International Journal of Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-9)

Research Article | **September 2014**

Security Enhancement of Outsourced Data on Cloud Using Identity Based Encryption

Varsha S. Agme*
Computer Department, BSIOTR, Pune University
Pune, India

Prof. Archana C. Lomte
Computer Department, BSIOTR, Pune University
Pune, India

Abstract—

Cloud computing is one of the most promising technology which plays a key role in the next generation of computer technology. It has been broadly accepted due to its ability to fewer costs associated with computing while increasing scalability and flexibility for computer processes. Cloud computing provides a facility of Data outsourcing, in which different data owner can upload data and different data user can access data. But, here the data should not be secure in the hands of cloud providers. Data owner have expressed concerns about the various security aspects that be present with the cloud computing. From the owner perspective, cloud computing security concerns, especially privacy protection issues of data and security of data, remain the primary hinder for adoption of cloud computing services. This paper describes an enhancement for the existing data security Model in cloud environment. The proposed data storage security model provides data security by using encryption, user authentication; re-encryption and this system also provide protection against DDOS attack. For owner convenience this proposed system also provides the facility of online notification of user access request in the form of SMS so no need to online all the time.

Keywords—Cloud Computing, DDOS, Identity Based Encryption, Outsourced data, Security, etc

I. INTRODUCTION

Cloud computing has become a commercial trend because of its desirable properties, such as scalability, fault-tolerance, elasticity, and pay per use. Small and medium-scaled companies can achieve great flexibility at a fewer price by outsourcing their data and query services to the cloud. The cloud infrastructures are more powerful and reliable than Local or personal computing devices, but they are still caused to internal threats (e.g., via virtual machines) and external threats (e.g., via system vulnerabilities) that may leak user's sensitive data. Therefore, many organizations still suspected to adopt cloud services [1].

Although still at its early stage, Cloud Computing has already drawn great attention, and its benefits have attracted an increasing number of users to outsource their local data centers to remote cloud servers. Data security is a critical issue for remote data storage. In particular, this system using a novel cryptography Identity Based Encryption (IBE) and re-encryption , and enhance it toward providing a full fledged cryptographic basis for a secure data sharing scheme on untrusted storage.

To prevent unwanted disclosure of sensitive information, data owners may have to encrypt their data before outsourcing. In this, only the authorized users with the decryption keys can recover the data, and other unsolicited accessors cannot decrypt the data without the decryption keys, e.g. the cloud service provider (CSP), cannot execute decryption, even if they successfully obtain the cipher-texts stored in the cloud [3].Including, this system also present one of the solutions for securing data server against DDOS attack which may more commonly happens in Cloud Computing.

A. Identity based encryption and proxy re-encryption

One significant drawback and barrier for the widespread use of public-key cryptography is its dependency on a public-key infrastructure that is shared within its users. Before secure communications can take place, both sender and receiver must generate encryption and signature key pairs, submit certificate requests along with proof of identity to a Certificate Authority (CA), and receive CA-signed certificates, which they can then use to authenticate one another and exchange encrypted messages.

This process can be both time-consuming and error-prone, and is especially prohibitive for novice computer users. Identity-based cryptography reduce these barriers by without any preparation on the part of the message recipient and it provides advantages over Public Key Infrastructure based approaches [8].No need to issue certificates or revocation of keys. In an IBE system, arbitrary strings such as e-mail addresses or IP addresses can be used to form public keys for users.

A proxy re-encryption (PRE) scheme involves three parties: e.g. Owner, User, and a proxy. PRE allows the proxy to translate a cipher text encrypted under owner's public key into one that can be decrypted by user's secret key. Unlike the traditional proxy decryption scheme, PRE doesn't need users to store any additional decryption key, in other words, any decryption would be finished using only his own secret keys [9].

B. DDOS attack

Though cloud computing is targeted to provide better utilization of resources using virtualization techniques and to take up much of the work load from the client, it is fraught with security risks. One of most serious threats is Distributed Denial of service attack (DDOS) which is easy to implement and affective [10].

