Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 4, April -2017

Enhancing Reliability for Digital Forensic Data in Cloud Computing using Linear Network Coding

Lashkare Hiral N.[1], Gayatri Pandi(Jain)[2]

[1]*Computer Engineering, L.J.E.E.T*
[2] *Computer Engineering, L.J.E.E.T*

Abstract — *Cloud computing is a fast developing technology widely used across industry as well as academia. With the growing popularity of cloud services, the probability of attacks on cloud systems has also gone up drastically. As a result there is a growing demand for enabling cloud systems with forensic capabilities. But, existing digital forensic techniques cannot be directly applied to cloud environments. In this context, at the datacenter level, we need a unified framework that permits reliable virtual and physical resource management, having in the same time the possibility for digital forensic investigators to access the data. Also provide reliability to data is also important concern for that liner network coding used.*

Keywords- *cloud forensic, Digital forensic, cloud computing, Reliability, Network Coding,*

I. INTRODUCTION

Cloud computing is being adopted rapidly by IT organizations and business, it offers a high degree of scalability, low cost computing and convenient pay-as-you-go services. Crime conducted using cloud is increased so need of digital forensic is also increased. The National Institute of Standards and Technology (NIST) define digital forensics as "an applied science to identify an incident, collection, examination, and analysis of evidence data". Maintaining the integrity of the information and a strict chain of custody for the data are mandatory. Digital forensics is the procedure of examining a computer system to determine potential legal evidence.

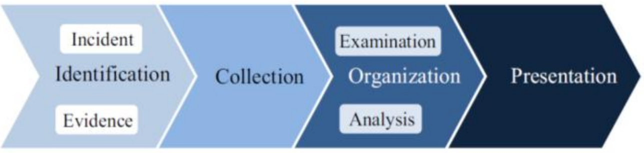


Figure 1. Digital Forensics Process Flow

From the above working definitions, we can state that digital forensics comprises four main processes:

- Identification: There are two main steps in identification: identification of an incident, and identification of the evidence, which will be required for successful investigation of that incident, with potential correlation to other incident(s).
- Collection: Collection is a process that extracts the digital evidence from different types of media e.g., hard disk, cell phone, e-mail, and many other types of data by an investigator. Additionally, preserves the integrity of the evidence by the investigator.
- Organization: Examination and analysis of the digital evidence are two main steps in the organization process. First examination phase, an investigator extracts and inspects the data and its characteristics. Second the analysis phase, investigator interprets and correlates the available data and come to a conclusion, which can serve to prove or disprove civil, administrative, or criminal allegations when interpreted legally.
- Presentation: In this process, an investigator makes an organized report to state his or her findings about the case. This report should be appropriate for presentation to the judge and jury.

II. RELATED WORK

Cloud Alecsandru Patrascu and Victor Valeriu Patriciu proposed the architecture [1] and the modifications needed to be made in order to create a digital forensic compliant framework it has database layer module with multiple building blocks the modifications will start at the physical servers dedicated forensics network port, just like a management port This port will be used by our Cloud infrastructure for collecting and processing data and also it will be used by the authenticated forensic investigators.

Shams Zawoad, Ragib Hasan, and Anthony Skjellum author proposed OCF (open cloud forensic) model [2]; they design a cloud computing architecture, an investigator subsequently gathers relevant verifiable ESI(Electronically stored information) then converted to verified ESI it means cryptographic information and published on internet to verify by authority.

Frank H.P. Fitzek, Tamas Toth, Aron Szabados, Morten V. Pedersen, Daniel E. Lucani, Marton Sipos, Hassan Charaf, Muriel Medard author proposed [3], random linear network coding (RLNC) to generate coded data in our cloud storage systems. RLNC linearly combines uncoded packets into any number of coded packets using random coding coefficients from a finite field plus some additional information referred to as the encoding vector, which comprises the values of the random coefficients used to generate that particular coded packet.

Marton Sipos, Frank H.P. Fitzek, Daniel E. Lucani, Morten V.Pedersen author proposed work [4] focuses on distributed storage solutions using RLNC. In this paper, they present a system that employs commercially available clouds to store files reliably. Proposed system is comprised of a client application that uploads and downloads data to the storage nodes and handles all computations related to encoding, decoding and recoding

Zhengwei Qi, Chengcheng Xiang, Ruhui Ma, Jian Li, Haibing Guan and David S. L. Wei author proposed [5] work for live forensics is an important technique in cloud security but is facing the challenge of reliability. they propose a special purpose hypervisor, called ForenVisor, which is dedicated to reliable live forensics. The reliability is improved in three ways: reducing Trusted Computing Base (TCB) size by leveraging a lightweight architecture, collecting evidence directly from the hardware, and protecting the evidence and other sensitive files with Filesafe module.

