Volume 6, Issue 4, April 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Network Based Collaborative Security Management with Encryption and Compression in Data Center for Cloud

Sarathkumar M S
PG Student of MCA, KVM CE and IT,
Cherthala, Kerala, India

Nidhy S Ravi
Assistant Professor, KVM CE and IT,
Cherthala, Kerala, India

Abstract-- A data center is a centralized repository and an infrastructure that supports Internet service. Using the cloud infrastructure web and mobile applications are used by millions of people day by day, so there will be a challenge in scale and flexibility that provided by the cloud computing for the shared physical infrastructures. Multiple tenants store and retrieve their data and applications in shared data centers, with different tenants have different security requirements. Data center ensure the security and storage capacity needed for different tenants. Generally network virtualization is used satisfy tenant specific requirements and enabling multi-tenant data centre activities. A collaborative network security prototype system used in a multi-tenant data center and use the encryption methods for data privacy and compression methods for reduce storage capacity in data center. It is centralized collaborative scheme and deep packet inspection with an open source UTM system. To simplify the security rule management, a security level based protection policy is used for vCNSMS. The data encryption and compression provide between peer UTM and security center. There are different packet inspection schemes for different security level and they are enforced with different security plugins and different encryption and compression methods are used according to the security level.

Keywords— Data center network; network security; collaborative network security; data security, file compression, encryption, decryption, optimization, cryptographic algorithm compression algorithm, network virtualization; cloud computing.

I. INTRODUCTION

A cloud data center is a centralized repository and an infrastructure that supports Internet service. A cloud data center may be defined from a different of perspectives, such as IaaS, PaaS, and SaaS proposed by the NIST [1] and include public cloud, private cloud, hybrid cloud, and other different categories. Other categories include computing, networking, and storage from a system's perspective and transmission from a data perspective. Specific to the cloud network, there are different characteristics of a cloud, within a cloud, and between cloud networks. The VMware NSX provides the virtualization of networks with Software-Defined Network (SDN) inside a data center. The SDN is the dynamic characteristic of network boundaries, that is the original static, natural, and physical boundaries within the traditional network are replaced by the dynamic and virtual logical boundaries of SDN. Effective working of web and application in the network are fully based on transformation of data, data are store in a shared approach so it use the store platform of network or cloud. An OpenFlow-based SDN [2,3] is used by the Google B4 network [4] to implement all the interconnections among cloud data centers in different locations. Blurring the network boundaries between each tenant cloud and the privacy and capacity of the information in data center are major issues in networking.

II. SECURITY ISSUES IN DATA CENTER NETWORKS

Firewalls, IDS, WAF such devices are traditional security devices set up with the Middle boxes model inside and outside networks. With the development of cloud computing technology, the arrangement of Middle boxes is facing new challenges in the large-scale data center network environment [5]. Pervasive visibility, deeper analytics, massive saleability, unified view are fundamental capabilities for the data security in the data center [6].

A. *Network security issues in data center network*

Network security is important for a data center network, huge number of users are used in various locations for saving the data in same server and the same tenant may store data on different servers with multiple backups, so the network boundaries between each user to become blurred. In traditional network may have several gate ways and data of several hot are from same gate way, the vantage points is ensure the gate way is safe and reliable. In data center network vantage is replaced by virtual logical gate way. It is used to protect security of virtual logical boundaries between tenants and provide security of dynamic boundaries caused by virtual machine migration, and meet the dynamic security requirements of virtual machines [7-10]. That is new changes in deployment location of middleboxes. Security requirements for different tenants are different, so the question is raise how to meet different security requirements when multiple tenants' data pass through the same security device and how to provide effective administration.

B. *Data security issues in data center network*

Most web and mobile applications are run with the help of data center and all the data are store in the data center network. Data center must ensure the security and capacity need for saving the data from different tenants. Major issues in secure data transfer that is cloud data center network physical security is lot because of shearing different companies with computing resources then no control or knowledge of where the resources run. A common standard to ensure data integrity does not yet exists it lead to secure software interface. And data separation in data center, customer may be able to use cloud service providers if privacy rights are violated, and in any case the cloud service providers may face damage to their reputation. For security we use the encryption and decryption algorithm and who controls the encryption and decryption key, it should be the user by logically, therefore it effect the data security stored data center. User access control in case of Payment Card Industry Data Security Standard (PCI DSS) data logs must be provide to security regulators [11-14].