In this proposed system an approach called traceback, count the no. Of request coming from user side with threshold of 40 seconds within time threshold, measure the time threshold that is start time and end time is 60 seconds. By performing IP Filter It was able to trace and identify the source most of these attacks messages of these attacks and block that IP, so it reduces the packets that reconstruction path required. It also had a high detection rates with low false positives.

II. LITERATURE SURVEY

In the following paragraphs, some of the literature papers are outlined:

A. Identity-based encryption from the weil-pairing

This scheme was first secure and practical identity-base encryption (IBE) scheme was proposed by Boneh and Franklin [11] based on pairing. Authors were proposed full functional identity based encryption scheme. This scheme had chosen cipher text security in random oracle model using elliptic curve variant of the computational Diff-Hellman problem.

1) Advantages

1. This was a Very basic encrypting scheme.
2. This scheme was a first practical identity based encrypting scheme.

2) Disadvantage

1. This scheme was provides only encryption.

B. Identity-based Proxy Re-encryption

This scheme was proposed by Anca Ivan, Yevgeniy Dodis[12],in this work authors revisited and formally study the notion of proxy cryptography. Intuitively, various proxy functions allow two cooperating parties F (the FBI) and P (the "proxy") to duplicate the functionality available to the third party U (the user), without being able to perform this functionality on their own (without cooperation). The concept was closely related to the notion of threshold cryptography, except they deal with only two parties P and F, and place very strict restrictions on the way the operations are performed (which is done for the sake of efficiency, usability and scalability).

For example, for decryption (resp.signature) P (F) sends a single message to F (P), after which the latter can decrypt the message. Authors formal modelling of proxy cryptography significantly generalizes, simplifies and simultaneously clarifies the model of"atomic proxy" suggested by Blaze and Strauss. In particular, authors define bidirectional and unidirectional variants of our model, and so this system extremely simple generic solutions for proxy signature and encryption in these models. Authors also give more efficient solutions for several specific schemes. Authors conclude that proxy cryptography was a relatively simple concept to satisfy when looked from the correct and formal standpoint.

1) Advantages

1. This scheme was a first identity based reencryption scheme.
2. It was unidirectional and bidirectional IBPE scheme.

2) Disadvantage

1. This scheme was not secure against the collusion attack.

C. Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage

Improved PRE was presented by G. Ateniese, K. Fu, M. Green, and S. Hohenberger [13] in which they predicted that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the widely used of this re-encryption has been hindered by considerable security risks.

In this paper they pointed out that the previous work of Ivon and Dodis was not collision safe. So, author M. Green, and G. Ateniese presented a paper Identity-Based Proxy Re-Encryption [REF 3], in which, proxy re-encryption scheme a

semi-trusted proxy converts a cipher text for Alice into a cipher text for Bob without seeing the underlying plain text. A number of solutions had been proposed in the public-key setting. In this paper, authors address the problem of Identity-Based proxy re-encryption, where cipher texts were transformed from one identity to another. This scheme was compatible with IBE deployments and did not require any extra work from the IBE trusted-party key generator. In addition, this system was non-interactive and one of them permits multiple re-encryptions. Their security was based on a standard assumption (DBDH) in the random oracle model.

Following papers can be divided as:

- The re-encryption key can be computed by the owner:

1) *Inter-domain Identity-based Proxy Re-encryption*

This paper was presented by Qiang Tang, Pieter Hartel, Willem Jonker [14],in which they presented that Proxy re-encryption, a cryptographic primitive developed to delegate the decryption right from one party (the delegator) to another (the delegatee).So far, research efforts had only been devoted to the intra-domain setting, where the delegator and the delegatee this system are registered in the same domain. In this paper, they investigated the proxy re-encryption in the inter-domain setting, where the delegator and the delegatee this system are from different domains, and focus on the identity-based case. Authors analyzed the trust relationships and possible threats to the plain text privacy, and provided rigorous security definitions.And in this system they were proposed a new inter-domain identity-based proxy re-encryption scheme and proved its security in their security model.