III. PROPOSED WORK

As the goal is to develop algorithm that provide reliability to digital forensic data. For that need architecture that have plug-in-play data center and on that data linear network coding apply to provide reliability. For publishing data first user login to cloud controller after authentication cloud controller get data from user and convert forensic data to integer file. Cloud controller use random key using this random key and cloud controller apply linear network coding and generate encrypted data and store new Encrypted data, Random key, UserId to that data and Integrity check value of encrypted data to database. Single data's multiple Encrypted data created and stored at cloud controller side. And only Encrypted data provided to user and that data stored on cloud. For Retrieving data user send request for authentication if user valid cloud controller calculate integrity check value of data if its match than cloud controller decrypt data and provide it to user. If integrity check value doesn't match to data its means data is modified. And for that modified data based on UserID find another copy of data and applying random linear coding cloud controller get back original data and provide that data to user. If data deleted than cloud controller find another copy of data and decrypt data by random linear network coding and give data to user. So using linear network coding we can provide reliability to forensic data.

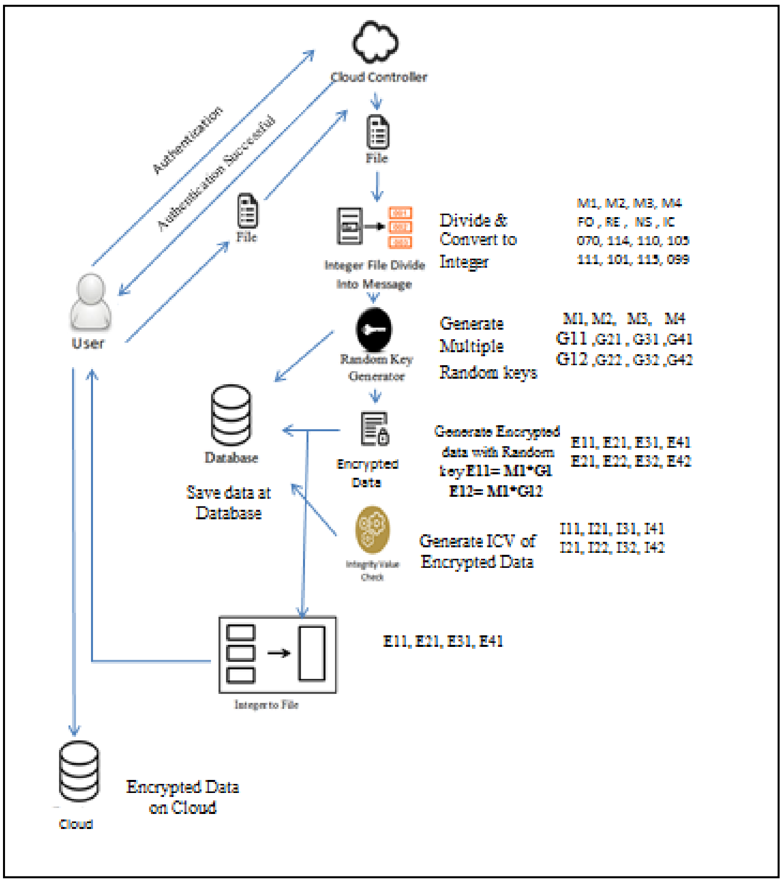


Figure 2. Proposed Architecture for Publishing Data

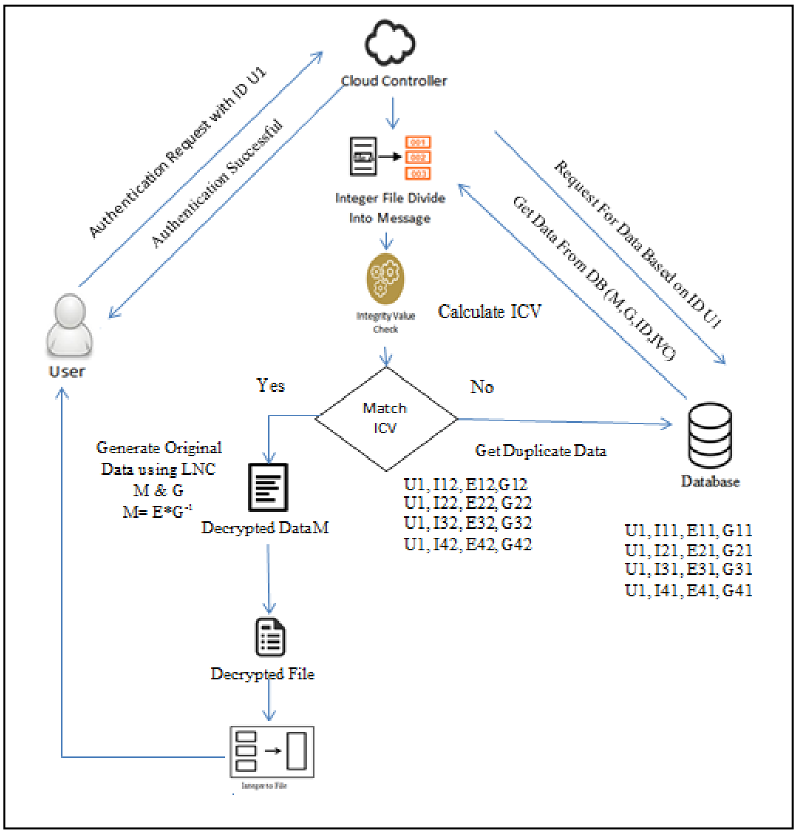
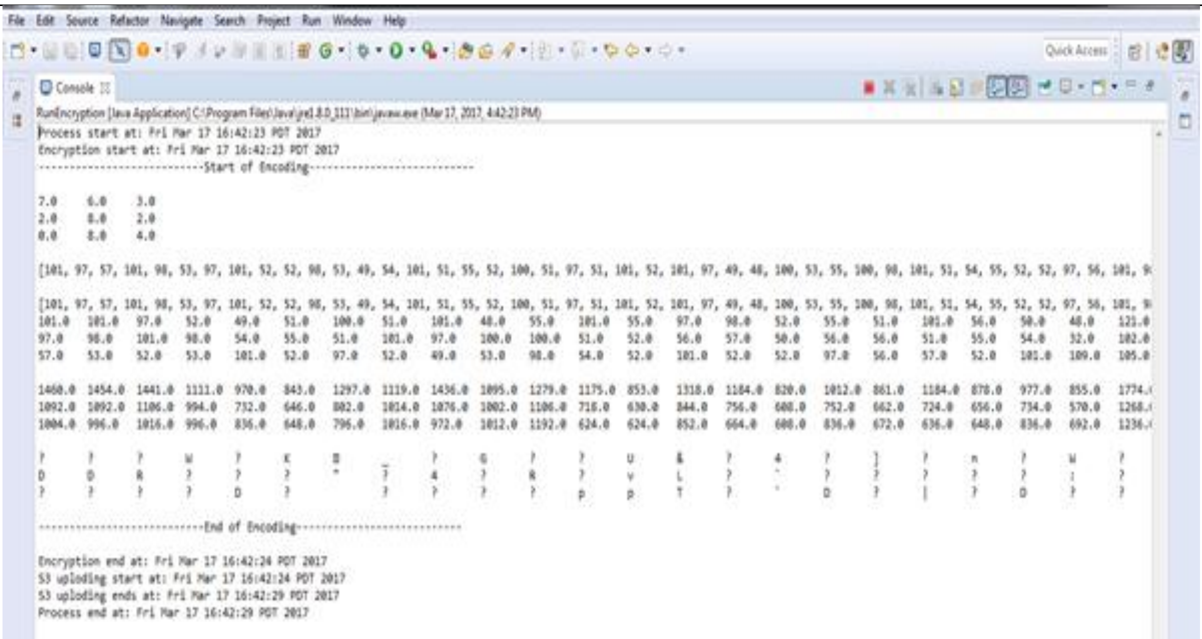


