ROBUST SECURITY SCHEME FOR BIG DATA IN DISTRIBUTED STORAGE SYSTEM

S.YUVARANI
DEPARTMENT OF CSE
PAAVAI COLLEGE OF ENGINEERING
ramyaapce@gmail.com

G.TAMILSELVI
DEPARTMENT OF CSE
PAAVAI COLLEGE OF ENGINEERING
tamilselviganesan24@gmail.com

P.JAYABRUNDHA
DEPARTMENT OF CSE
PAAVAI COLLEGE OF ENGINEERING
brundha31@gmail.com

1. ABSTRACT

Businesses are now collecting and using a huge amount of data. Much of this flows from an increasing range of smart devices, all interconnected as the IOT (Internet of Things). In business, highly sensitive information is stored, and it's necessary to observe government regulations to protect consumers. The design of secure remote user authentication and key agreement schemes for big data applications is still open and challenging. In this paper we proposed elliptic curve cryptography for mutual authentication and key agreement scheme for big data environment in distributed storage system which not only resolves the security weaknesses of schemes proposed till date but also extends the scheme to provide user anonymity which is one of the most desired features of big data systems. The proposed scheme thus provides more efficiency and security from any type of system intrusion. Open key conceal algorithm used to encrypt the data security consideration and then auditing result not only achieves the fast data error identifying the misbehaving server.

2. INTRODUCTION

Distributed storage system (DSS) is an emerging technology and has drawn a lot of attention from the Telecommunications industry. DSSs are used to store data reliably for a long period of time. A DSS is a collection of storage nodes which are distributed across a wide geographical area and are individually unreliable .Applications include large data centers and peer-to-peer storage clouds. In order to ensure the system reliability, data are stored redundantly on the storage nodes. Besides, a self-sustaining DSS must be able to repair failed nodes. The

most straightforward strategy of redundancy is replicating the data in multiple storage nodes. This method, though simple, has low storage efficiency. Another strategy is erasure coding which can offer better storage efficiency by using maximum distance separable codes Performance robustness is rarely studied for storage systems; however, it is very important for many large-scale applications. For example, interactive applications .the access latency to be robust in parallel processes, robust performance can reduce the synchronization overhead; robust performance also makes it easy to predict resource requirement and to schedule resources efficiently. Robust performance is the major goal of Robust. At the same time, we must maintain high access bandwidth and efficient storage space utilization. In a centralized storage system, data and files are managed by a central component.

3. LITERATURE SURVEY.

1. AUTHOR: Aliyu Lawal Aliyu, Peter Bull & Ali Abdullah

TITLE: A trust management framework for network applications within an SDN environment.

DESCRIPTION: The separation of control and data plane requires the controller to be logically centralized , and therefore maintain global knowledge of all the network states, which provides a means of developing more sophisticated network functions like routing, switching, load balancing and intrusion detection/prevention systems .

ADVANTAGES: privilege permissions.

DISADVANTAGES: Smart light and mitigate the issue of performance bottlenecks and single point of failure.

2. AUTHOR: Anders Fongen and Geir Køien

TITLE: Trust management in tactical coalition software defined networks.

DESCRIPTION: To trust management in tactical Software Defined Networks (SDN) when used with mobile nodes in a coalition operation. We analyze the problem space and suggests a set of security and constructional requirements, as well as an analysis on how existing technology may contribute to a solution.

ADVANTAGES: Even with a single security class data flowing in the SDN instance, robust flow separation is required.

DISADVANTAGES: user data traffic, since the control traffic flows (to and from the SDNC) are cryptographically separated from user data.

3. AUTHOR: Bassey I song, Tebogo Kgogo, Francis Lugayizi and Bennett Kankuzi.

TITLE: Trust Establishment Framework between SDN Controller and Applications.

DESCRIPTION: SDN controller can easily be attacked if these applications are malicious or compromised by an attacker to control the entire

network or even result in network failure since it represents a single point of failure in the SDN.