1) Advantages

1. The re-encryption key is computed by the data owner.

2) Disadvantage

1. This scheme is vulnerable to the collusion attack, malicious user can steal users decryption key.

- The re-encryption key can be computed by the Private Key Generator:

2) *New identity based proxy re-encryption schemes to prevent collusion attacks*

This system was proposed by L. Wang, M. Mambo, and E. Okamoto [15], in this system, the PKG computes the re-encryption key by checking the secret keys of the owner and the user.

1) Advantage

1. This system was collusion safe, collusion attack in not possible in this system.

2) Disadvantage

1. Untrusted third party PKG involved for generation re-encryption key.

D. Identity-Based Secure Distributed Data Storage Schemes

This scheme was proposed by Jinguang Han, Willy Susilo, and Yi Mu [16], in which they pointed out the previous schemes are intra domain and they presented first inter-intra domain proxy cryptosystem based on identity based encryption, which is the first cloud based system. In this system, a user's identity can be an arbitrary string and two parties can communicate with each other without checking the public key certificates. At first, the file owner encrypts his files under his identity prior to outsourcing them to servers. Then, he sends the cipher texts to the proxy servers. Consequently, the proxy servers can transfer a cipher text encrypted under the identity of the owner to a cipher text encrypted under the identity of the receiver after they has obtained an access permission (re-encryption key) from the owner [16-17].

1) Advantage

1. The file owner generates the re-encryption key independently without interaction with PKG after authentication of user.
2. This scheme is collusion safe, collusion attack in not possible in this system.
3. For one query user could get only one file; user can download one file for one request.

2) Disadvantage

1. In this scheme, for providing better security to the system, the data owner must have to be online for all the time to check the authenticated user and generate access permission for them.

III. PROPOSED SYSTEM

This system having three different entities: data owner, data user, and cloud server as in Data owner wants to upload the file F that he wants to outsource on the cloud server in encrypted form for effective data utilization reasons. To do so, before outsourcing, data owner will first provide encryption to the files C = Enc (F), and upload it on to the cloud server. For the required file user submits a query request in to the cloud server .For one query he can access only one file. Upon

receiving the query request, the cloud server transmits the query request to the data owner. Here, this system provides the facility of SMS on data owner mobile number regarding user request so need to be online all the time.

After receiving the request, the data owner checks for the authentication of user that the user is legitimate or not. If user is not legitimate then request not granted. If user is authorized then data owner generates the access permission (re-encryption key). This re-encryption key is send to the server and then server provides re-encryption as R=ENC (ENC (F) and sends re encrypted data to the user. After receiving the re encrypted data/file the authorized user can decry-pt thedata with provided decryption key as D= DEC (DEC (F)).

A. System Architecture

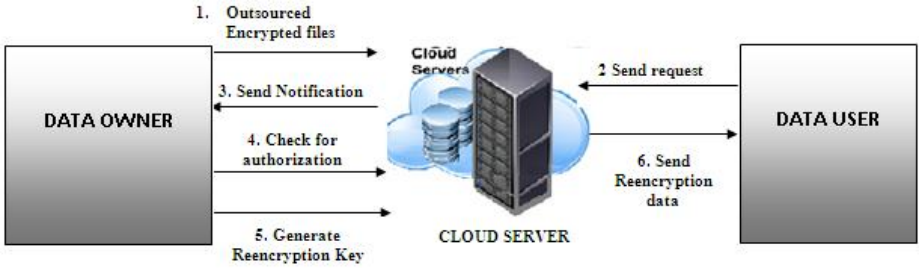

Fig 1.System architecture for Security Enhancement of Cloud Data Storage Using Identity Based Encryption

B. Project Modules

1. Registration /Log-in:

Log-in page make user to access an account in a cloud server. When user has an account in the cloud server for accessing data and provides other services. User can sign up the page directly else users needed to create new account using New User option. In this, separate modules for data owner who will work as administrator and the data users.

2. Encryption/Uploading file:

This is used to encrypt a plain text into a cipher text. The data M is encrypted with ID and pubic parameters. Data owner after sign up his/her account can upload encrypted data at cloud server. The AES algorithm is used for encryption.

3. User Query/request:

In this module User can send access request/query to cloud server for required file.

