Network Coding Based Data Security in Cloud Computing

Dipali Pandya1
Research Scholar, GTU PG School, Ahmedabad, India.
Email: pandyadipali1993@gmail.com
Harshal Trivedi2
Soft van, Ahmedabad, India.
Email: Harshal.softVan@gmail.com

ABSTRACT

Cloud computing is very popular in organizations and institutions because it provides storage and computing services at very low cost. However, it also introduces new challenges for ensuring the confidentiality, integrity and access control of the data. Some approaches are given to ensure these security requirements but they are lacked in some ways such as violation of data confidentiality due to collusion attack and heavy computation (due to large no keys). To address these issues we propose a scheme that the concepts of network coding in which data owner divides data into chunks and Apply deterministic linear network coding" on that data for which cloud controller will play an role of Third party for coefficient generation(i.e. key). Whenever user want to access the data cloud controller will provide respective co-efficient (i.e. key) in a secure manner. By using that key user will be able to decrypt the data. In this research Paper our proposed algorithm will outperform the existing approaches in form of computational complexity also provides robust confidentiality. Result show the better throughput and security by provide reliability and throughput graph with proposed scheme.

Keyword: - *Cloud Computing, Security Challenges, Data Security Issue, Network Coding, Confidentiality*

1. INTRODUCTION

Cloud computing is an emerging computing model .Cloud computing is the most widely used platform now a days. The US National Institute of Standards and Technology (NIST)[8] defines cloud computing as follows: “cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. Network, servers, storage, applications and services) that can be rapidly provisioned and released with a minimal management effort or service provider interaction. It provides Services according to three fundamental service models: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

Storage as a service is basically a platform as a service. The five characteristics of cloud computing are: on-demand service, self-service, location independent, rapid elasticity and measured scale service. These characteristics make cloud significant. Industries and institutions are exploiting these characteristics of cloud computing and increasing their profit and revenue [7]. That is why, industries are shifting their businesses towards cloud computing. However, data security is a major obstacle in the way of cloud computing. People are still fearing to exploit the cloud computing. Some people believe that cloud is unsafe place and once you send your data to the cloud, you lose complete control over it [7]. They are more or less right. Data of data Owners are processed and stored at external servers. So, confidentiality, integrity and access of data become more vulnerable. Since, external servers are operated by commercial service providers, data owner can't trust on them as they can use data for their benefits and can spoil businesses of data owner [4]. Data owner even can't trust on users as they may be malicious. Data

confidentiality may violet through collusion attack of malicious users and service providers. In this paper, the approach the concepts of network coding in which data owner divides data into chunks and Apply deterministic linear network coding [4]on that data for which cloud controller will play an role of Third party for coefficient generation(i.e. key). Whenever user want to access the data cloud controller will provide respective co-efficient (i.e. key) in a secure manner. By using that key user will be able to decrypt the data. Our proposed algorithm will outperform the existing approaches in form of computational complexity also provides robust confidentiality. The remaining portion of this paper is organized as follows. In Section 2, define cloud security and data security issue In Section 3 we describe related work In Section 4 we present our proposed scheme. In Section 5 we present my implementation. Finally, we conclude and Future Work the paper in section 6 and section 7.

2. CLOUD SECURITY

This section deals with various aspects of security in Cloud Computing. It includes information security principles, security requirements, security controls and security architecture. Information Security Principles: There are certain principles which we need to abide by so as to have a secure cloud communication. These principles are referred as Information Security Principles. CIA Triad is a well-known security model which deals with important aspects of IT security. It is used to identify security problems and provide its necessary solutions [10, 11]. In the CIA Triad, C stands for Confidentiality, I for Integrity and A stands for Availability. These security principles are also discussed in [9].

2.1 Data Security Issue

Different issue in the cloud with user data are briefly explain below.

1. Confidentiality - Confidentiality refers to protecting the information from unauthorized users. Its aim is to ensure that information is hidden from unauthorized users to access it. With the increase in number of applications and equipment's in cloud, threats also increases which lead to an increased number of access points.

2. Integrity - Integrity refers to the consistency and accuracy of data. The data should not be modified by any unauthorized user or in an unauthorized manner. It says that data should not be altered in transit.

3. Availability - The principle of availability says that the information must be available whenever it is needed. It refers to the property that the system must be usable and accessible when requested by the authorized users.