ADVANTAGES: SDN controller is protected and multitude of applications that regularly consume network resources are always trusted throughout their lifetime.

DISADVANTAGES: the controller being a single point of failure in the SDN can be protected given different sophisticated attacks.

4 PROPOSED SYSTEM

Big data analytics provide promising solutions to the management of this massive data. Distributed storage is the default technique for storing data in all new generation applications. The data from a file is stored in a decentralized manner on several unreliable nodes/disks that when collectively used are capable of recovering the entire file. Security of this big data storage need more today so we implementing ECC based protocols gained popularity and are the strongest public-key cryptographic systems known today. Compared with RSA, Rabin and Elgamal cryptographic systems, ECC has remarkable strength and efficiency advantages in terms of bandwidth, key sizes and computational overheads. They also eliminate the problem of key distribution and digital signatures as with traditional symmetric key cryptosystems. Thus ECC when used in password authentication and update schemes provide high security at a reasonable computational cost. In this paper, we proposed to use Open Key conceal Algorithm based on Symmetric Algorithms for security consideration on which one should be used for Cloud based applications and services that require data and link encryption. The Third party user is also one cloud server. The auditing result not only achieves the fast data error identifying the misbehaving server

ADVANTAGES:

Simple: to deploy, manage and maintain in the highly dynamic SDN environment.

Cost-effective: to ensure security can be deployed everywhere.

Secure: to protect against the latest advanced, targeted threats facing your organization.\

It also eliminate the problem of key distribution and digital signatures as with traditional symmetric key cryptosystems.

Security of this big data storage need more today so we implementing ECC based protocols gained popularity.

BLOCK DIAGRAM:

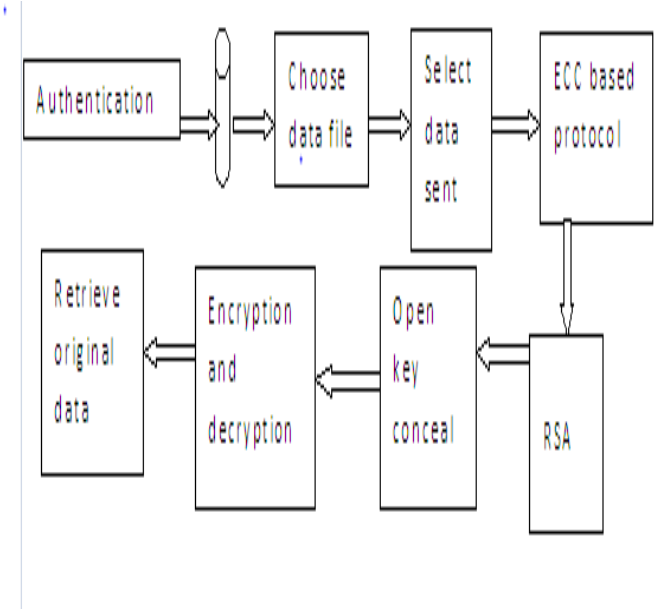


Fig-1 robust security scheme for big data in distributed storage system

MODULE DESCRIPTION

Authentication

In authentication module, we should get authorization to enter into the project. Unauthorized person does not allow executing this operation. To get authentication, we have to give username and password.

Choose the data file

In this module, we have to choose the required data file to transfer from source to destination. The authorized user can send the required file and that person only know about source file.

Send selected data

In this module, the choose data file will be send to another user. In source end one user will send the selected data and another user will receive that file in destination end.

Encryption

In encryption module, the original file transferred by one user, which has to convert to another format. The encryption method is used to done this operation. The common key will be used to identify the original data.