4. Notification:

In cloud server forward the request to data owner. The data owner can get the notification about request in the form of SMS on his/her registered mobile number.

5. Access Permission:

For authorized user, while sending access permission the data owner generate and send re-encryption key to server and server performs re-encryption to the cipher text and forward it to data user.

6. Data Retrieval:

Date retrieval is the final module of this project. User download data and decrypt the re-encrypted data using provided decryption key which is generated by using AES algorithm along with BASE64 and by following some custom steps. For each session different key will be generated and for second decryption, the key which used for encryption same key used for decryption.

IV. COMPARATIVE ANALYSIS

The following tables and graph shows the comparison between existing system and proposed system .The proposed system provides more number of properties as compare to existing system-

TABLE I: Comparison Study with Existing System

Property	Matsuo	WWMO	WWMO	GA	CT	THJ	IBSDDS	Proposed
Unidirectional	YES	YES	YES	YES	YES	YES	YES	YES
Non-interactive	NO	NO	NO	YES	YES	YES	YES	YES
Key optimal	YES	YES	YES	YES	YES	YES	YES	YES
Collusion-safe	YES	YES	YES	NO	NO	NO	YES	YES
Non-transitive	YES	YES	YES	YES	YES	YES	YES	YES
File-based access	NO	NO	NO	NO	NO	NO	YES	YES
Owner Convenient System	NO	NO	NO	NO	NO	NO	NO	YES
Offline Notification as SMS	NO	NO	NO	NO	NO	NO	NO	YES
DDOS Safe	NO	NO	NO	NO	NO	NO	NO	YES

TABLE III: NO. OF PROPERTIES APPLICABLE TO EXISTING SYSTEM AND PROPOSED SYSTEM

System	No. Of properties applicable
Matsuo	4
WWMO	4
WWMO	4
GA	4
CT	4
THJ	4
IBSDDS	6
Proposed System	9

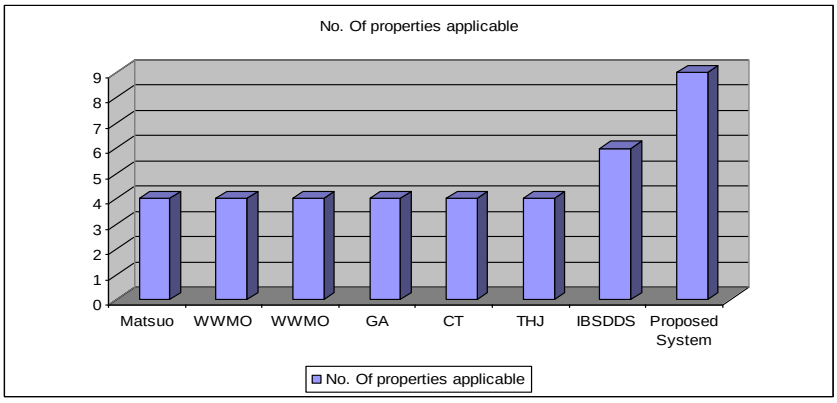

Fig 2.Graph for comparison of Proposed System and Existing System

V. RESULT ANALYSIS

The resultant table shows the time required for performing encryption, re-encryption and decryption of different file type and different file size. The time required for encryption , re-encryption and decryption is vary according to file type and file size .As file size increases the time is also increases .Time of decryption is more than encryption and re-encryption because it perform double decryption ,first decryption for encryption and second for re-encryption. Following graph shows the time required for encryption, ,re-encryption and decryption in milliseconds for different file types of different sizes.