Fig -1: Issues in cloud security[]

Here according to the services of different layers, security issues caused are addressed in table I.

Service Models	*Description*	*Examples*	*Security issues*
Software as a Service (SaaS)	It imparts simple software services along with user interface to end user.	Google docs, G mail, Yahoo, Salesforce.com (CRM application) etc.	Privacy of data, Security of network and locality, Integrity and access of data, Authentication, Backup, Availability etc.
Infrastructure as a Service (IaaS)	In this computer framework is treated like a service and the consumer does not purchase the resources instead they buy them.	Amazon web services, Windows Azure etc	1. Taking Virtual machines off creates security challenges. 2. Security issues in operating system are encountered in IaaS.
Platform as a Service (PaaS)	It provides with the deployment of apps without buying and managing the software and hardware for it. To build and deliver web apps Paas provides what all is required.	Google App Engine, SQL Azure etc.	1. Apps are built by users and this control is given to them by the provider. 2. Security of the apps is controlled by the provider only. 3. If hackers can attack the infrastructure of an app they are more likely to attack the visible code of it.

Table -1 SECURITY ISSUES IN VARIOUS SERVICE MODELS [1]

3. Related work

3.1 Network Coding: An Instant Primer

Network coding is a networking technique in which transmitted data is encoded and decoded to increase network throughput, reduce delays and make the network more robust. In network coding, algebraic algorithms are applied to the data to accumulate the various transmissions. The received transmissions are decoded at their destinations. This means that fewer transmissions are required to transmit all the data.[4]

3.2 Random Linear Network Coding

Random linear network coding is a simple yet powerful encoding scheme, which in broadcast transmission schemes allows close to optimal throughput using a decentralized algorithm. Nodes transmit random linear combinations of the packets they receive, with coefficients chosen from a Galois field. If the field size is sufficiently large, the probability that the receiver(s) will obtain linearly independent combinations (and therefore obtain innovative information) approaches 1. It should however be noted that, although random linear network coding has excellent throughput performance, if a receiver obtains an insufficient number of packets, it is extremely unlikely that they can recover any of the original packets. This can be addressed by sending additional random linear combinations until the receiver obtains the appropriate number of packets. Overall, large networks can increase their efficiency through the use of network coding, but high overhead costs may make them less amenable for small networks.

$$\begin{bmatrix} c_{1,1} & \cdots & c_{1,n} \\ \vdots & \ddots & \vdots \\ c_{n,1} & \cdots & c_{n,n} \end{bmatrix} \begin{bmatrix} P_1 \\ \vdots \\ P_n \end{bmatrix} = \begin{bmatrix} CP_1 \\ \vdots \\ CP_n \end{bmatrix}$$

$$\begin{bmatrix} P_1 \\ \vdots \\ P_n \end{bmatrix} = \begin{bmatrix} c_{1,1} & \cdots & c_{1,n} \\ \vdots & \ddots & \vdots \\ c_{n,1} & \cdots & c_{n,n} \end{bmatrix}^{-1} \begin{bmatrix} CP_1 \\ \vdots \\ CP_n \end{bmatrix}$$

With RLNC, sender combines a block of n original data packets P = {P1, P2…Pn} together with a set of random coefficients C= {c1,c2,..., cn} to generate a coded packet CP. Equations represents the coding and decoding equations respectively:

4. PROPOSED ALGORITHM

In my proposed system, I will develop an algorithms for data publishing and data retrieval which uses the concepts of network coding in which data owner divides data into chunks and Apply Random linear network coding on that data for which cloud controller will play an role of Third party for coefficient generation(i.e. key).

Whenever user want to access the data cloud controller will provide respective co-efficient (i.e. key) in a secure manner. By using that key user will be able to decrypt the data. In whole process the key will be secure using RSA algorithms.

Our proposed algorithm will outperform the existing approaches in form of computational complexity also provides robust confidentiality and provide high reliability of data.

Participant	Role
Data Owner (DO)	Data owner is a person who utilizes the storage services provide by the cloud service provider.
Cloud Controller (CC)	CC generates the key for user and authenticates the user and gives the permission to access the data.
Cloud Service Provider (CSP)	CSP provides the storage services to user.

