International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 1

Sharing the Secured Cloud Storage with Elliptic Curve Algorithm

Nuka Raju Kolli
Associate Professor, Department of CSE,
Diet, Anakapalle, Visakhapatnam

Dinesh Kumar Y
Associate Professor, Department of CSE,
Diet, Anakapalle, Visakhapatnam

ABSTRACT

Users store vast amounts of data on a big data platform. Sharing data will help enterprises reduce the cost of providing users with personalized services and provide value-added data services. However, secure data sharing is problematic. This paper proposes a framework for secure sensitive data sharing on a big data platform, including secure data delivery, storage, usage, and destruction on a semi-trusted big data sharing platform. At the same time, data owners retain complete control of their own data in a sound environment for modern Internet information security. we present an alternative approach which divides big data into sequenced parts and stores them among multiple Cloud storage service providers. Instead of protecting the big data itself, the proposed scheme protects the mapping of the various data elements to each provider using a trapdoor function. Analysis, comparison and simulation prove that the proposed scheme is efficient and secure for the big data of Cloud tenants. Secured data transmission using elliptic curve cryptography can be defined as transmission of data. This paper proposes an survey about Secured data transmission using elliptic curve cryptography. The main problem in existing system is security issues in transmitting data between source and the destination. After the survey on various literature papers, we are concluding a new way, that increases security considerations for transfer of data and to increment the efficiency using ECC(Elliptic Curve Cryptography). Efficiency and reliability will be increased for each transmission of data, While enclosing the proposed method by using the ECC algorithm which allow itself to encrypt and decrypt the data that is to be transferred and performs the active classification.

Keywords: *Cloud computing, big data, storage and sharing, security, secure sharing, elliptic curve cryptography algorithm*

1. INTRODUCTION

These data not only meet the demands of the enterprise itself, but also provide services to other businesses if the data are stored on a big data platform. Traditional cloud storage merely stores plain text or encrypted data passively. Such data can be considered as “dead”, because they are not involved in calculation. However, a big data platform allows the exchange of data (including sensitive data).It provides mass data storage and computational. In modern information technology, big data is a term applied to data sets whose size is beyond the ability of commonly used software systems to store, manage, and process within a tolerable elapsed time. Big data sizes are a constantly moving target, currently ranging from a few dozen terabytes to many peta bytes of data in a data center. Elliptic curve cryptography (ECC) is a public-key cryptography system which is based on discrete logarithms structure of elliptic curves over finite fields. ECC is known for smaller key sizes, faster encryption, better security and more efficient implementations for the same security level as compared to other public cryptography systems (like RSA). ECC can be used for encryption (e.g Elgamal), secure key exchange (ECC Diffie-Hellman) and also for authentication and verification of digital signatures.

The security of ECC is based on a trapdoor function where it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible. This is called

Elliptic Curve Discrete Logarithm Problem(ECDLP) which is considered to be computationally infeasible to solve. A data center mainly focuses on the storing and processing of big data sets, real-time data mining, and streaming media delivery etc. Data-intensive applications and research will be integral to many future scientific endeavors, but will demand specialized security mechanisms to make data centers efficient and secure. In addition, the research community now has the option of accessing storage and computing resources on demand, and the IT industry is currently building multiple big data centers for social efficient scheme for tenants to access their data on the data center storage is crucial. networks and applications. Consequently, large amounts of clients' private and secret data (including meta-data) will be stored in data centers, and will need protection during processing and transmission. Thus, data centers should be able to provide efficient security, access, and update mechanisms to not only huge files running into peta bytes, but also to small files that are only a few hundred bytes. In all the above cases, determining how to design a secure and efficient scheme for tenants to access their data on the data center storage is crucial. For some threats, especially the security threat of abusing private information and data is fatal for the tenant. Currently, the storing of tenants' data on a cloud platform is a popular practice, and this is becoming more complicated and diversified than ever. In modern advanced information society, people have a variety of personalized requirements about their data information. Undoubtedly, privacy and security of personal data information is the most important concern for tenants when they store their confidential data on cloud storages. In order to make the confidential big data of tenants secure, we propose a secure cloud big data storage scheme based on crypto graphic virtual mapping of the big data. The proposed scheme is described below. In the proposed scheme, we divide the big data or big data set into sequential data parts according certain principles, such as same data type block or IP-resembled (Internet Protocol) data packets.