TABLE IIIII: TIME REQUIRED FOR FILE UPLOAD AND DOWNLOAD IN MILLI SECONDS

				Time (ms)		
SR NO.	**File Name**	**File Type**	**File Size**	**Encryption**	**Reencryption**	**Decryption**
1	server	txt	30KB	0	20	10
2	connect111	txt	338KB	16	20	40
3	machine	txt	1.34MB	40	70	60
4	client	txt	14.7MB	360	480	850
5	document	doc	22KB	10	10	20
6	Implementation	doc	165KB	10	10	25
7	v1	doc	1.16MB	70	10	70
8	Varsha REPORT	doc	9.25MB	190	10	530
9	VisaCard Platinum	xls	18KB	10	20	10
10	2013-14 TT	xls	165KB	10	10	10
11	Tg data comp	xls	523KB	30	20	30
12	FACULTY TT	xls	1MB	30	20	20
13	christmas fair	pdf	11KB	0	10	10
14	iiiij	pdf	158KB	10	15	30
15	Identity	pdf	1.07MB	20	30	60

16	servlets	pdf	18.8MB	510	740	1030
17	Androids	pdf	46.7MB	1590	2077	3178
18	logo	jpg	8KB	0	10	10
19	user	jpg	176KB	10	10	10
20	DSC02901	jpg	1.89MB	40	20	90
21	DSC2002	jpg	2.29MB	60	10	110
22	disneyduck	audio	473KB	10	30	120
23	Tik Tik	audio	3.10MB	70	40	160
24	dhadang	video	2.50MB	50	10	120
25	Kashmir Main	video	51.1MB	1460	1470	3270
26	IBSDDS new	ppt	504KB	10	20	40
27	IBSDDS	ppt	1.6MB	20	40	80
28	AES	ppt	4.8 MB	90	70	300
29	AES ALGO	ppt	10 MB	230	280	590
30	setup	exe	27 KB	10	10	20
31	setup1	exe	116 KB	10	10	30
32	SQLYog	exe	7.59 MB	160	40	380
33	mysql-5.5	exe	31.7 MB	970	990	2200
34	CG10	zip	2 KB	31	10	50
35	dynamic pages	zip	22 KB	47	30	80
36	PPP prac	zip	131 MB	94	80	196
37	base64	zip	1.18 MB	297	300	587
38	comp	zip	10 MB	953	1045	2080

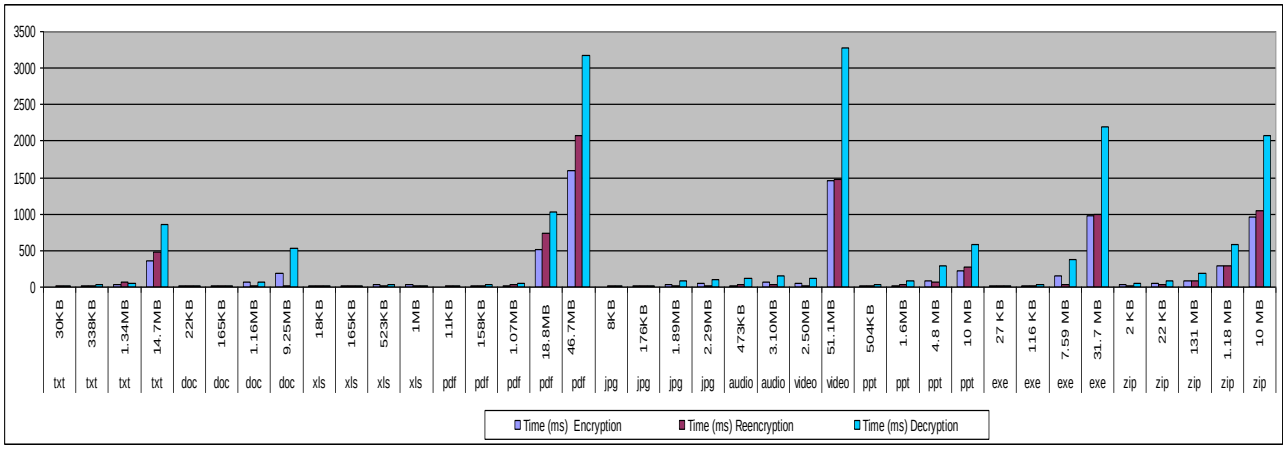

Fig 3.Graph of Proposed System results

Following screen shots shows that the DDOS attack from unauthorized user, that he/she send a request to server ,that requests are greater than thresholds value show IP address of that unauthorized user get blocked ,he/she can not access the system.