Table -2: ROLE OF PARTICIPANTS

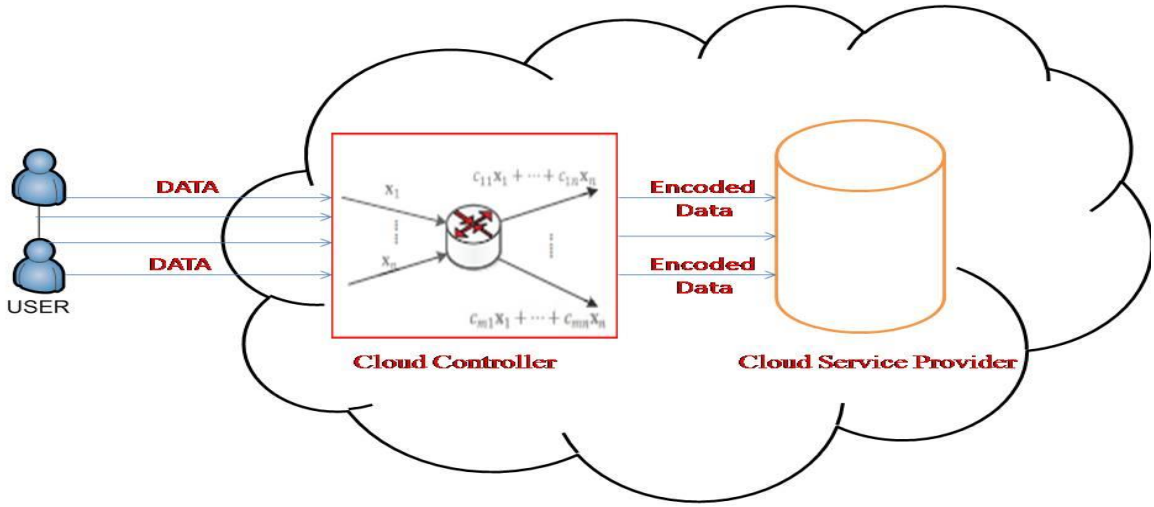

Fig -2 Proposed Schemes Based on Network Coding (Abstract Diagram)

4.1 Proposed Algorithm

1. Data_Publishing ()

1. Send Request to Cloud controller (CC) for Deterministic Co-efficient
2. CC will authenticate the user
3. CC will call Random Number Generator ()

   CC maps <RND_As_KEY, User_id>
4. Apply Network coding using RND_AS_KEY

$$X = \sum_{i=1}^{n} g^i M^i$$

5. User encrypt the generated key using RSA algorithm
6. Publish<Network_Coded_Data_Set, Encrypted Key> on Cloud

2. Data_Retrieval() :-

1. User Sends Request to CC
   CC will authenticate the user
   Key <- Find Key (User_id)
2. Send (key)
3. User Decrypt (key)
4. User will decrypt the data by applying Reverse Network coding

