INNOVATIVE APPROACH ENSURING SECURITY AND PRIVACY IN CLOUD COMPUTING

R. Masood and M.Aslam

Department of Computer Science and Engineering, University of Engineering and Technology Lahore.
Corresponding Author; E-mail;rabi.ravian@gmail.com

ABSTRACT: Many organizations had been keeping their data on the clouds. The trend nowhas been shifted from the pre-reservation of resources to store, manage and process data on clouds. In the information technology, the most challenging task isthe security of data and to avoid technical and internal failures and attacks of unauthorized accesses. Consequently, the emphasis of this study was toimplement Honey Encryption (HE)that offered more confidentiality and flexibility against the brute force attacks. HE ensured that the message that wasdecrypted with false keys, which looked like a valid key, so it was difficult to differentiate between authentic and unauthentic data. This study providedthe confidentiality of data and maintained consistent relations integral in the cloud. It empowered the user to perform computation and storage tasks withoutrevealing data innards.

Keywords: Cloud computing, honey encryption, data management, data privacy, data security and symmetric encryption.

(Received 01-06-2015 Accepted 04-02-2016)

INTRODUCTION

In this study, the security solution on clouds has been proposed. A Secure Repository Manager (SRM) at server and client systemscreated a secure repository. This SRM has used for cloud-based applications for security and privacy whereas Honey encryption is used for implementing security. Honeys encryption utilizes public key encryption. SRM uses theauthentic key for data decryption. The Public key encryption is used in the honey encryption process so that the data is unable to decrypt and it is safe from theft, breach, and inside attacks(Juels and Ristenpart, 2014).

After honey encryption process the SRM uses an algorithm which divides that data into small chunks. Furthermore, metadata of the chunks is stored in SRM and chunks are uploaded on multiple cloud servers. Information of distributed cloud servers is saved in SRM.For data retrieval, SRM algorithm is used. It gathers all the relevant information about data and keys and decrypts the data. Information about the data is stored in SRM i.e. key, number, size, order and location of data chunks(Kaur and Kinger, 2014).

In a studyKaurand Mahajan, (2013) reported thatdifferent algorithms have been devised for the security of cloud computing, but these security algorithms and models may fail to secure data properlyi.e.DES, DES3, BLOWFISH, RSA, and MD5. The idea of hardware encryption has been presented for security of data, but it is not efficient, because it is hard to implement for cloudsEncryption, which is a widely used technique to encrypt and protect data over the network and it is also good to encrypt data by using a symmetric key algorithm, (Kaur andKinger, 2014).It is further reported that for computer security,the honey word is used to prevent counter attacks of a system(Tyagi *et al.*, 2015).

Finally,the addition and contribution isencryption and chunking process to protect data over the network using honey encryption and is using the symmetric key algorithm.According to Voris *et al.*, (2012)Honeypots are the servers for the security of the data, they generate honey words from wash tables which seem similar to the real passwords. So these honey words can help in finding security breakage.

MATERIALS AND METHODS

According to the literature survey for privacy protection and data security issues, it was predictable to have an incorporated and complete security explanation to collect the requirements of protection in strength.

Concerning the data identification, the isolation and privacy protection was the most important factor. While designing the cloud-based applications, these issues should be measured. Data was not saved directly on the clouds, if this would happen without any security or privacy the user's data would easily be altered or hacked.So, in this study, the solution of a Secure Repository Manager (SRM) on the serverswas proposed. Cloud-based applications used that secure repository manager, to handle its security and privacy, honey encryption was implementedas is shown in Figure- 1.

