VOL. 11, NO. 9, MAY 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

STUDY ON SECURITY FRAMEWORKS AND DATA PROTECTION TECHNIQUES FOR PUBLIC CLOUD ENVIRONMENT

K. Meena[1] and M. Gomathy[2]
[1]Bharathidasan University, Trichirappalli, Tamilnadu, India
[2]Department of MCA, Shrimati Indira Gandhi College, Trichirappalli, Tamilnadu, India
E-Mail: drkmeena@gmail.com

ABSTRACT

Cloud computing provides computing resource in an on-demand manner. It is provisioned resources from huge data centers situated in different geographical locations in the world. It mainly supports small and medium scale enterprises to startup their business in globally. It has many advantages in resource provisioning and other services but it also has some security related problems. Cloud enables outsourced computing. The nature of outsourced computing brings up many security issues in cloud environment. Due to the security issues in cloud, users are not willing adopt the cloud. This paper presents an elaborated study on different security framework and data protection techniques in cloud environment. Each framework works on their functionality and address security issues in public cloud environment. Finally, paper discusses results of each framework and data protection techniques.

Keywords: public cloud, cloud computing, security, data protection.

1. INTRODUCTION

Cloud computing is a developing computing technology that uses the internet and multiple remote servers to maintain data and software applications [1]. Storage and maintenance of data are the most important task in all kinds of enterprises. Data storage in an enterprise involves high costs because it requires physical IT resources like servers, storage, operating system and network etc., and frequent management procedures like backup, tuning, etc. and skilled administrative experts for monitoring the whole data storage administration process [2]. This would increase the enterprises uncertainly with respect to storage and maintenance of the data [3]. The best solution for data storage and maintenance is data outsourcing in cloud environment [4]. The data are outsourced to CSPs, and then CSPs take care of the data within their own specialized structure to offer high availability and disaster protection. Cloud data outsourcing faces many issues especially in security aspects [5].

Cloud computing brings out a wide range of benefits including configurable computing resources, economic savings, and service flexibility [6]. However, security concerns are shown to be the primary obstacles to a wide adoption of clouds [7]. The new concepts that clouds introduce, such as multi-tenancy, resource sharing and outsourcing, create new challenges to the cloud data security. To address these challenges, it is necessary to tune the security measures developed for traditional computing systems and proposing a new security policy, models and protocols [8] for cloud.

Khalil *et al*., [9] provides a comprehensive study of cloud computing security concerns and identify cloud vulnerabilities. Vulnerabilities are classified into security threats and attacks. It is important to control the vulnerabilities, neutralize the threats, and calibrate the attacks.

2. CLOUD SECURITY FRAMEWORKS

Security enables cloud as a safe and secured environment to the users; it restricts many of the attacks on the data from hackers. There are number of security framework were proposed by different researcher. This section describes the security framework.

Kamara *et al.,* [10] proposed a cloud data storage framework for public cloud. The framework consisted of four components, namely, a Data Processor (DP), that processes data before they are sent to the cloud; a Data Verifier (DV), that checks whether the data in the cloud have been tampered with; a Token Generator (TG), that generates tokens which would enable the cloud storage provider to retrieve segments of customer data; and a Credential Generator (CG) that implements an access control policy by issuing credentials to the various users. This framework is designed in the scenario for both general and enterprise users. In the case of general users' scenario, they install the components of the framework that consists of a DP, a DV and a TG into their local machine. In the case of enterprise users' scenario, Medium-sized enterprises deploy dedicated machines within their network including a DP, a DV, a TG and a DG. If enterprises are very large, the prospect of running and maintaining dedicated machines to process all employees' data are infeasible. More precisely, in this case the dedicated machines only run data verifiers, token generators and credential generators while the data processing is distributed to each employee. In this framework, users have to maintain the components like DP, DV, TG and CG. Cloud is used only for storing the data. Users have the maximum responsibilities to execute this framework.

Yau *et al*., [11] presented an approach to secure the users' data from service providers. The approach contained three main parts, 1) separating software service providers, and infrastructure service providers, 2) hiding data owners' information in cloud and 3) data obfuscation. The approach consisted of seven entities namely, Software

Cloud, Infrastructure Cloud, Software Service Broker, Infrastructure Service Broker, Software Service Attestation Authority, Data Obfuscator and Data De-obfuscator. The Software Cloud and Infrastructure Cloud have the same features of the software layer in ordinary cloud computing architecture. However, the software layer and infrastructure layer are not managed by the same service provider. The Software Service Brokers and Infrastructure Service Brokers have the same functionality of the service brokers in Service Oriented Architecture (SOA), but they have the additional function for identity Anonymization. The Software Service Attestation Authority, Data Obfuscator and Data De-obfuscator are additional entities in this approach.

