ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Anomaly Detection with Cryptographic Operations and Transient secrets in CipherXray

Rupali Gharde, Archana Augustine

M.E. Student, Pillai HOC College of Engineering & Technology, Rasayani, Mumbai University, Maharashtra, India

Professor, Dept. of I.T., Pillai HOC College Of Engineering & Technology, Rasayani, Mumbai University, Maharashtra, India

ABSTRACT: Cloud computing is considered to be the most strategic technology. Many algorithm gets failed to handle the security of the remote data in case of cloud computing. Although a new approach using CipherXray has satisfactory workaround to protect and prevent our data, as with most of the techniques it uses end-to-end encryption for data security.End- to - end Encryption is a very simple way in which your data will be fully secured, even not able to readable by their servers. It will secure your messages and calls at highest possible security. This method gets failed if anonymous user misuses it, and we are not being able to read their messages. With end-to-end encryption there will be a possibility of law and order being overlooked at the face of confidentiality of users. It is necessary to track suspected activities of users. A technology called Anomaly detection is used to manage the risk of information misuse by anonymous users, which can track and identify users and their activities.

KEYWORDS: Cloud computing, Anomaly Detection, Information security, End-to-End encryption.

I. INTRODUCTION

Cloud computing has opened up a new world of opportunities and new way of data storing and sharing. There are many security challenges which need to be handled.To implement a cloud computing strategy, we need to place critical data in the hands of a third party and those are not fully trustworthy. It is most important to ensure that the data remains secure both at rest means when the data residing on storage media as well as when it is in transit. For security reasons data needs to be encrypted at all timesoperations.

Many methods have been used to make remote data secure in the cloud using encryption techniques and standard access controls. All of these approaches get failed for a variety of reasons, so building only trustworthy cloud computing environment is not enough. Instead, we need to use a different approach, otherwise accidents will continue to happen and information will get lost.A novel technique called CipherXray[1] can be able to protect and prevent the data from being modify.CipherXray is a hybrid algorithm which contains symmetric algorithm RSA, asymmetric algorithm AES and SHA hashing algorithm. It uses end-to-end encryption technique but this method gets failed if anonymous user misuses it, and we are not being able to read their messages.

Existing system's ability is contained to end-to-end encryption only. For achieving more security and privacy in our existing system, we are managing risk of information misuse by anonymous users. To achieve this, we will keep track and identify suspected activities of the user using anomaly detection technique so that we can prevent from misuse of our system.

II. RELATED WORK

In [2] authors proposed a new security model which uses hybrid symmetric encryption method for more security. In this data owner stores encrypted data to cloud server. This will make data hidden from anonymous users and only authorized users can be able to access the data with corresponding decryption key. The main disadvantage with this method is key transportation, it is not safe to share a key with receiver. In [3] author proposed a system with hybrid

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

cryptographic algorithm and steganography. Hybrid algorithm contains AES, RC6, blowfish and BRA algorithms. It will give block wise security to data. Each file is distributed into eight parts, each and every part is encrypted using different algorithm simultaneously. Data encryption keys are inserted into cover image using LBS technique and stego image is then send to valid receiver using email.

Most of the techniques performs end-to-end encryption, where the user initiates the encryption from source to destination. This also provides greater flexibility to the user in deciding which data to encrypt. Most widely used social networking applications chosen an end-to-end encryption to all of its messages. Earlier there have been security concerns of common people who are constantly worried that their privacy could be easily invaded and that sending or receiving pictures or videos over the app could actually be unsafe. With the end-to-end encryption technique, your messages are so safe that even their server couldn't get access to them even if they wanted to. With every advantage, there were disadvantages too. We aware of the fact that nobody is tracking what we are sending, there is a possibility of crime and misuse of technology. Law and order being overlooked, when the government would not be able to access information that is suspected or needs to be investigated. It would be like ignoring the safety of citizens from fraudsters and terrorists for giving priority to messaging privacy.

The end-to-end encryption system is making users happy but at the same time it is increasing the possibility of braking law and order. People would no longer be worried about the person's identity who could be a suspect and they would no longer have to fear for being involved with a wrong person.