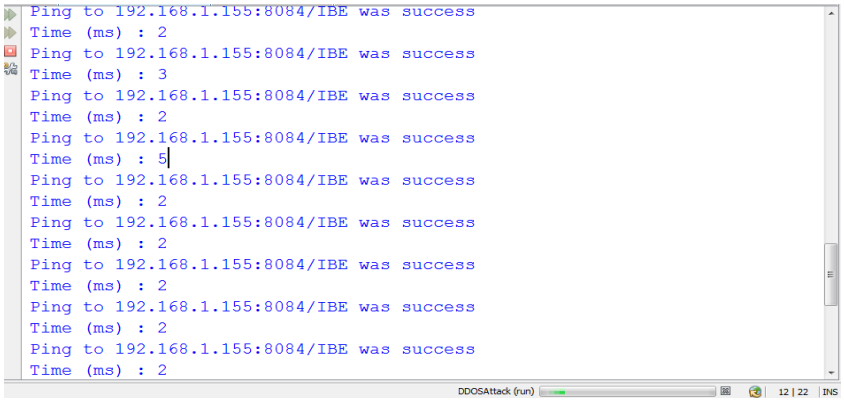

Fig 4. Shows DDOS attack from unauthorized user

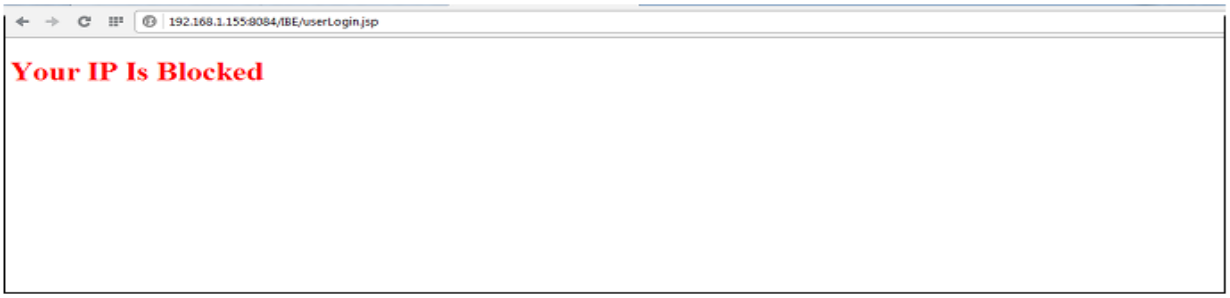

Fig 5. Shows IP address of unauthorized user get blocked

VI. CONCLUSIONS

Cloud computing is a distributed system where different users of different domains can share data among each other. Different Identity-based proxy re-encryption schemes have been proposed to outsource sensitive data from the owner to an external party. Nevertheless, they cannot be employed in cloud computing. Security of data storage is more important in cloud. The proposed system enhances the security of data storage by introducing the identity based secure encryption and re-encryption.

It provides many advantages like online notification in the form of SMS on owners' registered mobile number. So no need to be online all the time. Thus, this system over come the previous schemes and also provides security against Distributed Denial of Service attack and it provides secure model of cloud storage with safe data uploading .As discussed in comparative analysis, from Table I, Table II and from figure 2, conclude that the proposed system provides more strong properties and as in result analysis from Table III and from figure 3, shows the time for processing of encryption and decryption is vary as file sizes.

And from screen shots figure 4 and figure 5,conclude that if there is a DDOS attack then IP address of unauthorized user get blocked, thus proposed system resist the DDOS attack by counting the request to the server.

ACKNOWLEDGMENT

We would like to say thanks to all for their helpful comment and discussion and inspiration for this proposed work.

REFERENCES

[1] Michael Armbrust, Armando Fox, Rean Gri_th,Anthony D. Joseph, Randy Katz,Andy Konwinski,Gunho Lee, Dav id Patterson, Ariel Rabkin, Ion Stoica,and Matei Zaharia," A View of Cloud Computing",*communications of the ac m* ,April 2010, vol. 53 , no. 4,pg no.50-58

[2] Dimple patil, Madhuri Walse, Jagruti Warkhede, Priya Gawande," Cloud Computing Based Services", *International Journal Of Scientific Research And Education,* Volume 2,Issue 1 ,Pages 237-241,2014, ISSN (e): 2321-7545.