2. LITERATURE REVIEW

A tutorial on state of the art, issues, and challenges Developers prefer to utilize third-party libraries when they implement some functionalities and Application Programming Interfaces (APIs) are frequently used by them. Facing an unfamiliar API, developers tend to consult tutorials as learning resources. Unfortunately, the segments explaining a specific API scatter across tutorials. Hence, it remains a challenging issue to find the relevant segments. In this study, we propose a more accurate model to find the exact tutorial fragments explaining APIs. This new model consists of a text classifier with domain specific features. More specifically, we discover two important indicators to complement traditional text based features, namely co-occurrence APIs and knowledge based API extensions. In addition, we incorporate Word2Vec, a semantic similarity metric to enhance the new model. Extensive experiments over two publicly available tutorial datasets show that our new model could find up to 90% fragments explaining APIs and improve the state-of-the-art model by up to 30% in terms of F-measure.

Accelerating data-intensive science with Gordon and dash: There is a new trend emerging across university campuses to deploy Science DMZs (demilitarized zones) to support Science drivers that involve for e.g., data-intensive applications needing access to remote instrumentation or public cloud resources. Using advanced technologies such as "multi-domain" software-defined networking, zero-copy RDMA data transfers, active measurements and federated identity/access - accelerated flows are starting to be setup from Science DMZs over wide-area overlay networks, by-passing traditional campus firewalls. In this paper, we present a "campus Science DMZ reference architecture" for adaptively managing host-to-host accelerated flows of multiple researchers over wide-area overlay networks with shared underlay infrastructure components. We discuss our novel approaches in handling challenges of policy specification, security enforcement, and performance engineering within Science DMZs to support diverse accelerated flows on a scalable/extensible basis. Lastly, we present a multi-disciplinary case study of a bioinformatics science driver application in a double-ended campus Science DMZ testbed. Our case study illustrates how our reference architecture can enable new "High -Throughput Computing services" that improve remote accessibility and peer-collaboration of data-intensive science users, and simplify related operations/management for campus network service providers.

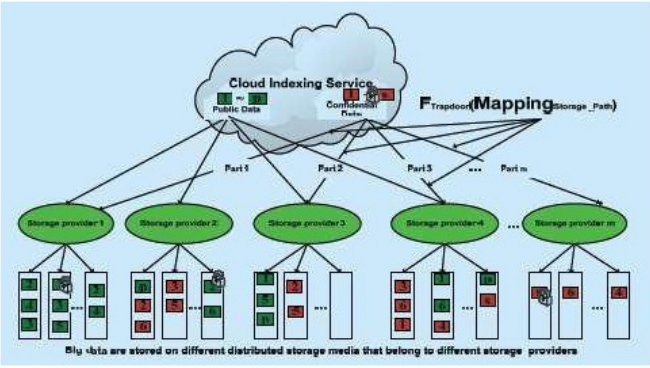
Ensured at a security in cloud storage
The cost of maintain a data center is increasing rapidly, especially for the medium data center. An economic choice is to use cloud computing and cloud storage instead of manage data center by itself. Small companies buy compute and storage service just like water and electronic. The difficulty is how to ensure their data safe in cloud storage. Cloud storage provider

claims that they can protect the data, but no one believes them. In this paper, we present a framework to ensure data security in cloud storage system. In the framework, we use SLA as the common standard between user and provider. And we discuss several technologies to make the data stored in cloud safe. These technologies can be divided into three parts: storage protect, transfer protect and authorize.

Secure and privacy preserving key word searching for clouds to rage services

Encrypted data search allows cloud to offer fundamental information retrieval service to its users in a privacy - preserving way. In most existing schemes, search result is returned by a semi-trusted server and usually considered authentic. However, in practice, the server may malfunction or even be malicious itself. Therefore, users need a result verification mechanism to detect the potential misbehavior in this computation outsourcing model and rebuild their confidence in the whole search process. On the other hand, cloud typically hosts large outsourced data of users in its storage. The verification cost should be efficient enough for practical use, i.e., it only depends on the corresponding search operation, regardless of the file collection size. In this paper, we are among the first to investigate the efficient search result verification problem and propose an encrypted data search scheme that enables users to conduct secure conjunctive keyword search, update the outsourced file collection and verify the authenticity of the search result efficiently. The proposed verification mechanism is efficient and flexible, which can be either delegated to a public trusted authority (TA) or be executed privately by data users. We formally prove the universally compassable (UC) security of our scheme. Experimental result shows its practical efficiency even with a large dataset.