5. IMPLEMENTATION

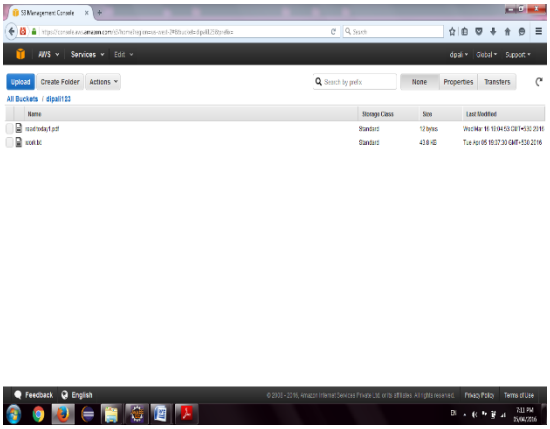

Fig -3: S3 Management Console

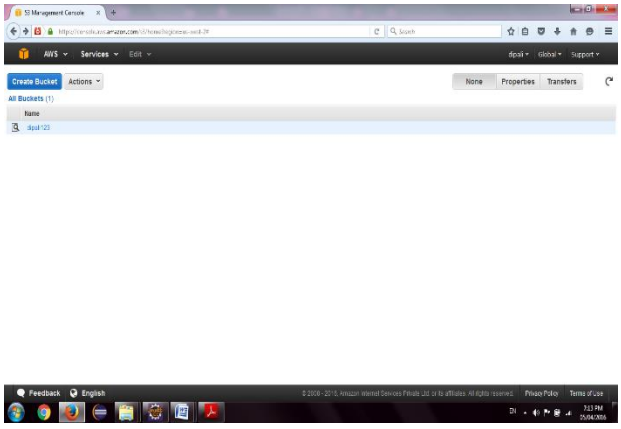

Fig -4: S3 Bucket

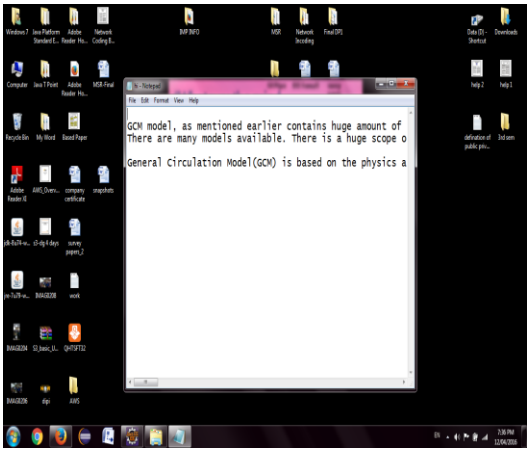

Fig -3: User Original File

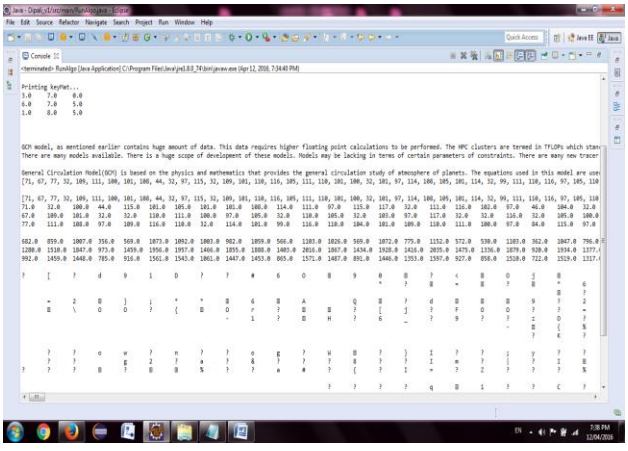

Fig -4: Eclipse Console

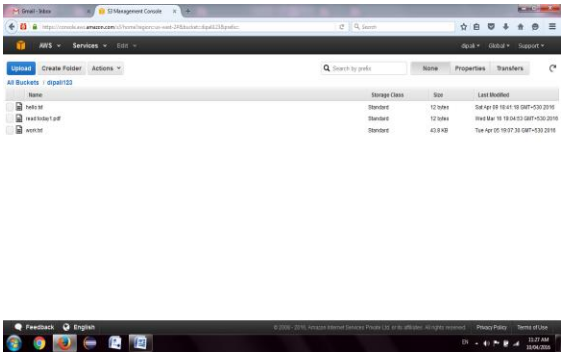

Fig -5: File Upload on S3

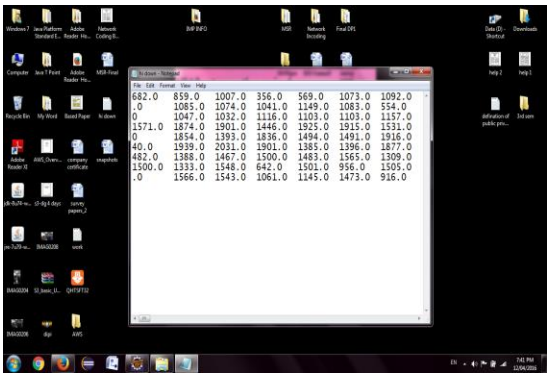

Fig -6: Encoded File

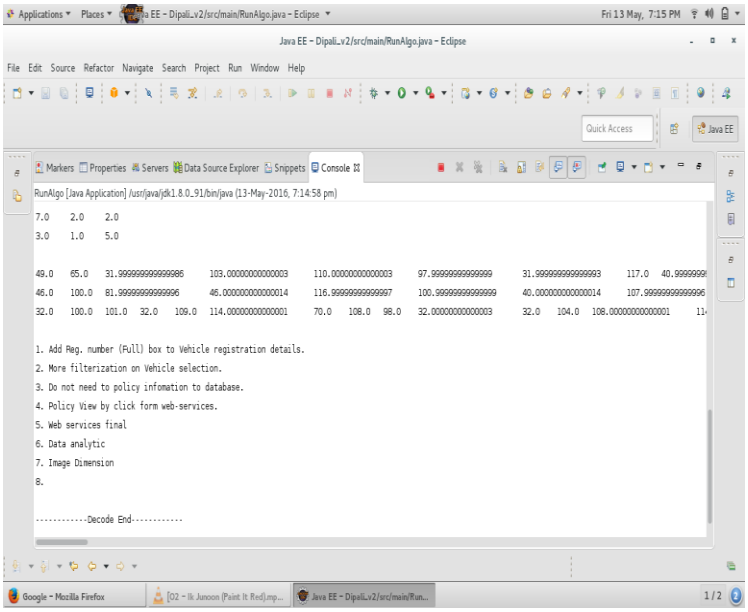

Fig -7: Decoded File

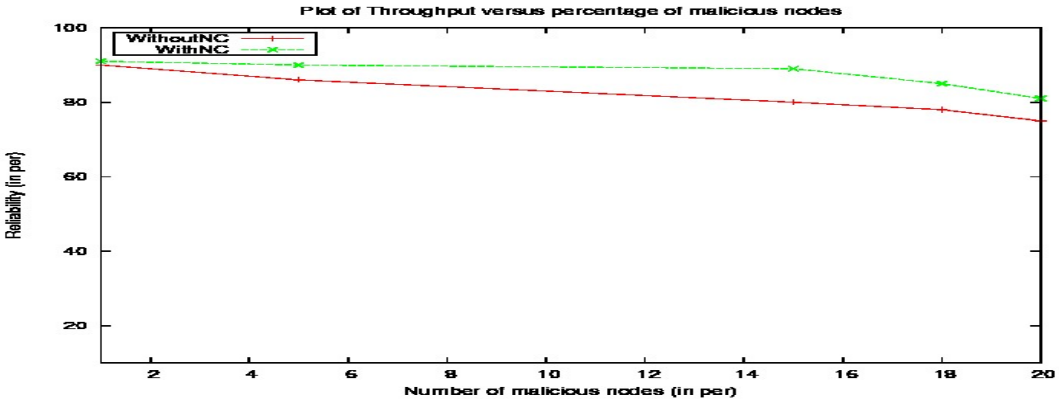

Fig -8: Reliability Graph

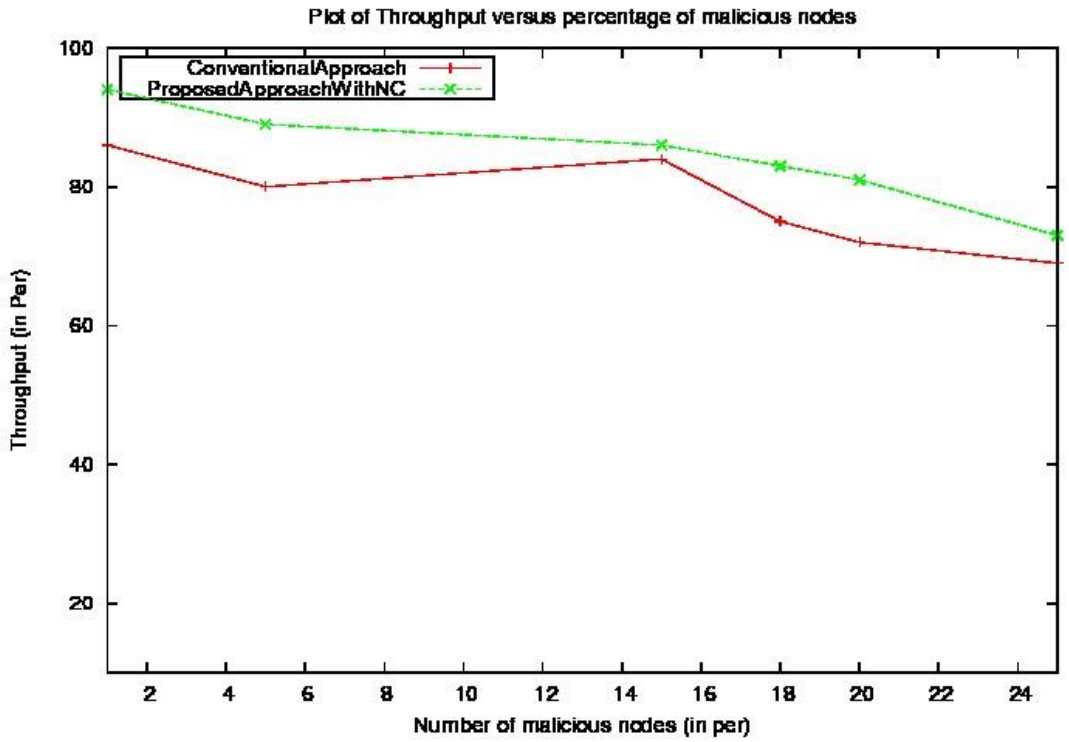

Fig -8: Throughput Graph

These two graphs show the throughput and reliability of data is better with network coding rather than traditional approaches used for data security. In Throughput graph, X axis represent percentage of malicious node introduced in simulation i.e.2%, 4%, 10%, 2% means 2 nodes are malicious out of 100 nodes. In our case node mean user requests and protocol mean two proposed algorithms. Its show we can got more throughput with network coding scheme. So in that graph we achieved more throughput with compared to protocol not consisting of network coding.

So our protocol i.e. with network coding outperforms over conventional protocol i.e. without network coding mechanism. Similarly Reliability means how many successful packets received by introducing malicious nodes. We got more reliability of data as dhow in reliability graph.