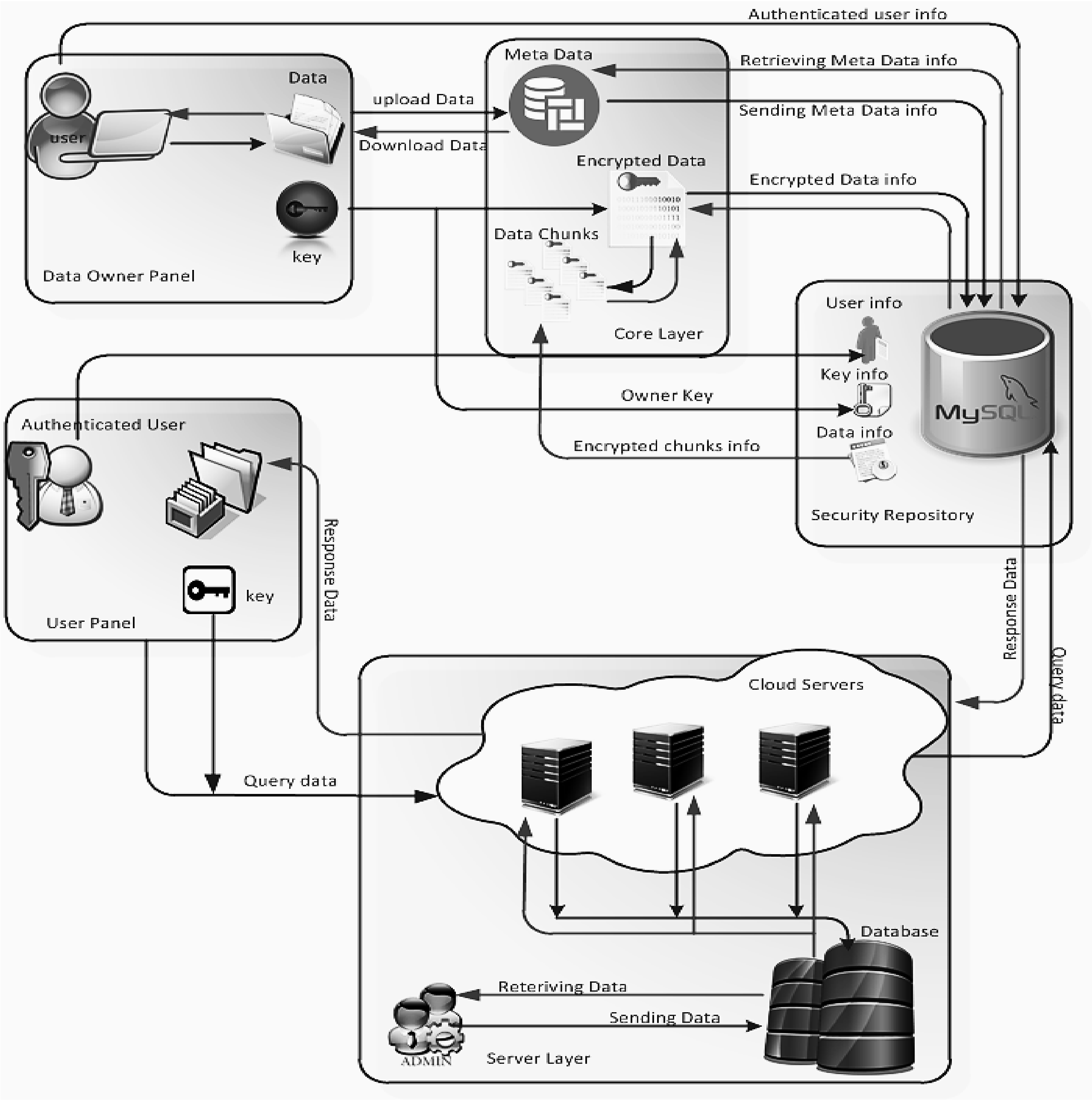

Figure-1 Cloud Computing Encryption Architecture

Thepassword based encryption was considered as a weak encryption because it was easy to decrypt using brute force attacks. The honey encryption was a new way to protect data. After honey encryption, hackers could get no information from the servers, because of honey pots. Honeypots generate honey words, which looked similar to the valid data, but it was difficult to differentiate between valid and invalid data.

