ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

A Service Level Agreement based Implementation of Security in Distributed Storage System

Shruthi Shetty J[1], Manjunath Kotari[2]

Department of Computer Science, Alva's Institute of Engineering and Technology, India[1]

Associate Professor & Head, Computer Science, Alva's Institute of engineering and Technology, India[2]

Abstract: The concept of Distributed Storage System (DSS) on to the Computing systems nowadays has a wide range of usage and applications. The most important criteria with regard to the storage are security, i.e ensuring the correctness of the data stored by the customers. Data which has to be distributed across multiple networks are most probably vulnerable to various attacks by number of malicious elements. Security in distributed Storage Systems is adopted by Cryptographic splitting the data through Service Level Agreement (SLA) layer. An SLA is a formal contract base, which guarantees that consumers needed services and the quality expectation of obtained services can be achieved.SLA is considered as the legal foundation for the customers from the service provider for the service delivery. The parties involved with SLA are users of SLA. Data is split using some adaptive algorithm like Rijndahl algorithm, which is the winner algorithm of Advanced Encryption Standard (AES). The split data is stored in different distributed storage systems where counter measures are to be taken to get the complete data, since the data is encrypted using an algorithm when it is stored in the different storage systems. The proposed system also considers the Trusted Third Party (TTP) who is not the owner of the data, still manages to secure the data stored in the Distributed Storage System. When there is the constraint on storage space in personal PC's of Individuals, governments sectors and private institutions such as banks, Insurance companies, hospitals and other business enterprises will only consider to store their secrets to a computer system if they can be absolutely certain of confidentiality. Hence this method provides complete security on the confidential data.

Keywords: DSS, SLA, Rijndael, TTP, Security.

I. INTRODUCTION

The modern era of Computer and Networks is all about that multiple computers working in a group in order to exchange information. Collaboration of Computers with each other, have led to very important applications in today's world for the purpose of communication, information exchange, processing, data transfer and storage. [1]. There is a common misconception that distributed system and Computer Networks are to be the same. Going with conceptual meaning of the concept, it is determined that Computer Networks and Distributed systems are different.

A computer networks is an interconnection of autonomous computers that communicates with each other. A user using a computer network understands that he uses different resources lying on different computers as a computer network does not hide the existence of multiple computers. But a distributed system on the other hand provides the feeling that the user is working on a single homogenous more powerful computer with more resources. The existence of multiple autonomous computers is transparent to the user as the distributed system application that is running on the computers would select suitable computers and allocate jobs without the specific intervention of the user.

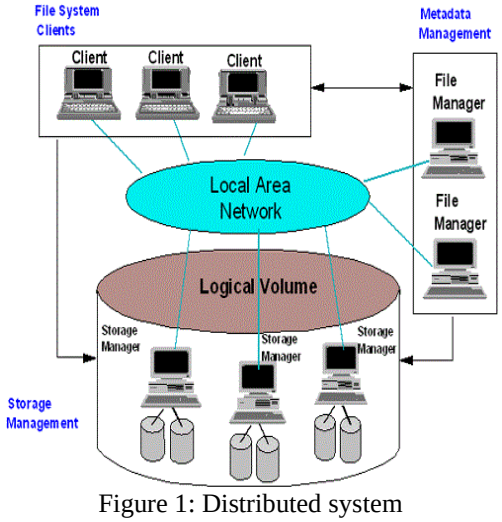

Figure 1: Distributed system

There are many distributed systems in operation today. The following are some of the most popular distributed systems in use today.

a. Distributed Storage Systems.
b. Distributed Databases.
c. Cluster Computing.
d. Grid Computing.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

A. Distributed storage systems

This paper concentrates on one of the Distributed Systems which is Distributed Storage systems (DSS), and it presents the security implementation on this system. Distributed Storage systems are the combination of networking and storage. Evolution of private Local Area Network (LAN) to public Wide area network (WAN) rose the new generation of DSS's which serves audience globally. The main objective of distributed storage systems is to protect the data in case of disk failure across multiple devices through duplicating (redundant) storage and to make data available in massively distributed system. There are mainly four types of distributed storage systems. There are namely,

- Server Attached Redundant Array of Independent Disks (RAID)
- Centralized RAID
- Network Attached Storage (NAS) and
- Storage Area Network (SAN).