Atiq ur Rehman *et al*., [12] proposed a framework to preserve confidentiality of data stored in Cloud Database as a Service (DaaS) model. The proposed framework stores sensitive data with a combination of encryption and obfuscation techniques. The framework consists of four modules namely, Encryption, Obfuscation, Metadata and Query optimizer. Encryption and obfuscation are used to encrypt and obfuscate the data respectively. Encryption and obfuscation are done before sending the data to the cloud DaaS. Metadata is maintained by cloud users for storing details of keys and for encryption and obfuscation techniques. Query optimizer is used to enable users' query to run on the encrypted and obfuscated data in the cloud storage. The four modules in the framework are executed from the users' side. Cloud users have more responsibility to generate the key and also to keep the key secured.

Basescu *et al*., [13] proposed a generic security management framework allowing providers of cloud data management systems to define and enforce complex security policies. They have designed the framework to detect and stop a large number of attacks defined through an expressive policy description language and to be easily interfaced with various data management systems. They have showed that they could efficiently protect a data storage system by evaluating their security framework on top of the BlobSeer data management platform [14]. The benefits of preventing a DoS attack targeted towards BlobSeer were evaluated through experiments performed on the Grid5000 test bed [15].

Govinda *et al*., [16] proposed an agent-based security framework for ensuring security. It helps users to control their sensitive information, and also ensures that the users have fewer burdens at their side. It assists the users by communicating their security related preferences to the service providers and assists the service providers in compliance with security law and regulations. An essential feature of agent-based security is obfuscation, used by users to protect the security of the data. Agent should control two entities namely; Obfuscator that obfuscates the data sent by user to the cloud, Data Retriever that retrieves the data sent by cloud to users. Agent could automatically obfuscate some or all the fields in a data structure before they are sent off to the cloud for processing, and translates the output from the cloud back into de-obfuscated form. The obfuscation and data retrieval are done using a key which is chosen by the agent and not revealed to CSP. Simple obfuscation technique can easily be broken. There is a need for proper SLA among users, agent and cloud providers.

Arokiam *et al.*, [17] framework for cloud data storage security to ensure the confidentiality of data stored in cloud storage. Framework has three services for security and key and storage. These three services are provided as a service to user from three different Cloud Service Providers. Security service has three different security service algorithms for encryption and obfuscation. Encryption and obfuscation are executed for specific type of data like numerical and non-numerical. Users have to select the specific security service from the framework then the encryption or obfuscation is processed. The key used for the security service algorithms are generated in key generation and management as a service. Generated keys are forwarded to users by the IP address given by security service. Keys are not communicated to any other csp providing services in cloud environment.

Munir *et al.,* [18] proposed a cloud security framework that identifies security challenges in cloud computing. The framework contains the following components. 1) *Client*: Users could access the client side with Multi-Factors Authentication (MFA) provided by End-User Service Portal (EUSP). 2) *End-User Service Portal*: When clearance is granted, a Single Sign-on Access Token (SSAT) could be issued using certification of user. Then the access control component shares the user information related with security policy and verification with other components in EUSP and CSPs. 3) *Single Sign-on (SSO)*: It enables user to access multiple applications and services in the cloud computing environment through a single login. 4) *Service Configuration:* The service enabler makes provision for personalized cloud service using user's profile. 5) *Service Gateway and Service Broker:* A service gateway manages network resources and VPN on the information lifecycle of service broker. 6) *Security Control*: It provides significant protection for access control, security policy and key management against security threats. 7) *Security Management*: It provides the security specification and enforcement functionality. 8) *Trust Management*: It is a challenging need of integrating requirements driven trust negotiation techniques with fine-grained access control mechanisms. 9) *Service Monitoring*: An automated service monitoring system guarantees a high level of service performance and availability.