If it was detected that the honey words were being used, then it means that the security was compromised and someone was attacking the system. The system could store the information about the attacks and it should be looked intoso that the next attacks could be avoided. Honey encryption was similar to the Format-Transforming Encryption (FTE) and Format-Preserving Encryption (FPE).

Both of these encryption plans had specific limitations for the message and cipher text spaces. In FPE, the cipher text space was the same as the message space. In FTE, the cipher text spacewas specified and wasdifferent from the message space. These encryption plans gave the comparative security results to honey encryption when utilized with uniform message spaces. The honey encryption offered better security for nonuniform message spaces, since it was not bound to mappings between the two message spaces but rather utilized a mapping between a message space and a much bigger seed space.

Honey encryption was applied to the data which needed to be encrypted, it utilized public key encryption. The main idea of implementing this feature was to upload data on the clouds in encrypted form, instead of being insecure on the clouds and keeping data safe from hackers. All the functionalities and methodologies were implemented on encrypted data.The SRM decrypted the data with authentic key only to make sure, that the encrypted result was correct. When public key encryption was applied to honey encryption process,then as a result, the hacker would be unable to decrypt the data and the data would be secure from theft, breach, and unauthorized access.

After encryption of data, the next step of SRM was to use an algorithm to divide encrypted data in chunks. The chunk size was dependent on the level of security. If data was private and highly sensitive, then the chunk size would be smaller, and If the data was average secure then the chunks would be of medium size and if the data was public and less secure then the chunks would be of large size. Information about all these chunk sizes and sequences were stored in the privacy manager. In this study,chunksize of 1024 KB wasused for experimentation.Afterward, the proposed system stored these data chunks at random locations or on the cloud servers at user's choice. Locations, where data was saved, could be anywhere or on any server. The location and server information was saved in the SRM.

If a client requested for the data retrieval, the SRM algorithm was then activated. It gathered all the necessary information i.e. key, chunk sequence and location from SRM at client-side so that data could be decrypted and kept in order to maintain its original form while retrieving. In this process of delivery, data could be damaged. To avoid these damages a secure connection be used to prevent damage, stop the use of HTTP, TELNET and give permission to get through HTTPS and SSH for encoded communication. With righteous verification and calculation, changes could be avoided in the data of clouds. If data was damaged, then the requestwas resent to the cloud server, so that client could have data in original form.

RESULTSAND DISCUSSION

In a study conducted by Juels and Ristenpart (2014) described honey encryption where all messages were kept in a message space. A Distribution-transforming encoder (DTE) was used to map these messages on seed space S. Few information was needed to map DTE seed ranges, especially cumulative distribution function (CDF). The Honey encryption process ispresented in Figure- 2.