[3] Ms.M.Shanthi, Mr. P. Ranjithkumar,"Protected Patients Data Centre in Cloud Computing*",Proc. of International Conference On Global Innovations In Computing Technology ,International Journal of Innovative Research in Computer and Communication Engineering* ,Vol.2,Special Issue 1,March 2014.

[4] Kanika Aggarwal , "Cloud Computing: The Future of Computing ", *Journal of Engineering, Computers and Applied Sciences* ,Volume 2, January 2013

[5] Vaibhav M. Hatwar , Vaibhav S. Wankhede,Prof.Kaustubh S. Satpute ,"SECURE FILE HOSTING*", International Journal of Research in Advent Technology,* January 2014 ,Vol 2, Issue 2,34-39

[6] Nilotpal Chakraborty , Raghvendra Singh Patel, "Security Challenges in Cloud Computing:A Comprehensive Study", *International Journal of Computer Science Engineering and Technology*, January 2014 ,Vol 4, Issue 1,1-4

[7] Pierangela Samarati and Sabrina De Capitani di Vimercati, "Data Protection in Outsourcing Scenarios:Issues and directions", *E-Business and Telecommunications: 6th International Joint Conference,* ICETE ,2011.

[8] Carl Youngblood, "An Introduction to Identity-based Cryptography",CSEP 590TU,University of Washington Online Course, free tutorials and lecture notes,March 2005

[9] Song Luo, Jianbin Hu and Zhong Chen, "New Construction of Identity-based Proxy Re-encryption*", International Association for Cryptologic Research* ,2010

[10] Lanjuan Yang,Tao Zhang ; Jinyu Song ; Jin Shuang Wang, "Defense of DDoS attack for cloud computing" ,*IEEE International Conference on Computer Science and Automation Engineering (CSAE),*(Volume:2) ,2012

[11] D.Boneh,M.Fraklin, "Identity based encryption from the weil pairing" ,in proc. Advances in Cryptography, Vol.2139,lecture Notes in Computer Science,pp.213-229,Aug-2001

[12] A.Ivan and Y .Dodis, "Proxy cryptography revisited" ,in proc. *Network and Distributed System Security Symposium* ,pp.1-20,The Internet Society, Feb.2003.

[13] G. Ateniese, K. Fu, M. Green ,and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage",in proc. Network and Distributed System Security Symposium , pp. 1-15, The Internet Society, Feb. 2005.

[14] Q. Tang, P. Hartel, and W. Jonker, "Inter-domain identity-based proxy re-encryption" , in Proc. Information Security and Cryptography -Inscrypt'08 , vol.5487 of Lecture Notes in Computer Science, pp.332-347 Dec. 2008.

[15] L. Wang, L. Wang, M. Mambo, and E. Okamoto, "New identity based proxy re-encryption schemes to prevent collusion attacks",in proc. Pairing-Based Cryptography - Pairing 10 , vol. 6487 of Lecture Notes in Computer Science,pp. 327-346, Dec. 2010.

[16] Han, J., Susilo, W. and Mu Yi, "Identity-based data storage in cloud computing", Future Generation Computer Systems: *international journal of grid computing*: theory, methods and applications, 673-681

[17] Jinguang Han, Willy Susilo,and Yi Mu,"Identity-Based Secure Distributed Data Storage Schemes", Computers, *IEEE Transactions* ,Volume-63 Issue-4

[18] Varsha S .Agme, Prof. Archana C.Lomte," Cloud Data Storage Security Enhancement Using Identity Based Encryption", International Journal of Application or Innovation in Engineering and Management ,Vol- 3, April 2014.

[19] Shibin D, M Manicka Raja, Christhuraj M R," Detection of DDOS attack using collated strategies and Anteater System" ,*IEEE Transactions On Cloud Computing IEEE*, Feb 2012

[20] S .Amritha, S .Saravana Kumar , "Secure Data Forwarding In Distributed Environment Using Cloud Storage System*"* ,*International Journal Of Computational Engineering Research* , Vol. 3,March,2013