Figure 3. Proposed Architecture for Retrieving Data

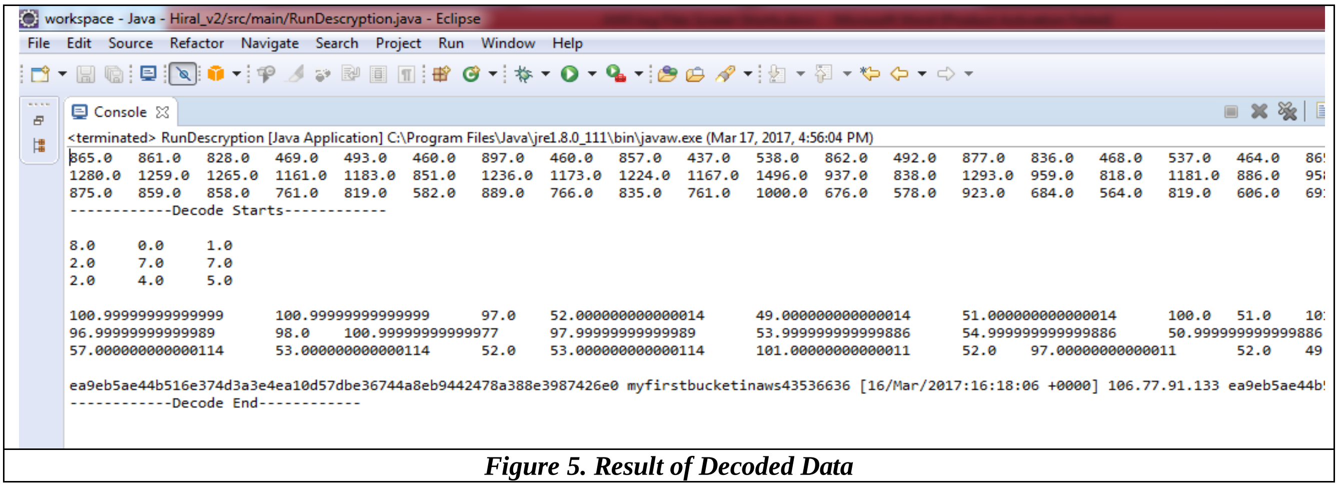
IV. RESULT AND ANALYSIS

Proposed work is implemented and result is generated in that results cloud logs files is converted into integer file and then encrypted and decrypted with linear network coding and hash code is generated on encrypted file. At decryption time hash code is not match then another copy of encrypted file is gated by this way reliability achieved.


File Edit Source Refactor Navigate Search Project Run Window Help
Quick Access
Console

```
RunEncryption [Java Application] C:\Program Files\Java\jre1.8.0_111\bin\javaw.exe (Mar 17, 2017, 4:42:23 PM)
Process start at: Fri Mar 17 16:42:23 PDT 2017
Encryption start at: Fri Mar 17 16:42:23 PDT 2017
---------------------------Start of Encoding---------------------------

7.0     6.0     3.0
2.0     8.0     2.0
0.0     8.0     4.0

[101, 97, 57, 101, 98, 53, 97, 101, 52, 52, 98, 53, 49, 54, 101, 51, 55, 52, 100, 51, 97, 51, 101, 52, 101, 97, 49, 48, 100, 53, 55, 100, 98, 101, 51, 54, 55, 52, 52, 97, 56, 101, 9

[101, 97, 57, 101, 98, 53, 97, 101, 52, 52, 98, 53, 49, 54, 101, 51, 55, 52, 100, 51, 97, 51, 101, 52, 101, 97, 49, 48, 100, 53, 55, 100, 98, 101, 51, 54, 55, 52, 52, 97, 56, 101, 9
101.0   101.0   97.0    52.0    49.0    51.0    100.0   51.0    101.0   48.0    55.0    101.0   55.0    97.0    98.0    52.0    55.0    51.0    101.0   56.0    50.0    48.0    121.0
97.0    98.0    101.0   98.0    54.0    55.0    51.0    101.0   97.0    100.0   100.0   51.0    52.0    56.0    57.0    50.0    56.0    56.0    51.0    55.0    54.0    32.0    102.0
57.0    53.0    52.0    53.0    101.0   52.0    97.0    52.0    49.0    53.0    98.0    54.0    52.0    101.0   52.0    52.0    97.0    56.0    57.0    52.0    101.0   109.0   105.0

1460.0  1454.0  1441.0  1111.0  970.0   843.0   1297.0  1119.0  1436.0  1095.0  1279.0  1175.0  853.0   1318.0  1184.0  820.0   1012.0  861.0   1184.0  878.0   977.0   855.0   1774.
1092.0  1092.0  1106.0  994.0   732.0   646.0   802.0   1014.0  1076.0  1002.0  1106.0  716.0   630.0   844.0   756.0   608.0   752.0   662.0   724.0   656.0   734.0   570.0   1268.
1004.0  996.0   1016.0  996.0   836.0   648.0   796.0   1016.0  972.0   1012.0  1192.0  624.0   624.0   852.0   664.0   608.0   836.0   672.0   636.0   648.0   836.0   692.0   1236.

?       ?       ?       W       ?       K       ▒       _       ?       G       ?       ?       U       &       ?       4       ?       ]       ?       n       ?       W       ?
D       D       R       ?       ?       ?       "       ?       4       ?       R       ?       V       L       ?       ^       ?       ?       ?       ?       ?       :       ?
?       ?       ?       ?       D       ?               ?       ?       ?       ?       P       P       T       ?       '       D       ?       |       ?       D       ?       ?

---------------------------End of Encoding---------------------------

Encryption end at: Fri Mar 17 16:42:24 PDT 2017
S3 uploding start at: Fri Mar 17 16:42:24 PDT 2017
S3 uploding ends at: Fri Mar 17 16:42:29 PDT 2017
Process end at: Fri Mar 17 16:42:29 PDT 2017
```