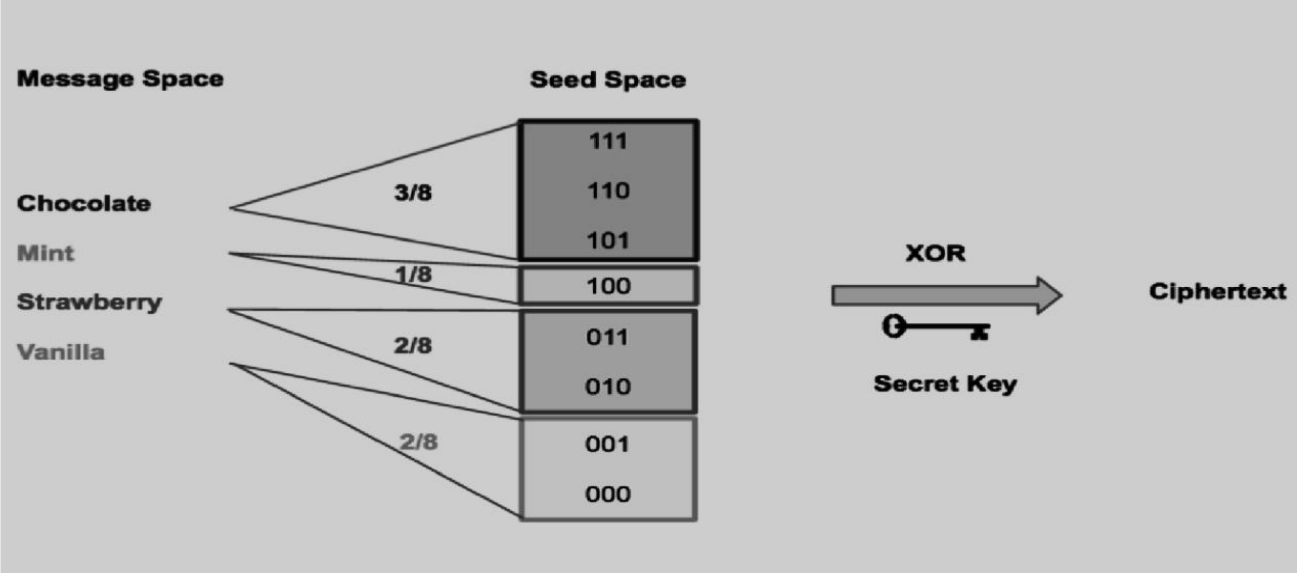

Figure- 2 Honey Encryption

Symmetric encryption was used to produce a cipher text C from a seed S. SRM was used to store and exchange keys without any interruption. In this construction, public key encryption was used instead of asymmetric key. Let's assume Distribution transforming encoder DTE = (encode, decode) which produced seeds space S = {0,1}s, and PKE = (enc, dec) was a public key encryption with some cipher text space C and message space S. RSA as a public key encryptionhas been used. The DTE is defined as HE[DTE, PKE] = (HEnc, HDec) encryption process. Firstly, it puts on DTE encoding and then encrypts the seed space S using public key encryption.

The Decryption was exactly a reverse order of it. First, decryption using public key I applied and then DTE, just like symmetric encryption. If PKE was secured, then the scheme was secured.

This study ensured that this PKE-based honey encryption shared the very same security limits as demonstrated by (Juels and Ristenpart, 2014)for symmetric based honey encryption [4]. This study showed that encrypted uniform messages can provide uniform cipher text.Also, it was accepted that s ← S;c ← enc(k,s) and c ← C;s ← dec(k,c) which yielded indistinguishable circulations for all k ∈K. This presumption equally held for some PKE plans, thus, this could be utilized in any of these and land at indistinguishable security limits, as honey encryption plans with symmetric keys. This development to standard honey encryption plans permitted thecustomers to effect significantly pass and store encoded data, without the requirement for a protected channel of key correspondence or key storage components.

Security repository manager database: Security Repository Manager contains information about thefile, i.e.file id, file size, file encryption key, file chunks and file uploaded cloud server path. Different information stored in the database is shown in the Figure-3.