III. PROPOSED WORK PLAN

A. *Network security in data center network*

vCNSMS[15], a collaborative network management prototype system derived from CNSMS [16-20] for multi-tenant data center networks vCNSMS is based on a prototype system with a home brewed version of an untangle open source multifunction gateway. The principle of collaborative network security in DCN follow a Basic network topology that is, the Security Center and peer-UTMs are deployed in the data center network. In the starting stages, the peer- UTM is running a registration process for the Security Center. The Security Center receives the registration information and displays the registered UTMs.

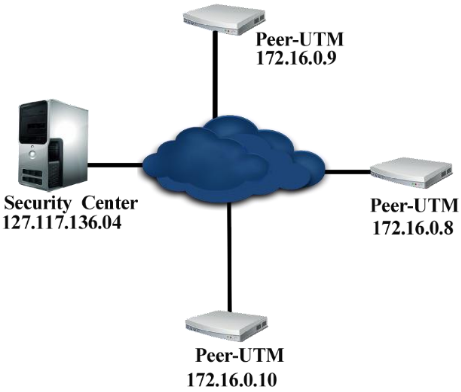


Fig 1: network topology and it set up the vCNSMS configuration

In the fig 1 three peer-UTMs and one security center are connected through a data center. The peer-UTMs 172.16.0.8, 172.16.0.9, 172.16.0.10 are registered in the security center 127.117.136.04 via data center, peer-UTM passed information to security center at the time of registration it is happens at the bootstrap stage. We can see how collaborative security in DCN works, first Security center interacts with the peer-UTMs.

- Different rules are issued by security center: There is web User Interface (UI) and in include a help option for rule creation and an option for the rule issued.
- Events are reported by peer-UTM: The security events reported by peer-UTMs displayed on Security Center web interface.
- Events inform between peer-UTMs: The peer-UTM collaborative security module have a web-based UI. The web UI shows the different peer-UTMs to the Security Center and displays any occurred security events.

Another working phase is an Antivirus module in collaborative security which deals with virus signature database. Virus signature is a unique string of bits, or the binary pattern, of a virus and it is like a fingerprint in that it can be used to detect and identify specific viruses. The virus signature used in Anti-virus software to scan for the presence of malicious code.

- The Security Center have an option to import the virus signature database.
- The Security Center have an option to issue the virus signature database.
- An interface displays that the virus database has been updated: The time changes.
- Virus signature database synchronization between peer-UTMs is performed using the p2p mode.

Firewall module in collaborative security have different actions such as,

- Security Center importing Firewall rules
- Security Center issues issuing the Firewall rules.
- Firewall rules have been updated displayed in interface: There is a web UI in the peer-UTM collaborative security Firewall module. The web UI shows the new Firewall rules that will be updated.
- Updated rules are implemented by the peer-UTMs by choosing correct one: In the display UI of the update rules, the peer-UTMs are allowed to let a certain rule lapse if that rule is not applicable.

Working procedure at the Security rule center, the security rule center in security center includes a rule distribution module. The rule distribution module is divided into server and client, and the server program is a socket communication module written in Java that is manually activated in the Security Center. The client program is running in the peer-UTM Firewall and Rules control module. When the server and client programs are running normally, the Security Center can quickly transfer rules in a specific folder to the peer-UTM's rule control module.