6. CONCLUSIONS

The data store in cloud by traditional encryption way cause the data Confidentiality problem we consider the network coding based scheme to Forward and retrieve data because this is very secure way to communication. It will be propose a new data publishing scheme and data retrieval Scheme with provide key security by using RSA algorithm because till now it's most secure asymmetric algorithm which is widely used over Internet for security purpose. So, by proposed scheme we provide more data security in term of provide better data confidentiality with more data reliability in cloud.

7. FUTURE WORK

The future work is with completion of this dissertation now next plan is to do extend this work using homomorphic cryptosystem for better security.

8. REFERENCES

[1]. Neha Kajal, Nikhat Ikram, Prachi " SECURITY THREATS IN CLOUD COMPUTINGT ", International Conference on Computing,Communication and Automation (ICCCA2015)ISBN:978-1-4799-8890-7/15/31:00c 2015IEEE

[2]. Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu "Data Security and Privacy in Cloud Computing" International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903, 9 pages http://dx.doi.org/10.1155/2014/190903

[3]. Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu "Data Security and Privacy in Cloud Computing", International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903, 9 pages http://dx.doi.org/10.1155/2014/190903.

[4].Christina Fragouli , JeanYves Le Boudec , J¨org Widmer "Network Coding: An Instant Primer" ACM SIGCOMM Computer Communication Review Volume 36, Number 1, January 2006

[5]. Mohammed V-Rabat University, tarik CHANYOUR, Rachid SAADANE,"Cooperation based instantly decadable network coding for mobile clouds", 978-1-4673-8224-3/15/31:00c 2015IEEE:

[6]. "A History of Cloud Computing". Computer Weekly.

[7]. T. Mather, S. Kumaraswamy, and S. Latif, "*Cloud Security and Privacy*," O'Reilly Media, Sep. 2009.

[8]. WENTAO LIU, "RESEARCH ON CLOUD COMPUTING SECURITY PROBLEM AND STRATEGY", 978-1-4577-1415-31121 ©2012 IEEE

[9].http://www.techrepublic.com/blog/it -security/the-ciatriadl

[10]. Mircea Georgescu, Natalia Suicirnezov, "Issues Regarding Security Principles In Cloud Computing",The USV Annals of Economics and Public Administration Volume 12, Issue 2(16), 2012.

[11].http://www.techrepublic.com/blog/it -security/the-ciatriadl

[12].http://www.slideshare.net/bharathraob/the-cia-triad 28739772

[13]T. Ho, R. Koetter, M. Medard, D. R. Karger and M. Effros, "The Benefits of Coding over Routing in a Randomized Setting" in 2003 IEEE International Symposium on Information Theory. doi:10.1109/ISIT.2003.1228459