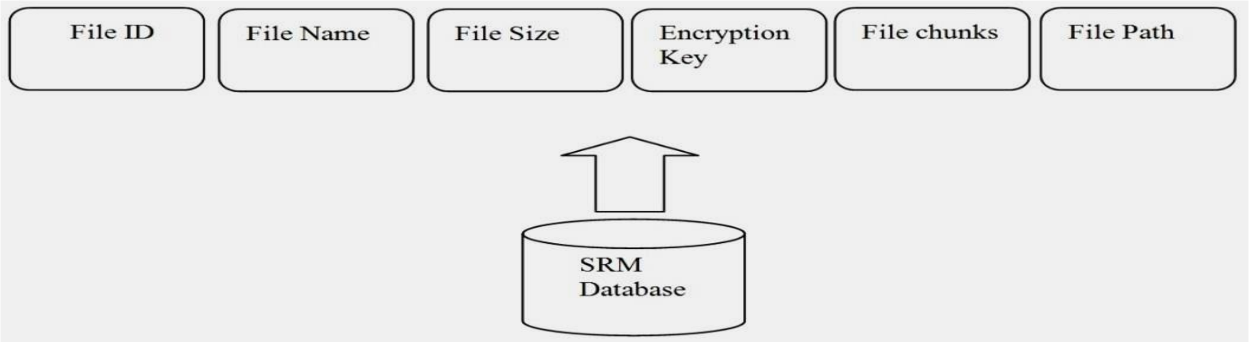

Figure- 3 SRM Database

The proposed idea, that meets the intention to provide thesecurity method and it made the messages secure by encrypting, chunking, and uploading on different servers as is shown in Figure- 4.

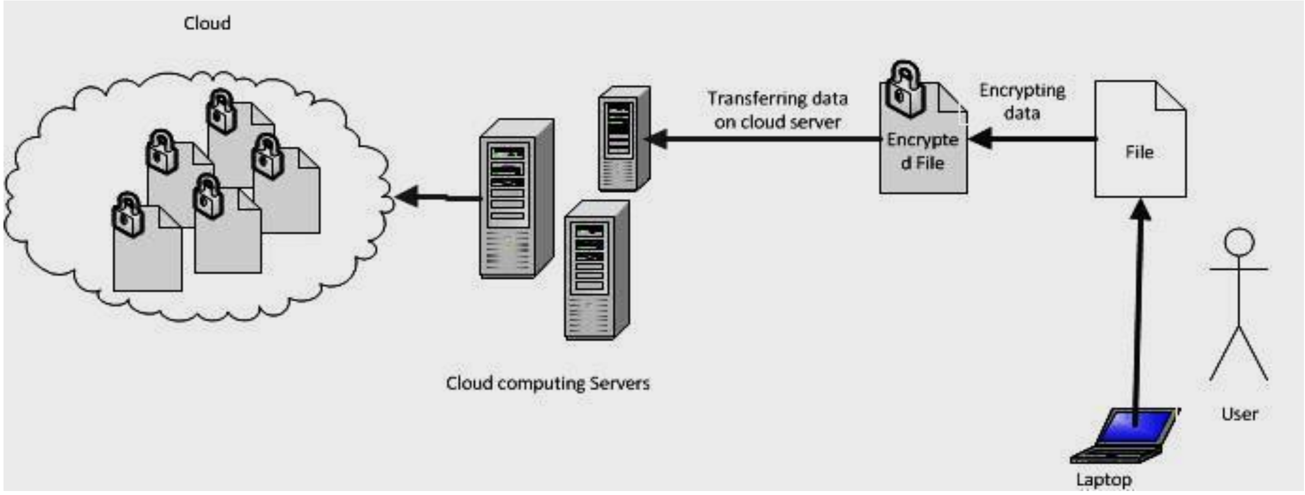

Figure-4 File Upload Procedure

The latest advancement of honey encryption offered numerous password based security plans, flexibility to brute force offline assaults by yielding conceivable plaintexts, which were decoded by invalid keys. Honey encryption has been presented for encryption purpose. Specifically, the key testhas been tended for creating conceivable honey messages for each of these spaces by looking into the probabilistic dissemination of the message spaces and developed great DTEs for each. Additionally, augmented the base honey encryption plan to support PKE, and demonstrated that this augmentation keeps honey encryption's security high.

After the Encryption file size wasincreased and the number of chunks of encrypted file was also increased as is shown in Table- 1.

Table-1. File size before and after encryption.