Hamdan Al-Sabri *et al*., [19] proposed Cloud Storage Encryption (CSE) architecture by using encryption techniques to provide a high level of data protection to cloud storage. The CSE architecture allows to encrypt and to index data in a manner that ensures the protection of data. The proposed architecture is composed of seven components. 1) *Director generated Keys and privileges*: A center within the organization to generate public and private keys for data users, as well as granting special privileges to the suitable roles inside the organization. 2) *Data users*: Clients or employees within the organization. 3) *User Roles*: It determines the

characteristics and privileges for users. 4) *Encryption Point*: It is used to encode and index the data and divide data into several packages. Each package is stored in different cloud servers. A specific code is included in the divided packets, so that it can be assembled during the retrieval. 5) *Searchable Encryption*: It is a technique to search for the encrypted data during the retrieval of data from cloud storage without decryption. 6) *Decryption Point*: It is used to decode the encrypted data retrieved from cloud storage. 7) *Cloud Data Storage*: Databases for data storage. Users should maintain this architecture with all components. It increases the user encumbrance.

3. DATA PROTECTION TECHNIQUES

To protect the data in the cloud storage, the following data protection techniques are reported, i) Data encryption [20] [21] and ii) Data obfuscation [16] [22] [11] [23].

The goal of these techniques is to store data on the cloud servers in an inaccessible format using encryption and obfuscation. Encryption is the procedure of transforming the data from readable form into unreadable form using a cryptographic algorithm and a key. Obfuscation is a method that masks the users' data from illegitimate users by implementing a specific mathematical function or using programming methods. The major difference between encryption and obfuscation is that encrypted data cannot be processed until they are decrypted, whereas obfuscated data can be processed without de-obfuscation.

A. Data encryption

Data encryption is a traditional technique for ensuring the confidentiality of data in transit or data at rest [24]. Cloud providers should use the data encryption based on their own internal structure. It is not sure that all the providers should absolutely encrypt customer's data. For example, EMC's Mozy Enterprise does encrypt a customer's data. However, Amazon Web Service (AWS) S3 does not encrypt a customer's data. Customers are able to encrypt their own data prior to uploading, but S3 does not provide encryption [25]. This leads to the data confidentiality issue in cloud storage. Users do not know whether the data are encrypted in the cloud storage or not. Users should encrypt their data before they are uploaded to the cloud storage [26]. Many researchers have proposed different encryption algorithms for security of data in cloud. From the literature review, the symmetric encryption algorithm is suitable for cloud storage, because asymmetric encryption techniques are about 1000 times slower than symmetric encryption which makes it impractical when trying to encrypt large amounts of data [27]. The next sub section discusses several symmetric encryption algorithms proposed by different researchers.

Symmetric encryption used for cloud

Some researchers have suggested the traditional encryption technique for data security in cloud such as DES, 3DES and Blowfish. This section describes the working procedure of these algorithms. Some researchers have tried to propose new encryption algorithms.

Data Encryption Standard (DES) is based on a feistel block cipher [28]. It is developed by the IBM cryptography researcher Horst Feistel [29]. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions and Exclusive OR operations. DES is a 64-bit block cipher as it uses the same key for both encryption and decryption and only operates on 64-bit blocks of data at a time. The key size used is 56-bits; however a 64-bit (or eight-byte) key is actually input. The least significant bit of each byte is used for parity and does not increase the security in any way. Once a plaintext is received for encryption, it is arranged into 64-bit blocks required as input. If the number of bits in the message is not evenly divisible by 64, then the last block is padded. DES performs an initial permutation on the entire 64-bit block of data. It is then split into two, 32-bit sub-blocks, namely, L_i and R_i which are then passed into first round, of which there are 16 rounds. At the end of the 16^{th} round, the 32-bit L_i and R_i output quantities are swapped to create the pre-output. The concatenation of R_{16} and L_{16} is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64-bit ciphertext [30]. There are many attacks and methods that exploit the weaknesses of DES, which shows that DES is an insecure block cipher [31].

Triple DES (3DES) [32] is simply a concatenation of three DES algorithm operations. The procedure for encryption is exactly the same as regular DES, except that it is passed through the DES engine three times. The first pass is a DES encryption, the second pass is a DES decryption of the first DES ciphertext result and the third pass is a DES encryption of the second pass result. This produces the resultant 3DES ciphertext. The procedure for decrypting a 3DES ciphertext is the same as 3DES encryption except in reverse order. Note that although the input key for DES is 64-bits long, the actual key used by DES is only 56-bits in length. This means that the effective key strength for TDES is actually 168-bits. Let *EK (I)* and *DK (I)* represent the DES encryption and decryption of *I* using DES key *K* respectively. Each 3DEA encryption and decryption operation is a compound operation of DES encryption and decryption operations [33].