Figure 4. Result of Encoded Data


workspace - Java - Hiral_v2/src/main/RunDescryption.java - Eclipse
File
Edit
Source
Refactor
Navigate
Search
Project
Run
Window
Help
Console

```
<terminated> RunDescryption [Java Application] C:\Program Files\Java\jre1.8.0_111\bin\javaw.exe (Mar 17, 2017, 4:56:04 PM)
865.0   861.0   828.0   469.0   493.0   460.0   897.0   460.0   857.0   437.0   538.0   862.0   492.0   877.0   836.0   468.0   537.0   464.0   86
1280.0  1259.0  1265.0  1161.0  1183.0  851.0   1236.0  1173.0  1224.0  1167.0  1496.0  937.0   838.0   1293.0  959.0   818.0   1181.0  886.0   95
875.0   859.0   858.0   761.0   819.0   582.0   889.0   766.0   835.0   761.0   1000.0  676.0   578.0   923.0   684.0   564.0   819.0   606.0   69
------------Decode Starts------------

8.0     0.0     1.0
2.0     7.0     7.0
2.0     4.0     5.0

100.99999999999999      100.99999999999999      97.0    52.000000000000014      49.000000000000014      51.000000000000014      100.0   51.0    10
96.99999999999989       98.0    100.99999999999977      97.99999999999989       53.999999999999886      54.999999999999886      50.999999999999886
57.000000000000114      53.000000000000114      52.0    53.000000000000114      101.00000000000011      52.0    97.00000000000011       52.0    49

ea9eb5ae44b516e374d3a3e4ea10d57dbe36744a8eb9442478a388e3987426e0 myfirstbucketinaws43536636 [16/Mar/2017:16:18:06 +0000] 106.77.91.133 ea9eb5ae44b
------------Decode End------------
```

Figure 5. Result of Decoded Data

V. CONCLUTION

After surveying many research methodologies for reliability in digital forensic data in data center get cloud forensic architecture with database storage with forensics manager access and random linear network coding method used for providing reliability to data. Random linear network coding is used for optimize performance, availability, reliability of data. Main objective of work is to provide reliability to forensic data and it can be done by authenticating data user and encoding and decoding data using linear network coding.

REFERENCES

[1] Alecsandru Patrascu and Victor Valeriu Patriciu "Implementation of a Cloud Computing Framework for Cloud Forensics" In International Conference on System Theory, Control and Computing, 2014 IEEE, DOI:10.1109/IAdCC.2014.6779427, pg no. 440-445

[2] Shams Zawod, Ragib Hasan, and Anthony Skjellum "OCF: An Open Cloud Forensics Model for Reliable Digital Forensics" In 8th International Conference on Cloud Computing, 2015 IEEE, DOI: 10.1109/COMSNETS.2014.6734930, pg no. 437-444

[3] Frank H.P. Fitzek, Tamas Toth, Aron Szabados, Morten V. Pedersen, Daniel E. Lucani, Marton Sipos, Hassan Charaf, Muriel Medard "Implementation and Performance Evaluation of Distributed Cloud Storage Solutions using Random Linear Network Coding" ICC'14 - W13: Workshop on Cooperative and Cognitive Mobile Networks , 2014, DOI:10.1109/ICDSE.2014.6974610, pg no. 249-254

[4] Marton Sipos, Frank H.P. Fitzek, Daniel E. Lucani, Morten V. Pedersen "Dynamic Allocation and Efficient Distribution of Data Among Multiple Clouds Using Network Coding" IEEE 3rd International Conference on Cloud Networking (CloudNet), 2014, DOI: 10.1109/CloudNet.2014.6968974, pg no. 90-95

[5] Zhengwei Qi, Chengcheng Xiang, Ruhui Ma, Jian Li, Haibing Guan and David S. L. Wei "ForenVisor: A Tool for Acquiring and Preserving Reliable Data in Cloud Live Forensics" IEEE Transactions on Cloud Computing , Volume: PP, Issue: 99, DOI: 10.1109/TCC.2016.2535295, pg no. 1-14.

[6] Sameera Almulla, Youssef Iraqi and Andrew Jones "Cloud forensics: A research perspective" Computer published by the IEEE computer society, 2013 IIT'13 1569711939, pg no. 1-6

[7] Rajkumar Buyya et. el., Cloud Computing: Principles and Paradigms, Wiley India Edition