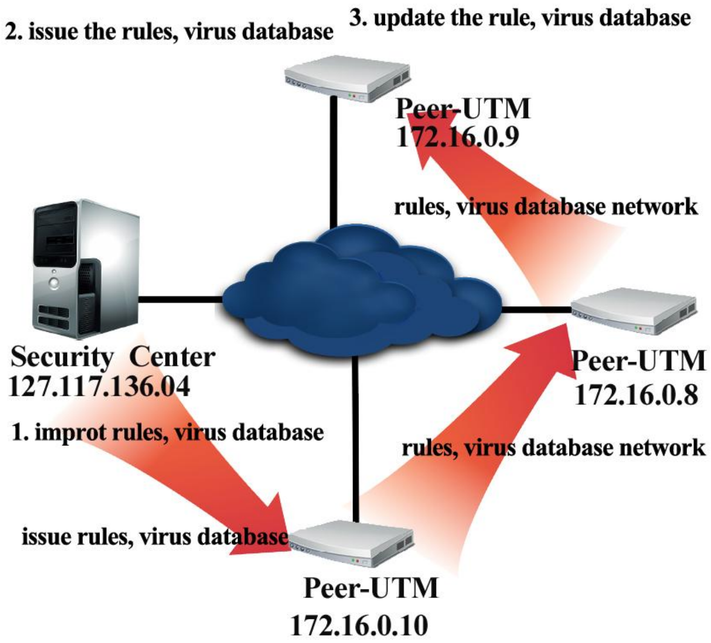

2. issue the rules, virus database
3. update the rule, virus database
Peer-UTM
172.16.0.9
rules, virus database network
Security Center
127.117.136.04
Peer-UTM
172.16.0.8
1. improt rules, virus database
rules, virus database network
issue rules, virus database
Peer-UTM
172.16.0.10

Fig: 2 working of rules and virus database in network

B. Data security in data center network

Different encryption and decryption algorithms are widely available and it used for data security. Generally two type of algorithms are there Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys [21]. For data security in data center network we can use different encryption algorithms [22].

1) RSA Algorithm

RSA is the most common Public Key algorithm, invented by Rivest, Shamir, and Adleman (RSA). RSA is basically an asymmetric encryption /decryption algorithm. It is asymmetric in nature, that here public key distributed to all and we can encrypt the message by using this public key and private key which is secret and used for decryption, the private key not shared to everyone. RSA working method in data center network environment, RSA algorithm is used to ensure the security of data in data center network in cloud. In RSA algorithm we have encrypted our data to provide security so only authorized users can access it. After encryption data is stored in the data center. So that when it is required then a request can be placed to security center in data center network. Security center authenticates the user and delivers the data to user. As RSA is a Block Cipher in which every message is mapped to an integer. In the proposed data center network environment, Public key is known to all, whereas Private Key known only to user who originally need the data. Thus encryption and decryption are done by the security center. Once the data is encrypted with the Public key, it will be decrypted using the corresponding Private Key only.

2) AES Algorithm

Advanced Encryption Standard (AES) [23], also known as Rijindael is used for securing data. AES is a symmetric block cipher and is used widely now-a-days. AES Working methods in data center network environment. Advanced Encryption Standard, symmetric key encryption algorithm is use 128-bits key length for this purpose. Implementation proposal states that First, peer-UTM(user) register to the security centre and establish the connection through data center after the data will be migrate on data center. When transfer the data to the data center happens at that time the security center first encrypt data using AES algorithm and then sent to data center. Once encrypted, data is uploaded on the data center, any request to read the data will occur after it is decrypted by security center. This encryption solution is transparent to the security center and can be integrated quickly. To store the keys, a physical key management server can be installed in the data center. Encryption protects the data and keys and guarantees that they remain under control of security center.

3) DES Algorithm

The Data Encryption Standard (DES) is a block cipher. Data can be encrypted in blocks of size 64 bits each. That is in DES encryption algorithm input is 64 bits of plain text and it produces 64 bits of cipher text. DES use the concept of minor differences, that is same algorithm and key are used for encryption and decryption. The key length of this algorithm is 56 bits; however a 64 bits key is actually input. DES is therefore a symmetric key algorithm. The encryption take place in the security center and result will store in data center and the decryption done by the security center and provide the result to peer-UTM.