The following operations are executed,

i. 3DEA encryption operation: The transformation of a 64-bit block *I* into a 64-bit block *O* that is defined as, $= EK_3 (DK_2 (EK_1 (I)))$
ii. 3DEA decryption operation: The transformation of a 64-bit block *I* into a 64-bit block *O* that is defined as, $= DK_1 (EK_2 (DK_3 (I)))$

There are several keying methods that 3DES uses. All three keys can be independent of each other, or the first and third keys can be identical, with the second key being unique [34]. All three keys can also be identical, which provides least security and it takes time to encrypt than DES.

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data [35]. It takes a variable-length key, from 32-bits to 448-bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all users. Blowfish Algorithm is a Feistel Network [36], iterating a simple encryption function 16 times. A Feistel network is a general method of transforming any function (usually called F function) into a permutation [37] [38]. Blowfish uses a large number of sub keys. These keys must be pre computed before any data encryption or decryption. The input is a 64-bit data element and produces the 64-bit cipher text.

Most of the researchers have proposed an encryption algorithm for cloud by integrating any two or three existing algorithms. But this is not a complete solution for cloud environment. Cloud needs a complete security service algorithm to protect users' data in the cloud storage.

B. Data obfuscation

Data Obfuscation (DO) [39] [40] is a form of data masking where data is purposely scrambled to prevent unauthorized access to sensitive data. This form of DO results are in meaningless or confusing [41]. The techniques listed below have two main goals; protect sensitive data from disclosure and create usable test data with the same data shape as the original. It is ideal to use more than one technique to bring added protection.

Masking

Data masking replaces sensitive characters or fields with a meaningless character such as "X". Masking preserves the data shape for display on screens and reports.

Substitution

Substitution replaces the fields of data with similar content that is unrelated to the original data. An example of substitution is to replace the actual first and last names with names randomly picked up from a large list of valid first and last names that have been created specifically for use in substitution. Substitution preserves the original data shape while hiding the actual sensitive information.

Shuffling records

Shuffling and substitution are similar except that shuffling uses the source data itself instead of an external list. Shuffling moves data between rows so that the data shape is preserved but the original details of the sensitive information are hidden.

Number and date variance

Variance modifies number or date by replacing the field with similar information that is a random percentage of the original. The percent variance is chosen to keep the new data within valid ranges for the field. Variance keeps the data shape while hiding the original sensitive information.

Gibberish generation

Gibberish generation is used when to hide the sensitive data with associated data such as correspondence that can identify the original data. A practical example would be bank records. Users could obfuscate the account information of customers in the database tables but the records are linked to images of the monthly statements sent to the customers. The stored statements contain the entire information that customers wish to hide. To prevent the sensitive information from being revealed, gibberish generation replaces the confidential data with random junk of data files with equivalent size.

Data generation

Data generation creates fictitious or mock data from scratch or other sources which are usable for testing purposes.

4. RESULTS AND DISCUSSIONS

Many researchers and practitioners work on identifying cloud threats, vulnerabilities, attacks, and other security issues, in addition to providing countermeasures in the form of frameworks. Each framework has some problems like maximum work burden to users, time consuming process of encryption and description. Table-1 represents comparison of existing cloud security frameworks.

Table-1. Comparison security framework.

Framework	Cloud	Data form	Components	Users' work burden	Services	Data protection technique	No. of CSP
Kamara *et al*.,	Public	Data at Rest	Four	Yes	IaaS	Encryption	Single
Yau *et al*.,	Public	Data at Rest	Three	No	SaaS, IaaS	Obfuscation	Multiple
Atiq ur Rehman *et al*	Public	Data at Rest	Five	Yes	SaaS	Encryption& Obfuscation	Single
Basescu *et al*	Public	Data at Rest	Five	Yes	IaaS	Encryption	Single
Govinda *et al*.,	Public	Data at Rest	Agent based	No	IaaS	Obfuscation	Single
Arockiam *et al*.	Public	Data at Rest	Three service	No	SaaS, IaaS	Encryption & Obfuscation	Multiple
Munir *et al*.,	Public	Data at Rest	Eight	Yes	IaaS	Encryption	Single
Hamdan Al-Sabri *et al.,*	Public	Data at Rest	Seven	Yes	IaaS	Encryption	Single

5. CONCLUSIONS

Security is the main issue in cloud environment. Many research works are carried out to solve the security issues especially aimed at concentrating on confidentiality of data in the cloud. From the study, it is clear that many novel research works are needed to strengthen the public cloud storage environment. If the security services are stronger and well established, then it will prevent many security issues either from CSP or other users of the cloud. The security service should be fast and at the same time security should not be compromised. In order to effectively secure the public cloud storage, data sent to the cloud are masked using prominent security services. Each framework is discussed in this paper has address some security issues at same time it has some problems like maximum work burden to users and users should depend on single CSP for all services. It is better tune the framework to even more efficient to address the security issue in the cloud.