The above requirements can be accomplished by using Anomaly Detection techniques which will be able to track and identify suspected activities of users. It is also very essential to prevent data from being modified. CipherXray is a techniques which will add more security to the system.

III. PROPOSED SYSTEM

A. *System Architecture:*

This paper proposes a system which will track and identify suspected activities of users using Anomaly detection technique and enables more security. It consist of 5 different modules- user module, anomaly detection module, cloud service provider or administrator module, encryption and decryption module. In the proposed system, before uploading or downloading a file to the cloud it will be checked for anomaly detection using Parallel Hybrid Feature Selection Algorithm. This algorithm will divide the file into sections and then analyse them in parallel to each other. This will take less time and make system more efficient as compared to the existing system. If anomaly is detected then the signal isgiven to the administrator. Administrator can be able to view and detect the person who has uploaded the file to cloud. If file is not detected for anomaly then encoding or decoding is performed on the file and then file is uploaded or downloaded to or from system. In this way proposed system make sure that system will not get compromised by anonymous data.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

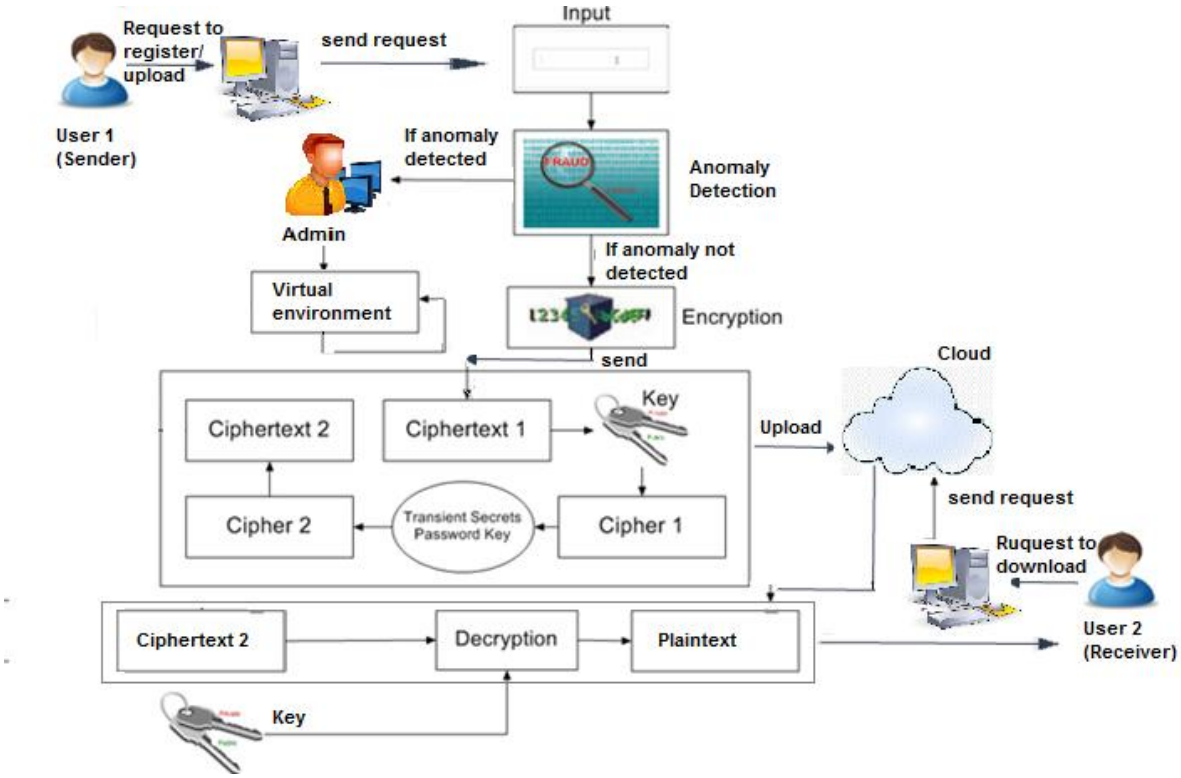

Figure 1: System Architecture

- Sequentially, providing a secure and flexible cryptography mechanism raises the needs for analyzing and comparing different encryption algorithms for the aim of enhancing the security during the encryption process.
- Hence, this paper suggested a cryptography mechanism in the block cipher by managing the keys sequentially.
- These keys will works dependently for extracting and generating the content relation to be managed later by the key management that helps to communicate and share sensitive information.
- In particular, the importance of thorough, consistent key management processes among public safety agencies with interoperable functions cannot be overstated.
- This model aims to secure dissemination, loading, saving, and eliminating faults of keys to make encryption implementations effective.
- There are inherent possibilities if suitable key management processes are not accompanied because of the intricacy of dispensing keys to all block in a certain fashion. This risk can be meaningfully appeased through sufficient key controls and proper education on encryption key management.
- Getting Confirmation from the receivers side before transmitting the data
- Cost efficient process and really nice Performance.