C. Storage optimization in data center

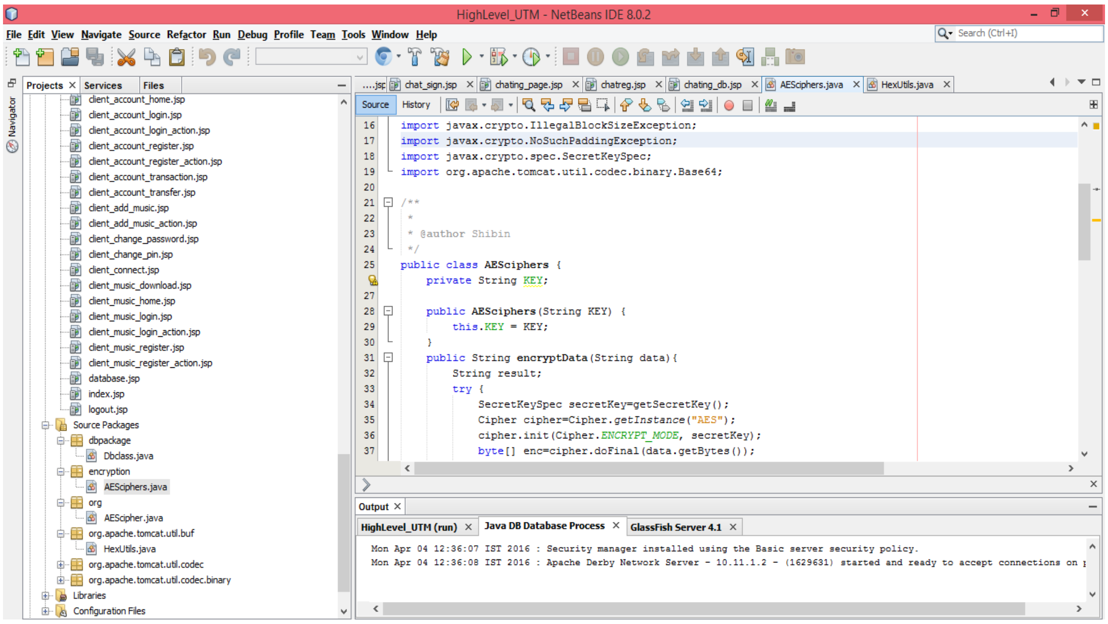
The major advantage of data center in cloud is users can access data at any time and it automatically analysis user's requirement and locate and transform data. Day by day enter web and mobile application are used the data center for store data so the capacity to store data is become a great issue so we must optimize the data storage and ensure effective data access. Commonly we use different optimization algorithm for data. Such as Huffman coding [24], LZ77, LZ78 [25-29] and LZW. Using the grid computing tools github repo we can implement gzip or bzip2 optimization/compression method. LWZ in one the new method for optimization of data in data center.

1) LZW Compression

LZW compression [30] technic never understand the input text and it interchanges a set of characters with single code. LZW generally construct a table know as string translation table and the text is compressed using this table. The string translation table created by LZW generates a strict-length of code to strings. The translation table is initialized with all single-character strings. The LZW compression algorithm takes each input sequence of bits of a given length and creates an entry in a table for that particular bit pattern, consisting of the pattern itself and a shorter code. As input is read, any pattern that has been read before results in the substitution of the shorter code, effectively compressing the total amount of input to something smaller. Unlike earlier approaches, known as LZ77 and LZ78, the LZW algorithm does include the look-up table of codes as part of the compressed file. The decoding program that uncompressed the file is able to build the table itself by using the algorithm as it processes the encoded input.

IV. IMPLEMETATION AND RESUT

Implementation of algorithms has been done using NetBeans IDE with Java. Coding used for implementing algorithm are shown below:


HighLevel_UTM - NetBeans IDE 8.0.2
File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
Search (Ctrl+I)
Projects Services Files
client_account_home.jsp
client_account_login.jsp
client_account_login_action.jsp
client_account_register.jsp
client_account_register_action.jsp
client_account_transaction.jsp
client_account_transfer.jsp
client_add_music.jsp
client_add_music_action.jsp
client_change_password.jsp
client_change_pin.jsp
client_connect.jsp
client_music_download.jsp
client_music_home.jsp
client_music_login.jsp
client_music_login_action.jsp
client_music_register.jsp
client_music_register_action.jsp
database.jsp
index.jsp
logout.jsp
Source Packages
dbpackage
Dbclass.java
encryption
AESciphers.java
org
AESCipher.java
org.apache.tomcat.util.buf
HexUtils.java
org.apache.tomcat.util.codec
org.apache.tomcat.util.codec.binary
Libraries
Configuration Files
....jsp chat_sign.jsp chating_page.jsp chatreg.jsp chating_db.jsp AESciphers.java HexUtils.java
Source History
Output
HighLevel_UTM (run) Java DB Database Process GlassFish Server 4.1