REFERENCES

[1] Dr. L. Arockiam, S. Monikandan, G. Parthasarathy. 2011. Cloud Computing: A Survey. International Journal of Internet Computing. 1(2), ISSN: 2231 - 6965, pp. 26-33.

[2] Dimitrios Zissis and Dimitrios Lekkas. 2012. Addressing Cloud Computing Security Issues. Journal of Future Generation Computer Systems, Elsevier Science. 28(3): 583-592.

[3] Ahmad Azarnika, JafarShayana, MojtabaAlizadehb and Sasan Karamizadeha. 2012. Associated Risks of Cloud Computing for SMEs. Open International Journal of Informatics. 1: 37-45.

[4] Pierangela Samarati and Sabrina De Capitani di Vimercati. 2010. Data Protection in Outsourcing Scenarios: Issues and Directions. Proceedings of ACM Symposium on Information, Computer and Communications Security. pp. 1-14.

[5] Deyan Chen and Hong Zhao. 2012. Data Security and Privacy Protection Issues in Cloud Computing. Proceedings of IEEE International Conference on Computer Science and Electronics Engineering. pp. 647-651.

[6] Vaquero L M, Luis Rodero-Merino, Juan Caceres and Maik Lindner. 2009. A Break in the Clouds: Towards a Cloud Definition", ACM SIGCOMM Computer Communication Review, Volume 39, Issue 1, pp. 50-55.

[7] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez. 2013. An Analysis of Security Issues for Cloud Computing. Journal of Internet Services and Applications, Springer-Verlag. 4(1): 1-12.

[8] Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo. 2014. Secure Data Sharing in the Cloud. Security, Privacy and Trust in Cloud Systems, Chapter-1: Cloud Security, Springer-Verlag Berlin Heidelberg. pp. 45-72.

[9] Khalil I. M., Abdallah Khreishah and Muhammad Azeem. 2014. Cloud Computing Security: A Survey. Journal of open access computers. 3: 1-35.

[10] Kamara S., Lauter K. 2010. Cryptographic Cloud Storage. Financial Cryptography and Data Security, Springer Berlin Heidelberg, LNCS. 6054: 136-149.

[11] Yau SS, An HG. 2010. Confidentiality Protection in Cloud Computing Systems. International Journal of Software Informatics. 4(4): 351-365.

[12] Atiq ur Rehman and M. Hussain. 2011. Efficient Cloud Data Confidentiality for DaaS. International Journal of Advanced Science and Technology. 35: 1-10.

[13] Basescu C., A. Carpen-Amarie, C. Leordeanu, A. Costan, and G. Antoniu. 2011. Managing Data Access on Clouds: A Generic Framework for Enforcing Security Policies. Proceedings of IEEE International Conference on Advanced Information Networking and Applications. pp. 459-466.

[14] Nicolae B., G. Antoniu, and L. Bougé. 2009. BlobSeer: How to Enable Efficient Versioning for Large Object Storage under Heavy Access Concurrency. Proceedings of ACM International Conference on Data Management in Peer-to-Peer Systems, St-Petersburg, Russia. pp. 18-25.

[15] Jegou Y., S. Lantéri, J. Leduc. 2006. Grid'5000: A Large Scale and Highly Reconfigurable Experimental Grid Testbed. International Journal of High Performance Computer Applications. 20(4): 481-494.

[16] Govinda K. and Sathiyamoorthy E. 2012. Agent Based Security for Cloud Computing using Obfuscation. Elsevier, Science Direct, Procedia Engineering. 38: 125-129.

[17] Dr. L. Arockiam, S. Monikandan. 2015. AROMO Security Framework to Enhance Security of Data in Public Cloud. International Journal of Applied Engineering Research, Print ISSN 0973-4562, Online ISSN 1087-1090, 10(9), (Special Issue) 6740-6746.

[18] Munir K and Dr. Sellapan Palaniappan. 2013. Framework for Secure Cloud Computing. International Journal on Cloud Computing: Services and Architecture. 3(2): 21-35.

[19] Hamdan M. Al-Sabri and Saleh M. Al-Saleem. 2013. Building A Cloud Storage Encryption (CSE) Architecture for Enhancing Cloud Security. International Journal of Computer Science Issues. 10(2): 259-266.