- Anomaly detection be the another technique introduced in this dissertation where before ciphering data it will be first checked for presence of anomaly by using anomaly detection filter where given data is checked forpresence of fraud related words like bomb, theft, kill etc. if detector gives positive result it means anomaly is present and that document is not processed further.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

B. *Goal of the System:*

The goal of the proposed system is to,

1. Track and Identify suspected activities of users.
2. Protect and prevent the data modification.
3. Makes the system more efficient and secure.

IV. SIMULATION RESULTS

1. Detects the fraud users.
2. Administrator can be able to monitor suspected users and their activities, and will take necessary action.
3. Take less time for detection.
4. More efficient as compared to existing system.

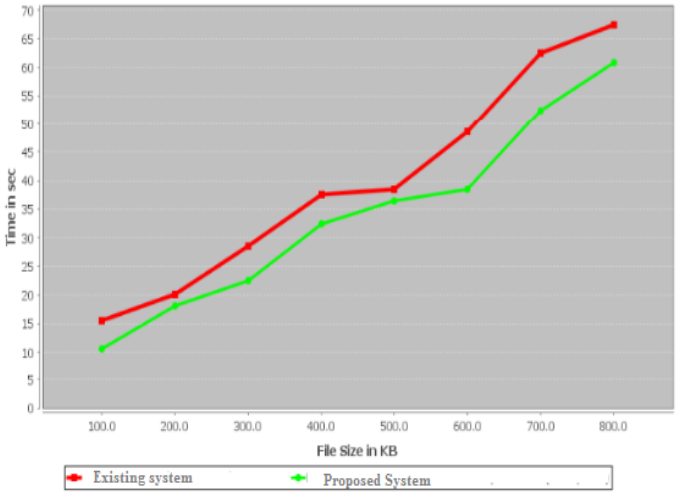

Fig.1.Ratio of Detection time

In this graph x axis denotes file size in kb and y axis denotes the time in sec. This graph shows that our proposed system is more efficient. When compared with existing systems,our proposed system will take less time for detection.

V. CONCLUSION AND FUTURE WORK

As an End-to-End encryption scheme gives freedom of sending messages without any concern of monitoring, but there is a possibility of misuse of technology. In this project we propose Parallel Hybrid Selection Algorithm that has been used for anomaly detection, which will keep track of anonymous activities. This algorithm will divide the file into sections and analyze them in parallel. Hence, it achieves more security and also prevents possible type of attacks. It is very essential to prevent our data from being modified. CipherXray technique is used to identify the modified data in the file. It will ensure system performance and make the system more efficient.

Anomalies and cryptography might be induced in the data for a variety of reasons, such as malicious activity, for example, credit card fraud, cyber-intrusion, terrorist activity or breakdown of a system, but all of the reasons have the common characteristic that they are interesting to the analyst. The interestingness or real life relevance of anomalies is a key feature of anomaly detection with Cryptographic Operations.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

There are several promising directions for further research in anomaly detection. Contextual and collective anomaly detection techniques are beginning to find increasing applicability in several domains and there is much scope for development of new techniques in this area. The presence of data across different distributed locations has motivated the need for distributed anomaly detection techniques.