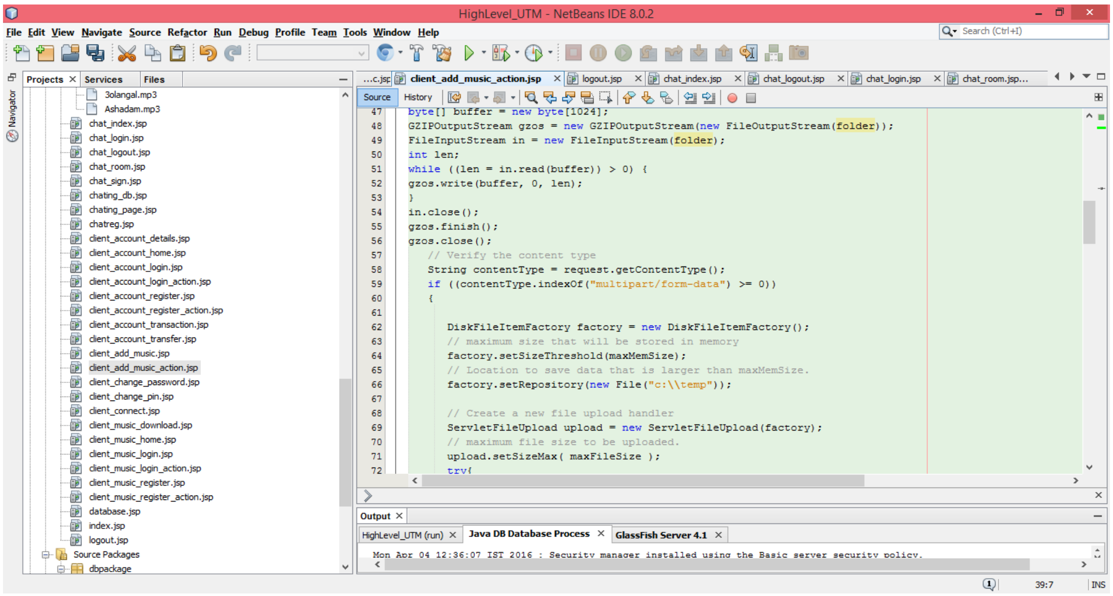
```java
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.spec.SecretKeySpec;
import org.apache.tomcat.util.codec.binary.Base64;

/**
 *
 * @author Shibin
 */
public class AESciphers {
    private String KEY;

    public AESciphers(String KEY) {
        this.KEY = KEY;
    }
    public String encryptData(String data){
        String result;
        try {
            SecretKeySpec secretKey=getSecretKey();
            Cipher cipher=Cipher.getInstance("AES");
            cipher.init(Cipher.ENCRYPT_MODE, secretKey);
            byte[] enc=cipher.doFinal(data.getBytes());
```

```
Mon Apr 04 12:36:07 IST 2016 : Security manager installed using the Basic server security policy.
Mon Apr 04 12:36:08 IST 2016 : Apache Derby Network Server - 10.11.1.2 - (1629631) started and ready to accept connections on p
```

Fig 3: coding for encryption algorithm


HighLevel_UTM - NetBeans IDE 8.0.2
File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
Search (Ctrl+I)
Projects Services Files
3olangal.mp3
Ashadam.mp3
chat_index.jsp
chat_login.jsp
chat_logout.jsp
chat_room.jsp
chat_sign.jsp
chating_db.jsp
chating_page.jsp
chatreg.jsp
client_account_details.jsp
client_account_home.jsp
client_account_login.jsp
client_account_login_action.jsp
client_account_register.jsp
client_account_register_action.jsp
client_account_transaction.jsp
client_account_transfer.jsp
client_add_music.jsp
client_add_music_action.jsp
client_change_password.jsp
client_change_pin.jsp
client_connect.jsp
client_music_download.jsp
client_music_home.jsp
client_music_login.jsp
client_music_login_action.jsp
client_music_register.jsp
client_music_register_action.jsp
database.jsp
index.jsp
logout.jsp
Source Packages
dbpackage
...c.jsp client_add_music_action.jsp logout.jsp chat_index.jsp chat_logout.jsp chat_login.jsp chat_room.jsp...
Source History
Output
HighLevel_UTM (run) Java DB Database Process GlassFish Server 4.1
39:7 INS

```java
byte[] buffer = new byte[1024];
GZIPOutputStream gzos = new GZIPOutputStream(new FileOutputStream(folder));
FileInputStream in = new FileInputStream(folder);
int len;
while ((len = in.read(buffer)) > 0) {
gzos.write(buffer, 0, len);
}
in.close();
gzos.finish();
gzos.close();
   // Verify the content type
   String contentType = request.getContentType();
   if ((contentType.indexOf("multipart/form-data") >= 0))
   {

      DiskFileItemFactory factory = new DiskFileItemFactory();
      // maximum size that will be stored in memory
      factory.setSizeThreshold(maxMemSize);
      // Location to save data that is larger than maxMemSize.
      factory.setRepository(new File("c:\\temp"));

      // Create a new file upload handler
      ServletFileUpload upload = new ServletFileUpload(factory);
      // maximum file size to be uploaded.
      upload.setSizeMax( maxFileSize );
      try{
```

```
Mon Apr 04 12:36:07 IST 2016 : Security manager installed using the Basic server security policy.
```