File	File Size (KB)	Encrypted File Size(KB)	Number of Chunks	Key size(bit)
1	14.8	30.1	1	16
2	100	225	1	16
3	200	1300	2	16
4	446	32500	3	16
5	800	7100	7	16
6	1000	8500	9	16
7	2000	15000	14	16

Encryption of these messages was done while uploading and decryption was done while downloading them on any machine by authenticated users only. Only authenticated users had the key for decryption. The results achieved in this studywere found through the Data Encryption Standard algorithms. It was implemented in Java, and Net BeansIDE was used for developmental purposes. Roughly client-server architecture was created to implement this study. Encryption approach was used by few researchers i.e.(Tebaa *et al.*,2012 andKaur and Kinger, 2014), but the messages were not encrypted. Encryption was found to decrease the risk of insider attacks. Finally outlines of proposed algorithms for file uploading and downloadingis presented as under.

File upload pseudo

```
•   Authenticate
user $\alpha \rightarrow \beta$  $\alpha$ sends an access request  message
•   If authentication successful, $\alpha_{\mathrm{REC}} = \{\mathrm{id}, \mathrm{dac}, \mathrm{key}\}$
•   Create a secure connection: HTTP:
•   The user selects a file to upload to the cloud
•   The user was required to enter password
•   File encryption ʜᴇ[ᴅᴛᴇ, ᴘᴋᴇ] = (ʜᴇŋc,ʜᴅẹc )
•   Encrypted file was converted into chunks
•   Chunks were uploaded to cloud servers
•   The session was closed if chunks have been uploaded successfully.
```

File download pseudo

```
•   Authenticate
user $\alpha \rightarrow \beta$  $\alpha$ sends an access request  message
•   If authentication successful, $\alpha_{\mathrm{REC}} = \{\mathrm{id}, \mathrm{dac}, \mathrm{key}\}$
•   Create a secure connection: HTTPS:
•   The user selects file, which He/she needs to download from the cloud
•   The user enters keyᴅẹc $(\kappa, c)$
•   Chunks were gathered and joined
•   The file was decrypted $c \leftarrow C$; S←ᴅẹc $(\kappa, c)$
•   The file was downloaded to the user's device
•   The session was closed if file download was successful
```

Experimental parameters and settings: Java Platform was used for experimentation. The Honey encryption methodology was used for testing and experimentation in the cloud architecture. Further details are shown in Table-2.

Table 2. Parameters and settings for study

Operating System	Microsoft® Windows® 7
HDD	250 GB
RAM	4 GB
Simulation	JAVA SE 7
Simulation Tool	Net Beans IDE
Communication	Wireless
Communication through	Client Server Architecture
Upload Speed	300kbps
Download Speed	500kbps

According to Mei *et al.* (2008), a lot of advantages wereachieved by service and pervasive computing in cloud computing. In a study(Rubóczki and Rajnai, 2015), showed the solution of security and privacy breaching. They created a privacy manager which managed user's data and made it secure on the clouds. The main concern was observed to store private data on clouds in an encrypted form instead of normal form.

The core idea of (Pearson, 2009)was found in hisstudy, which was client based. Trusted computing was used to enhance obfuscation method. According to the studies carried out by(Abadi, 2009) it was reported that database normally costs high in both hardware and software, so data management applications were good for use in the clouds. In a study conducted by(Vesset, 2006) reported that a research conducted by Yahoo and Microsoft in which cloud computing propertieswere implementedi.e. Pig Project and SCOPE.Another technique wasused by(Dean and Ghemawat, 2008), which was in map reduced form and Tplatform form.(Dillon*et al.*,2010), trusted computing encrypts the data and seals all other applications. After sealing it sends decryption keys to the trusted programs and applications only. Also, according to Peng*et al.*,(2009), trusted computing contained conventional behavior in approximately every operating system and it resistedthe viruses and physical interference by any means or applications. A security system for cloud computing proposed by Nafi *et al.*, (2012) established secure communication among nodes and it encapsulated information from other users. Another security system proposed by Tebaa *et al.*, (2012) devised a method to perform operations on encapsulated data. This data gave the similar results as the operations were applied to raw data and encrypted data. In another study,Patial and Behal, (2012) reported that security issue in cloud computing wasthe main concern. The data which was encrypted was grounded in the key of RSA algorithm. If this private key was known to the unauthorized user then the data could be decrypted,(Aoun*et al.,*2013).