REFERENCES

1. XIN LI, XINYUANWANG AND WENTAOCHANG,"CIPHERXRAY: EXPOSING CRYPTOGRAPHIC OPERATIONS AND TRANSIENT SECRETS FROM MONITOREDBINARY EXECUTION,"IEEE TRANSACTIONS ON DEPENDABLE SECURE COMPUTING, MARCH/APRIL2014.
2. SHWETAKAUSHIK AND CHARUGANDHI, "CLOUD DATA SECURITY WITH HYBRID SYMMETRIC ENCRYPTION," INTERNATIONAL CONFERENCE ON COMPUTATIONAL TECHNIQUES IN INFORMATION AND COMMUNICATION TECHNOLOGIES (ICCTICT), MARCH 2016.
3. PUNAM V. MAITRI AND ARUNAVERMA,"SECURE FILE STORAGE IN CLOUD COMPUTING USING HYBRID CRYPTOGRAPHY ALGORITHM,"IEEE WIRELESS COMMUNICATIONS, SIGNAL PROCESSING AND NETWORKING (WISPNET), MARCH 2016.
4. SUNILKUMARGAUTAM AND HARIOM, "ANOMALY DETECTION SYSTEM USING ENTROPY BASED TECHNIQUES," NEXT GENERATION COMPUTING TECHNOLOGIES (NGCT), SEPTEMBER 2015.
5. RASHMIGOURKAR AND GARIMASINGH, "BLOCKING MISBEHAVING USER & ACTIVITIES IN SOCIAL NETWORK," INTERNATIONAL JOURNAL OF SCIENCE AND RESEARCH (IJSR),APRIL 2016.
6. ASHALATHA R, JAYASHREEAGARKHED, AND SIDDARAMAPATIL," DATA STORAGE SECURITY ALGORITHM FOR MULTI CLOUD ENVIRONMENT," INTERNATIONAL CONFERENCE ON ADVANCES IN ELECTRICAL, ELECTRONICS, INFORMATION, COMMUNICATION AND BIO-INFORMATICS (AEEICB 16) , FEBRUARY 2016.
7. KALYANIGANESHKADAM AND PROF. VAISHALIKHAIRNAR,"HYBRID RSA-AES ENCRYPTION FOR WEB SERVICES", INTERNATIONAL JOURNAL OF TECHNICAL RESEARCH AND APPLICATIONS, SEPTEMBER 2015.
8. PRAVEEN J U AND P JAYAREKHA, "IDENTIFYING THE MISBEHAVING USER IN A NETWORK AND TRAPPING THEM USING HONEYPOT", INTERNATIONAL JOURNAL OF INNOVATIVE SCIENCE AND MODERN ENGINEERING (IJISME), MAY 2014.
9. NIKITA L. VIKHAR AND G. R. BAMNOTE, "MISBEN: RELIABLE AND RISK FREE APPROACH OF BLOCKING MISBEHAVING USERS IN ANONYMIZINGNETWORKS ", INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND EXPLORING ENGINEERING (IJITEE), MAY 2013.
10. FADHISALMAN ABED, "A PROPOSED METHOD OF INFORMATION HIDING BASED ON HYBRID CRYPTOGRAPHY AND STEGANOGRAPHY", INTERNATIONAL JOURNAL OF APPLICATIONS OR INNOVATION IN ENGINEERING & MANAGEMENT, APRIL 2013.
11. L. AROCKIAM AND S. MONIKANDAN, "DATA SECURITY AND PRIVACY IN CLOUD STORAGE USING HYBRID SYMMETRIC ENCRYPTION ALGORITHM", INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER AND COMMUNICATION ENGINEERING, AUGUST 2013.

BIOGRAPHY

Rupali Gharde is a Student of the Information Technology, College of Engineering, Mumbai University. She received Bachelor of Engineering (BE) degree in 2011 from SOLAPUR, Maharashtra, India. Her research interests are Information security (wireless Networks), Algorithms, Cryptography, web 2.0 etc.