Fig 4: coding for compression algorithm

For implementing the data center and peer-UTM we have to update Firewall rules and use them and ensure the cloud networking analysis find the specified network flow which blocks firewall module. The content filtering in UDP which also help for implementation process. For cloud set use the build in cloud virtualization and structure the network topology in that cloud. With the help of java build in class we have to integrate the security center and peer-UTM functions.

V. CONCLUSION

We can conclude that different encryption methods and compression methods can be applied in the collaborative network security in data center. Using the vCNSMS methods we can solve the security problems in network it details with the security center and peer-UTMs and connected through data center. The data center can arrange vCNSMS for flexibility and scalability to protect different tenants with different network policies and security requirements. Information security in data center network can be provided by using encryption algorithms such as RSA, AES, and DES. The security center provide the corresponding algorithm to the user data and it store in the data center. Data optimization is accomplished by using compression algorithms, LZW is used as one of the compression algorithm. Security center control the compression algorithm and compressed data store in the data center. Using collaborative network security, encryption, and compression the data center network is protected from general issues.

REFERENCE

[1] NIST definition of cloud computing, http://csrc.nist.gov/publications/PubsNISTIRs.html, 2007.

[2] J.D. Liu, A. Panda, A. Singla, B. Godfrey, M. Schapira, and S. Shenker, Ensuring connectivity via data plane mechanisms, presented at 10th USENIX Symposium on Networked Systems Design and Implementation, Lombard, IL, USA, 2013.

[3] J. D. Liu, B. H. Yan, S. Shenker, and M. Schapira, Datadriven network connectivity, in Proc.10th ACM Workshop on Hot Topics in Networks, New York, USA, 2011, p. 8.

[4] S. Jain, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A.Singh, S. Venkata, J. Wanderer, J. Zhou, M. Zhu, J. Zolla, U. Hozle, S. Stuart, and A. Vahdat, B4: Experience with a globally-deployed software defined WAN, in Proc. ACM SIGCOMM 2013 Conference on SIGCOMM, Hong Kong, China, 2013, pp. 3-14.

[5] Qihoo 360 Internet Security Center, Development trend of enterprise security in the internet ages, http:// www.gartner.com/technology/mediaproducts/pdfindex.jsp? g=Qihoo issue1, 2013.

[6] Five Steps for Securing the Data Center: Why Traditional Security May Not Work http://www.cisco.com/web/SG/fsi_summit/pdf/five_steps_for_securing_the_data_center_white_paper.pdf, 2014.

[7] X. M. Chen, B. P. Mu, and C. Zhen, NetSecu: A collaborative network security platform for in-network security, in Proc. 3rd International Conference on Communications and Mobile Computing, Qingdao, China, 011, pp. 59-64.

[8] D. H. Ruan, C. Lin, Z. Chen, and J. Ni, Handling high speed traffic measurement using network processors, presented at International Conference on Communication Technology, Guilin, China, 2006.

[9] J. Ni, C. Lin, and Z. Chen, A fast multi-pattern matching algorithm for deep packet inspection on a network processor, presented at the IEEE International Conference on Parallel Processing, Xi'an, China, 2007.

[10] Z. Chen, C. Lin, J. Ni, D.H. Ruan, B. Zheng, Y. X. Jiang, X. H. Peng, Y. Wang, A. A. Luo, B. Zhu, Y. Yue, and F. Y. Ren, AntiWorm NPU-based parallel bloom filters for TC/IP content processing in giga-Ethernet LAN, in Proc. the IEEE International Conference on Communications, 2006, pp. 2118-2123.