The most popular distributed storage techniques out of the four SAN and NAS

B. Security in distributed storage systems

The most important concern with regard to the distributed storage system is management of the data stored in the storage devices of the system. The data is the most important resource in DSS's and hence it has to be labeled and protected properly. Therefore any protection system introduced must not only protect the data stored after the security scheme is installed but also the data that had been there prior to the introduction of that scheme. In other words, protection methodology introduced must be backward Compatible. A security issue that has to model is Confidentiality, Integrity, Availability and Authentication.[1]

II. RELATED WORK

According to Hasan et al., CIAA model (Confidentiality, Integrity, Availability and Authentication) identify the different threats on the distributed storage system and then they are organized under the class of CIAA, and provide protection techniques for the given class that can be used to bypass the threats. Classes of CIAA constitute class under Confidentiality, Integrity, Availability and Authentication. Based on the classical security principles and data life cycle model two different processes for creating the threat model for storage system has been proposed.[3]

The ultimate purpose of threat modeling with CIAA model is to organize system threats and vulnerabilities into general classes and then to be addressed with known storage protection techniques. The process concerns with some minor limitations, while atempting to group the different possible threat which is tedious task, and in some cases it is not possible.

The listed attacks will be outdated when new different attacks start emerging in the DSS.

The Data Lifecycle Threat Model Process addresses different types of physical attacks related to storage systems and also improves the quality of standards and interoperability of various storage systems. But the protection technique to be addressed for the threats detected using this standard exist only for a subset of the threats in the storage systems rather addressing all the identified threats.[3]

Dikaliotis, Dimakis and Ho have proposed a linear hashing technique which can detect errors in the storage nodes in the distributed storage systems specifically which is encoded. The Mutually Cooperative Recovery (MCR) mechanism makes possible the system to recover data in situations of failure of multiple nodes. MCR mechanism works on Multiple Node failure and hence the data will be protected. MCR stands better than other 2 protection mechanism in terms of storage cost and maintenance bandwidth.[2] But MCR transmission and coding schemes are mathematical implementations and hence it is very hard to implement.

III. EXISTING SYSTEM

Security policies are enforced with the help of security mechanisms.

A. The role of cryptography

Cryptography is the science that for encrypting the data by generating secret key to ensure the confidentiality of important information of any individual or organization. Confidentiality is the main goal of cryptographic systems a certain degree of integrity assurance is packaged as the side effect of encryption. The data which can be modified by unauthorized malicious programs or users, by placing information with Worms and Trojans, becomes nearly impossible if the data is under the control of cryptographic functions. Hence this involves encrypting the data into user unreadable format, and getting back the data whenever it is required by decrypting it using same or by different key.

C. Digital signatures

Digital signatures is one more essential requirement for strong and the secure systems. They are needed in order to protect by certifying certain information by providing trustworthy statements which binds user's identities to their public keys or which binds some access rights or roles to users identities.

D. Firewall security

Firewall is a network security system designed to provide unauthorized access to the private network. Firewall is implemented both in hardware and software or combination of both. Any information that is entering the private network has to pass through the firewall where each messages and blocks are examined which does not meet security criteria. These are some of the security measures under taken for the security of DSS. The proposed system advances with a kind of advanced technique for ensuring the security in Distributed Storage System.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

IV. PROPOSED SYSTEM

The proposed system is a combination of 2 different Methodology.

A. SLA (Service Level Agreement)

An SLA is a formal contract base, which guarantees that consumers need services and the quality expectation of obtained services can be achieved. SLA is considered as the legal foundation for the customers from the service provider for the service delivery. The parties involved with SLA are users of SLA [5]. Beyond the SLA layer the security mechanism is enhanced. Any kind of data such as documents, images, audio and video can be secured using this methodology.

B. Storage security using Cryptographic Splitting of data.

Cryptographic splitting is an algorithm which splits the information into n shares. The split part is encrypted using some adaptive algorithm and then stored in the distributed storage system. When there is a need to access the information, first it is decrypted and then it is combined to form the original data. The method seemed to more secure since the parts are encrypted using different key which are generated randomly. Each part is encrypted using different keys and when there is a need to decrypt the data same key is used for decrypting. The encrypted parts are stored in the different distributed system and are decrypted when they are accessed. The algorithm used is Rijndael Algorithm which is the winner algorithm of Advanced Encryption Standard (AES). Rijndael is the AES winner algorithm. It's a Symmetric key Cryptosystem. Allows only 128, 192, and 256-bit key sizes. Different Rounds are set-up, where each round is uniform. [6] The proposed system also has a module named Trusted Third Party (TTP) in order to manage the random key generation. Hence TTP is responsible for overall management of Random key generation.