3. SYSTEM ARCHITECTURE



4. RELATED WORK

ECC was developed by Certicom, a mobile e-business ECC was developed by Certicom, a mobile e-business security provider, and was recently licensed by Hifn, a manufacturer of integrate circuitry (IC) and network security products. RSA has been developing its own version of ECC. Many manufacturers, including 3COM, Cylink, Motorola, Pitney Bowes, Siemens, TRW, and VeriFone have included support for ECC in their products. I assume that those who are going through this article will have a basic understanding of cryptography (terms like encryption and decryption). The equation of an elliptic curve is given as, Few terms that will be used,

E -> Elliptic Curve
P -> Point on the curve
n -> Maximum limit (This should be a prime number)
The figure show are simple elliptic curve.
Key Generation
Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.
Now, we have to select a number 'd' within the range of 'n'.
Using the following equation we can generate the public key
Q = d * P
d = The random number that we have selected within the range of (1 to n-1). P is the point on the curve.
'Q' is the public key and 'd' is the private key.

Encryption
Let 'm' be the message that we are sending. We have to represent this message on the curve. This have in-depth implementation details. All the advance research on ECC is done by a company called certicom. Consider 'm' has the point 'M' on the curve 'E'.
Randomly select 'k' from [1 – (n-1)].
Two cipher texts will be generated let it be C1 and C2.
C1 = k*P
C2 = M + k*Q
C1 and C2 will be send.
Decryption
We have to get back the message 'm' that was send to us,
M = C2 – d * C1
M is the original message that we have send.
Proof
How does we get back the message,
M = C2 – d * C1
'M' can be represented as 'C2 – d * C1'

C2 – d * C1 = (M + k * Q) – d * (k * P) (C2 = M + k * Q and C1 = k * P)
= M + k * d * P – d * k *P(canceling out k * d *P) = M (Original Message)

The procedure of establishing communication key between tenant

A and other cloud user, for example B Tenant A computes parameter YA: Choose XA <q
Compute YA = _XA mod q .
User B computes parameter YB:
Choose XB <q
Compute YB = _XB mod q .
Tenant A encrypts YA ,IDA and IDB using IBE algorithm and then send to B:
Encrypt (YA ,IDA and IDB)→B
User B encrypts YB ,IDB and IDA using IBE algorithm and then send to B:
Encrypt (YB ,IDB and IDA)→A
Tenant A decrypts message and computes K1 = (YB)XA mod q
User B decrypts message and computes K2 = (YA)XB mod q

5. OVERVIEW

We In order to make the confidential big data of tenants secure, we propose a secure cloud big data storage scheme based on cryptographic virtual mapping of the big data, and the concept is shown in. The proposed scheme is described below. In the proposed scheme, we divide the big data or big data set into sequential data parts according certain principles, such as same data type block or IP-resembled Internet Protocol data packets.

We first introduce the trapdoor function before describing the proposed scheme. A trapdoor function is a function that is easy to compute in one direction, yet believed to be difficult to compute in the opposite direction finding its inverse without special information privacy called the trapdoor. Trapdoor functions are widely used in cryptography. In mathematical terms, if f is a trapdoor function there some secret information y, such that given and y it is easy to compute.

Cloud computing

In cloud computing, big data storage services represent a basic function for their tenants. In the proposed scheme, firstly, tenants' big data will be separated into many sequenced parts before storage, and then will be stored on different storage media owned by different cloud storage providers. When tenants access their data, the data parts in different data centers will be collected together and then be restored into original form based on the sequenced number of each data part. Generally, the tenants' big data which is stored in cloud storage can be classified into public data and confidential data. There are no extra security requirements for public data, and each tenant can access these data freely, on the other hand, confidential data should always be kept secret and inaccessible to irrelevant persons or organizations.

1. Big Data

In order to make the confidential big data of tenants secure, we propose a secure cloud big data storage scheme based on cryptographic virtual mapping of the big data, and the concept is shown in Fig1. The proposed scheme is described below. In the proposed scheme, we divide the big data or big data set into sequential data parts according certain principles, such as same data type block or IP-resembled (Internet Protocol) data packets. Evidently, n is always far greater than m, these m storage providers belong to different organizations, such as Google, Amazon and Yahoo. Each data part stored on certain cloud storage providers will be allocated to some physical storage media that belongs to the storage provider, so, when big data of a tenant is stored, it will form a unique storage path for the big data given.