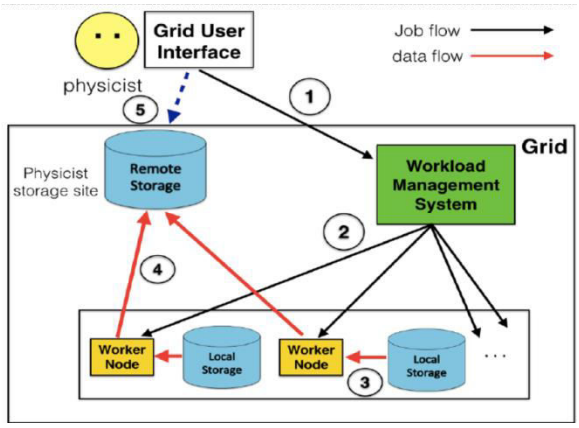
Decryption

In decryption module, the original data will be retrieved by done the decryption method. Here the same key will be used by another user in destination end. The common key is known by authorized user only.

Retrieve original data

In this module, our original data will be displayed by using decryption operation. The required data will transfer to destination end. The framework will be enhanced to ensure seamless and secure execution of the network functions of the underlying Software Defined Network platform.

Data flow Diagram



APPLICATIONS

Visual basic .net comes with features such as a powerful new forms designer, an in-place menu editor, and automatic control anchoring and docking. With visual basic .net we can create web applications using the shared web forms designer and the familiar "drag and drop" feature.

FUTURE ENHANCEMENT

The cloud servers work scheduling is based on the work load for the particular server. Scheduling is perform to reduce the time delay for the user request to search and provide a particular data. If many users are searching a data in server, then the server work load is split into multiple to provide an efficient.

CONCLUSION

Software Defined Network (SDN) platform provides a flexible execution platform for running different Network Control and Management Functions. These network functions are driven by heterogeneous and complex network policies defined by different administrators through distributed Application and Management Servers. The design of secure remote user authentication and key agreement schemes for big data applications is still open and challenging. Security of this big data storage need more nowadays so we implementing ECC based protocols gained popularity and are the strongest public-key cryptographic systems.

REFERENCES

1. Aliyu Lawal Aliyu, Peter Bull & Ali Abdullah" A Trust Management Framework for Network Applications within an SDN Environment" IEEE 2017, Pg.No:93-98.
2. Anders Fongen and Geir Køieny "Trust Management in Tactical Coalition Software Defined Networks" IEEE 2018, Pg.No:354-361.
3. Bassey Isong, Tebogo Kgogo,Francis Lugayizi and Bennett Kankuzi " Trust Establishment Framework between SDN Controller

and Applications" IEEE 2017,Pg.No:101-107.

4. Weizhi Meng, Kim-Kwang Raymond Choo, Steven Furnell, Athanasios V.Vasilakos, and Christian W. Probst " Towards Bayesian-based Trust Management for Insider Attacks in Healthcare Software-Defined Networks" IEEE 2018,Pg.No:343-355.
5. Bata Krishna Tripathy, Ananta Gopal Sethy and Padmalochan Bera ohammad Ashiqur Rahman“. A Novel Secure and Efficient Policy Management Framework for Software Defined Network" IEEE 2016, Pg.No:424-430.
6. Abide Mehmood, Iynkaran Natgunanathan, Yong Xiang, Guang Hua and Song Guo, PROTECTION OF BIG DATA PRIVACY, IEEE 2014,pp (1822-1834).
7. Hadeer Mahmud, Abdelfatah Hegazy Mohamed, H. Khadafy," An approach for Big Data Security based on Hadoop Distributed File system ",IEEE 2018,pp (109-114).
8. Bing Wei, Li-Min Xiao, Member, Wei Wei, Yao Song, Bing-Yu Zhou," A New Adaptive Coding Selection Method for Distributed Storage Systems ",IEEE access,2017,pp (1-8).
9. Derek Feichtinger, Andreas J. Peters," Authorization of Data Access In Distributed Storage Systems", IEEE 2005,pp (172-178).
10. Bingheng Yan, Depew Qian, Yuanqiang Huang," Data Currency in Replicated Distributed Storage System", IEEE 2009,pp (1-7).