[11] Z. Chen, C. Lin, J. Ni, D. H. Ruan, B. Zheng, Y. X. Jiang, and F. Y. Ren, AntiWorm NPU-based parallel bloom filters for TCP/IP content processing in Giga-Ethernet LAN, in Proc. the IEEE International Conference on Local Computer Networks, Sydney, Australia, 2005, pp. 748- 755.

[12] Wang, J.K.; Xinpei Jia, Data Security and Authentication in hybrid cloud computing model, Global High Tech Congress on Electronics (GHTCE), 2012 IEEE, On page(s): 117-120.

[13] Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing, January 2011. http://docs.ismgcorp.com/files/external/Draft-SP-800-145_cloud-definition.pdf.

[14] Iankoulova, I.; Daneya, M., Cloud computing security requirements: A systematic review, Research Challenges in Information Science (RCIS), Sixth International Conference on, 2012, On page(s): 1 - 7.

[15] Zhen Chen, Wenyu Dong, Hang Li, Peng Zhang, Xinming Chen, and Junwei Cao, Collaborative Network Security in Multi-Tenant Data Center for Cloud Computing, International Conference on Tsinghua Science and Technology, February 2014, 19(1): 82-94.

[16] F. Han, Z. Chen, H. Xu, H. Wang, and Y. Liang, A collaborative botnets suppression system based on overlay network, International Journal of Security and Networks, vol. 7, no. 4, pp. 211-219, 2012.

[17] Z. Chen, F. Han, J. Cao, X. Jiang, and S. Chen, Cloud computing-based forensic analysis for collaborative network security management system, Tsinghua Science and Technology, vol. 18, no. 1, pp. 40-50, 2013.

[18] X. Chen, K. Ge, Z. Chen, and J. Li, AC-Suffix-Tree: Buffer free string matching on out-of-sequence packets, in Proc. 2011 ACM/IEEE Seventh Symposium on Architectures for Networking and Communications Systems, IEEE Computer Society, Brooklyn, NY, USA, 2011, pp. 36-44.

[19] T. Li, F. Han, S. Ding, and Z. Chen, LARX: Largescale antiphishing by retrospective data-exploring based on a cloud computing platform, in Proc. IEEE 20th International Conference on Computer Communications and Networks, Maui, HI, USA, 2011, pp. 1-5.

[20] B. Mu, X. Chen, and Z. Chen, A collaborative network security management system in metropolitan area network, in Proc. IEEE 3rd International Conference on Communications and Mobile Computing, Qingdao, China, 2011, pp. 45-50.

[21] Idrizi, Florim, Dalipi, Fisnik and Rustemi, Ejup. “Analyzing the speed of combined cryptographic algorithms with secret and public key”. International Journal of Engineering Research and Development, e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 8, Issue 2 (August 2013), pp. 45.

[22] Rachna Arora, Anshu Parashar, Secure User Data in Cloud Computing Using Encryption Algorithms, International Journal of Engineering Research and Applications (IJERA), Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926.

[23] Douglas Selent, Advanced Encryption Standard, Rivier Academic Journal, Volume 6, Number 2, Fall 2010.

[24] D.A. Huffman, "A Method for the Construction of Minimum Redundancy Codes", Proceedings of the I.R.E., September 1952, pp 1098-1102.

[25] T. Bell, J. Cleary, and I. Witten, “Data compression using adaptive coding and partial string matching,” IEEE Transactions on Communications, Vol. 32 (4), p. 396-402, 1984.

[26] A. Moffat, Implementing the PPM data compression scheme, IEEE Transactions on Communications, Vol. 38 (11), pp. 1917-1921, November 1990.

[27] Ziv, J., & Lempel, A. “A Universal Algorithm for Sequential Data Compression,” IEEE Transactions on Information Theory, 23(3), pp.337-343, May 1977.

[28] Ziv, J., & Lempel, A. “Compression of individual sequences via variable-rate coding,” IEEE Trans. Inform. Theory, 24(5), 530-536, September 1978.

[29] M. Burrows and D. J. Wheeler, “A Block-sorting Lossless Data Compression Algorithm”, Digital Systems Research Canter Research Report 124, May 1994.

[30] K.Govinda , Yuvaraj Kumar, Storage Optimization in Cloud Environment using Compression Algorithm, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),Volume 1, Issue 1, May-June 2012.