[20] Sascha Fahl and Marian Harbach. 2012. Confidentiality as a Service - Usable Security for the Cloud. Proceedings of IEEE International Conference on Trust, Security and Privacy in Computing and Communications. pp. 153-162.

[21] Mohit Marwaha and Rajeev Bedi. 2013. Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing. International Journal of Computer Science Issues. 10(Issue 1, No. 1): 367-370.

[22] Siani Pearson, Yun Shen and Miranda Mowbray. 2009. A Privacy Manager for Cloud Computing. Proceedings of International Conference on Cloud Computing, Springer-Verlag Berlin, Heidelberg, LNCS. 5931: 90-106.

[23] Maheshwari V, Arash Nourian and Muthucumaru Maheswaran. 2012. Character-Based Search with Data Confidentiality in the Clouds. Proceedings of IEEE International Conference on Cloud Computing Technology and Science. pp. 895-899.

[24] Hamlen K, Murat Kantarcioglu, Latifurkhan and Bhavani Thuraisingam. 2010. Security Issues for Cloud Computing. International Journal of Information Security and Privacy. 4(2): 39-51.

[25] Tim Mather, Subra Kumaraswamy and Shahed Latif. 2009. Cloud Security and Privacy. O'Reilly Media, Inc.

[26] Dr. L. Arockiam, S. Monikandan. 2015. AROcrypt: A Confidentiality Technique for Securing Enterprise's Data in Cloud. International Journal of Engineering and Technology, ISSN: 0975-4024, 7(1): 245-253.

[27] Dr. L. Arockiam, S. Monikandan. 2013. Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm. International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), 2(8), ISSN: 2278-1021, 3064-3070.

[28] William Stallings. 2005. Cryptography and Network Security: Principles & Practices. 4th edition, Prentice Hall, ISBN: 978-0-13-187316-2.

[29] Michael Backes. 2007. Block Ciphers. Lecture Notes for CS-578 Cryptography, Saarland University. pp. 1-15.

[30] Garima Saini and Naveen Sharma. 2014. Triple Security of Data in Cloud Computing. International Journal of Computer Science and Information Technologies. 5(4): 5825-5827.

[31] Jawahar Thakur and Nagesh Kumar. 2011. DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. International Journal of Emerging Technology and Advanced Engineering. 1(2): 6-12.

[32] Kaur A, Manisha Bhardwaj. 2012. Hybrid Encryption for Cloud Database Security. International Journal of Engineering Science & Advanced Technology. 2(3): 737-741.

[33] Monika Agrawal and Pradeep Mishra. 2012. A Comparative Survey on Symmetric Key Encryption Techniques. International Journal on Computer Science and Engineering. 4(05): 877-882.

[34] Rashmi Nigoti, Manoj Jhuria and Dr. Shailendra Singh. 2013. A Survey of Cryptographic Algorithms for Cloud Computing. International Journal of Emerging Technologies in Computational and Applied Sciences. 4(2): 141-146.

[35] Shirole Bajirao Subhash and Dr Sanjay Thakur. 2014. Data Confidentiality in Cloud Computing with Blowfish Algorithm. International journal of Emerging Trends in Science and Technology. 1(1): 01-06.

[36] Hoang VT and Phillip Rogaway. 2010. On Generalized Feistel Networks. Proceedings of International annual conference on Advances in cryptology, Springer Berlin Heidelberg, LNCS. 6223: 613-630.

[37] Andrey Bogdanov and Kyoji Shibutani. 2013. Generalized Feistel Networks Revisited. Journal of Designs, Codes and Cryptography, Springer US. 66(1-3): 75-97.

[38] Saravana Kumar S.G. and Dr. A. Shanmugam. 2014. Modified F-Function for Feistel Network in Blowfish Algorithm. International Journal of Engineering and Innovative Technology. 4(4): 229-232.

[39] Randy Raymond. 2015. Data Obfuscation for Test Environments. xensight, www.xensight.com, 2010, pp. 1-7.

[40] Chad Robertson. 2015. PDF Obfuscation - A Primer. TBA, the SANS Institute, https://www.sans.org/reading-room/whitepapers/engineering/pdf-obfuscation-primer-34005, 2012, pp. 1-38.

[41] S. Monikandan and Dr. L. Arockiam. 2015. Confidentiality Technique to Enhance Security of Data in Public Cloud Storage Using Data Obfuscation. Indian Journal of Science Technology, ISSN (Print): 0974-6846, ISSN (Online): 0974-5645, 8(24): 1-10.