Skies Cloud computing security concerns, threats, and controls.

[12] N. Ramdeo (2012, September). Evaluation of Data Encryption Algorithms, *International Journal of Scientific & Engineering Research.*

[13] Song, D., Shi, E., Fischer, I., & Shankar, U. (2012). Cloud data protection for the masses. *Computer*, (1), 39-45.

[14] F. Sabahi (2011). Cloud computing security threats and responses, *2011 IEEE 3rd International Conference onCommunication Software and Networks (ICCSN),* pp. 245-249.

[15] Mohamed, E. M., Abdelkader, H. S., & El-Etriby, S. (2012, May). Enhanced data security model for cloud computing. In *Informatics and Systems (INFOS), 2012 8th International Conference on* (pp. CC-12).IEEE.

[16] Du meng(2013), Data security in cloud computing, in *8th International Conference on Computer Science & Education (ICCSE)*:, 2013, pp. 810-813, IEEE.

[17] https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet, accessed on 07-12-2014.

[18] K. T. James A. Lewis (2011). Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization, White paper,Center for Strategic and International Studies (CSIS).

[19] W. Itani, A. Kayssi, and A. Chehab (2009). Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures, *Eighth IEEE International Conference onDependable, Autonomic and Secure Computing, 2009. DASC'09.*, pp. 711-716.

[20] Thakare, M. S. V., & Gore, M. D. V. 3D Security Cloud Computing using Graphical Password.

[21] Eswaran, S., &Abburu, S. (2012). Identifying data integrity in the cloud storage. *International Journal of Computer Science Issues (IJCSI)*, *9*(2), 403-408.

[22] M. A. Wright (2001), "The advanced encryption standard," *Network Security,* pp. 11-13.