In this study, solution for security in cloud computing infrastructurewas discussed. A security repository manager was created for implementing security, SRM implementedan encryption feature an thenencrypted data uploaded on the cloud database. So encrypt data on the clouds was hard to understand and all the functionalities were implemented on encrypted data. But, still there were many issues which needed to be resolved and these methods needed to be matured so that security risk could be reduced.

Conclusion: A lot of work needs to be done to make users satisfied about the security of cloud computing.This study elaborated the distinguished feature about security and privacy. The data which was uploaded on the cloud platform from client machine was encrypted using Honey encryption and DESencryption function in Java. Encryption methodology was used to avoid insider malicious attacks in cloud architecture.In future, other encryption techniques with different encryption algorithms would be tested, i.e Riveset Cipher, AES. Moreover, similarity and comparison of different features were discussed under different security architectures and alternate cloud services and model of cloud security.

REFERENCES

Abadi,D.J.(2009). Data Management in the Cloud: Limitations Opportunities. IEEE Data Eng. Bull. 32(1): 3-12.

Aoun, R., C.E.Abosi, E. A. Doumith, R. Nejabati, M.Gagnaire and D. Simeonidou (2013). Towards an optimized abstracted topology design in a cloud environment. Future Generation Computer Systems. 29(1): 46-60.

Dean, J., and S. Ghemawat(2008). MapReduce: simplified data processing on large clusters. Communications of the ACM. 51(1): 107-113.

Dillon, T., C. Wu and E. Chang (2010, April). Cloud computing: Issues, challenges. In Advanced Information Networking Applications (AINA), IEEE International Conference on. 24 (1): 27-33.

Juels, A., and T. Ristenpart (2014). Honey Encryption: Encryption beyond the BruteForce Barrier Security Privacy. IEEE.12(4):59-62, 293-310

Kaur, G., and M. Mahajan (2013). Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms. IJERA. 3(5): 782-786.

Kaur, R., and S. Kinger (2014), Analysis of Security Algorithms in Cloud Computing.IJAIEM.

Mei, L., W. K. Chanand T. H. Tse (2008). A tale of clouds: paradigm comparisons some thoughts on research issues. APSCC. IEEE. 464-469

Nafi, K. W, T.Shekha kar, S. A.Hoque and M.M.A Washem. (2012). A Newer User Authentication, File Encryption Distributed Server Based Cloud Computing Security Architecture. Int. J. Adv. Comp. Sci. App.

Patial, A and S. Behal (2012). RSA Algorithm achievement with Federal information processing Signature for Data protection in Cloud Computing.Int.J.Comp.Tech.

Pearson, S., Y.Shen, and M. Mowbray (2009). A privacy manager for cloud computing. Springer Berlin Heidelberg. 90-106

Peng, B., B. Cui and X. Li (2009). Implementation Issues of a Cloud Computing Platform. IEEE Data Eng. Bull. 32(1):59-66.

Rubóczki, E. S., and Z. Rajnai(2015). Moving towards Cloud Security.INDECS.13 (1): 9-14.

Tebaa, M., S.El Hajji and A. El Ghazi (2012, July). Homomorphic encryption applied to the cloud computing security. WCE. 1(1):4-6.

Tyagi, N., J.Wang, K.Wen, andD.Zuo (2015). Honey Encryption Applications, Network Security.

Vesset, D. (2006). Worldwide data warehousing tools 2005 vendor shares. Technical Report, IDC. 203229.

Voris, J.,N. Boggs, and S.J. Stolfo(2012). Lost in translation: Improving decoy documents via automated translation. In IEEE Symposium on Security and Privacy Workshops (SPW). 129-133.