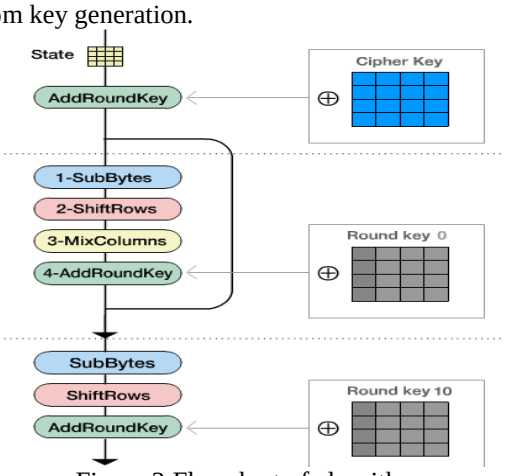

Figure 2:Flowchart of algorithm

Each round has the following 4 steps.

Sub Bytes (byte-by-byte substitution using an S-box)

Shift Rows (a permutation, which cyclically shifts the last three rows in the State)

Mix Columns (substitution column wise that uses Galois Fields)

Add Round key (bit-by- bit XOR with an expanded key)

The figure depicts the overall system design.

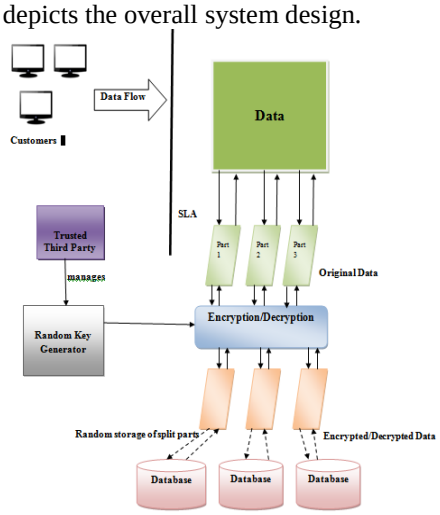

Figure 3:System design for security in Distributed Storage System

V. CONCLUSION

Storage plays a fundamental role in computing, whereas distributed storage is also the major concern. The stored data has to be confidential and integrity has to be preserved. In other words data has to be secured. Security is the major challenge in Distributed storage system. To cope up with this challenge innovative methods and processes has been recognized.

One such method is cryptographic splitting through SLA layer. In this method data is split, encrypted and stored in different distributed storage systems. The split parts are encrypted using key generated by Random Key Generator. There is also a separate TTP which manages the overall key generation. Hence the methodology implemented is unique and innovative. The most important resource in any storage system is data. Hence it is protected using this proposed system.

REFERENCES

[1] Mohamed Firdhous ,Faculty of Information Technology, University of Moratuwa, Moratuwa, Sri Lanka,Mohamed.Firdhous@uom.lk – "Implementation of Security in Distributed Systems A Comparative Study".

[2] Yuchong Hu, Yinlong Xu, Xiaozhao Wang, Cheng Zhan, and Pei Li, "Cooperative Recovery of Distributed Storage Systems from Multiple Losses with Network Coding," IEEE Journal on Selected Areas in Communications, vol. 28, no. 2, pp. 268-276, February 2010.

[3] Ragib Hasan, Suvda Myagmar, Adam J Lee, and William Yurcik, "Towards a threat model for storage systems," in Proceedings of the 2005 ACM Workshop on Storage Security and Survivability (StorageSS '05), FairFax, VA, USA, 2005, pp. 94-102.

[4] David Dodgson, Unisys-" Storage security Cryptographic splitting".

[5] Linlin Wu and Rajkumar Buyya "Service Level Agreement (SLA) in Utility Computing Systems Cloud Computing and Distributed Systems (CLOUDS) Laboratory".

[6] http://www.securityfit.cz/download/kib/rijndael_ingles2004.sw