2. Storage and sharing

In cloud computing environment, the tenants such as some companies or enterprises, when they transfer and store their big data on cloud storage center directly, it maybe arise some serious problems such as system crash or failure, however, in the proposed scheme, the big data of tenants will be divided into some smaller data blocks, these smaller data blocks will be stored in cloud storage media one by one, because these data blocks are smaller than the primitive big data ,they are very efficient for remote-distance data transmission and storage. Under the same network conditions, the transmission failure probability of the proposed scheme is lower than when the big data store and transmit directly.

3. Security

Now we compute the vulnerability of security of proposed scheme. Let x be an adversary who want to acquire the storage path of the big data illegally, according to the proposed scheme, the adversary can observe the whole big data only when he/she gets the storage paths of all data blocks. So, we can judge the security of storing part of big data on different cloud storages only by computing the probability that x

knows the storage paths all of data blocks. Some tenants are still reluctant to deploy their big data in the cloud. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. In work [16], a survey of the different security risks that pose a threat to the cloud is presented and the work focused on the different security issues and concerns that have emanated due to the nature of the service delivery models of a cloud computing system.

5. CONCLUSION

We presented a computation model for big data analytics in the cloud and surveyed several cryptographic techniques that can be used to secure these analytics in a variety of settings. While these techniques give a good starting point for secure cloud computing, further research is needed to turn them into practical solutions that can achieve secure cloud computing in the real world. Due to its enormous size, owners of big data need to consider the cost (both in terms of time and money) of encryption. Our presented solution avoids this by splitting the data among several cloud providers, and protecting the virtual mapping (needed to reconstruct reassemble the big data) using a trapdoor function. The proposed system a content sharing scheme that is safe in the cloud computing environment, based on a conditional proxy re-encryption scheme. This system can significantly reduce burden of a client due to two characteristics. First is re-encryption process is delegated to a cloud server. A client is only involved in process of encryption and decryption of data and creation of re-encryption keys. Second, the number of re-encryption keys to be required for sharing is minimized. Secure data access when sharing in a group, Implementation and maintenance, Reliability and scalability; Guaranteed levels of services, Total cost of ownership are the main feature of this system. We analyze the efficiency and security of the proposed scheme through some theoretical proof, at the same time; we compare the proposed scheme with other related schemes and technology by simulation under two different scenarios; the simulation results coincide in the analysis very well. All the results show that the proposed scheme is effective and feasible to protect the big data for cloud tenants.

6. FUTURE WORK

In future work, we plan to analyze the overheads of our detection techniques such as the various distance-based methods in comparison with contemporary approaches. At present, this was developed to provide the requirements needed to provide security to data, we study and analyze big cloud storage in cloud computing. Customers put their data into single cloud which is liable to vendor lock in risk. In addition, the loss of service availability and data integrity are the major problems for the customer. This paper presented some recent advances and schemes to provide multi - cloud security and their comparison based on security issues. Distributed based approaches seem to be simple but provide less security than others. Hybrid based approaches were more realistically meeting organizational needs however they comes with private cloud costs.

References

1) Shmueli, Erez, et al. “Database encryption: an overview of contemporary challenges and design considerations.” ACM SIGMOD Record 38.3 (2010): 29-34.
2) Sabahi F. Virtualization-level security in cloud computing[C]//Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on. IEEE, 2011: 250-254.
3) Popa R A, Stark E, Helfer J, et al. Building web applications on top of encrypted data using Mylar[C]//USENIX Symposium of Networked Systems Design and Implementation. 2014.
4) Cao N, Wang C, Li M, et al. Privacy -preserving multi-keyword ranked search over encrypted cloud data[J]. Parallel and Distributed Systems, IEEE Transactions on, 2014, 25(1): 222-233.
5) Soundararajan O M, Jenifer Y, Dhivya S, et al. Data Security and Privacy in Cloud Using RC6 and SHA Algorithms[J]. Networking and Communication Engineering, 2014, 6(5): 202-205.
6) D. Kusnetzky. What is “Big Data?” [Online].Available: http://blogs.zdnet.com/virtualization/? p=1708.
7) K. Kant, “Data center evolution: A tutorial on state of the art, issues, and challenges,” Computer Networks, vol.
8) 53, no. 17, pp. 2939– 2965, 2009, virtualized Data Centers[Online]. Available: http://www.sciencedirect.com/science/ article/pii/S1389128609003090