International Journal of Advanced Science and Technology
Vol. 29, No. 8, (2020), pp. 5497 - 5509

`

Data Theft Protection In Cloud Storage Using Three Layer Architecture Using Decoy Documents

D.Sai Maneesha,

M.Tech Student, Dept of Computer Science and Engineering, JNTUA College of Engineering, Pulivendula-516390, Andhra Pradesh, India

Dr.S.Jessica Saritha,

Assistant Professor, Dept of Computer Science And Engineering, JNTUA College of Engineering, Pulivendula-516390, Andhra Pradesh, India

Abstract

Recent years witness the development of cloud computing technology. With the explosive growth of unstructured data, cloud storage technology gets more attention and better development. Cloud computing promises to significantly change the way to use computers and access and store our personal and business information. With these new computing and communications paradigms arise new data security challenges. Traditional privacy protection schemes are usually based on encryption technology, but these kinds of methods cannot effectively resist attack from the inside of cloud server. Proposed system provides small part of data in local machine and fog server in order to protect the privacy. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively. But here data is divided into blocks and stored in multiple systems, access data blocks and combining is tremendous work. In order to solve this problem, Proposing a three-layer storage framework based on fog computing. The proposed framework can both take full advantage of cloud storage and protect the privacy of data. Propose a different approach for securing data in the cloud using offensive decoy technology. Monitors data access in the cloud and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions, to protect data, launching a disinformation attack by returning large amounts of decoy information to the attacker. Proposing Enhanced A Three-Layer Privacy Preserving Cloud Storage using multi cloud servers and multi fog servers, an efficient, distributed and scalable data processing system through Multi Cloud Server Security.

Keywords: *Stress detection, micro-blog, social media, social interaction, Word Semantic*

I. INTRODUCTION

With the rapid development of network bandwidth, the Volume of user's data is rising geometrically. User's requirement cannot be satisfied by the capacity of local machine any more. Therefore, people try to find new methods to store their data. For more powerful storage capacity, a growing number of users select cloud storage. Cloud storage is a cloud computing system which provides data storage and management service. With a cluster of applications, network technology and distributed file system technology, cloud storage makes a large number of different storage devices work together coordinately. Nowadays there are lot of companies providing a variety of cloud storage services, such as Dropbox, Google Drive, iCloud, Baidu Cloud, etc. These companies provide large capacity of storage and various services related to other popular applications. However, cloud storage service still exists a lot of security problems. The privacy problem is particularly significant among those security issues. In history, there were some famous cloud storage privacy leakage events. User

ISSN: 2005-4238 IJAST

`

uploads data to the cloud server directly. Subsequently, the Cloud Server Provider (CSP) will take place of user to manage the data. In consequence, user do not actually control the physical storage of their data, which results in the separation of ownership and management of data.

Now the cloud server is divided into three different layers for ensuring the security purpose and to avoid the location awareness. The three different privacy preserving layers are Cloud server, Fog server and Local server. A complete data is now partitioned and stored into three different layers. The ratio of the partition of data is major part of the data is stored in the cloud server, neither high nor low range of data is stored in the fog server and finally lower amount of local server. When the data required it can be combined into a single data using pattern matching method

Fog computing is familiar with cloud computing. It consists of low latency and increasing the geographical range of distribution. Fog computing can perform the data processing and limited storage capabilities. Fog computing consist of three-level architecture, the uppermost is a cloud computing layer, it can be used as storing data and computing data. The middle layer is the fog computing layer. Fog computing layer can perform critical data transmission to cloud server. And finally the third layer is wireless sensor network layer. This layer's main job is to collect data and upload it to the fog server. In addition, the rate of transfer between the fog computing layer and other layers is faster than the rate between the cloud layer and the lower layer.

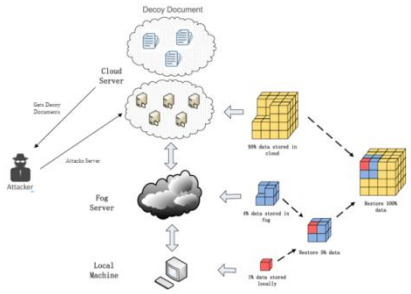

Fig 1: Three Cloud Architecture with Cloud

Confidentiality is a basic for strong confidentiality security in all online computing sides, but confidentiality alone is not satisfies. Companies and customers are ready to use online computing only if they have the belief that their data will stay confidential and safe. Thus to produce a trusted surrounding for customers, we need to create a software, assist and works with confidentiality in mind. The location of physical assets and accessories being allowed in general doesn't known to the particular user. It also affords services for user to form up, use and maintain their data in the applications on the cloud, which maintains and manages the virtualization of assets by itself. Cloud memory is a method of networked online memory in which the data is stored in virtual group of stash that is generally being introduced by the third person. Cloud memory makes data stored remotely to be limitedly cached on mobiles, PC or other Internet connected devices. Confidentiality and cost are the barriers in this field, depending on the dealers. Although the first achievement and identification of the cloud model and the broad availability of producers and tools, a number of trials and prospects are intuitive to this new design of computing.

II. LITERATURE SURVEY

A. A Secure Data Privacy Preservation For On-Demand Cloud Service

This paper is focus on privacy and security of data stored in the cloud. They albeit computing is introduced to provide to increasing its efficiency, optimization and effectiveness of the cloud

ISSN: 2005-4238 IJAST

`

environment. Thus author introduce Privacy Preserving Model to Prevent Digital Data Loss in the Cloud. This proposal helps the Cloud Requester/Users to trust their proprietary information and data stored in the cloud.

B.Privacy-Preserving Security Solution For Cloud Services

This paper is based on the privacy-preserving security solution for cloud. It based on the signature scheme for the nonbilinear group providing the unidentified access to the cloud server and shared storage server. It makes Unidentified Authentication for the registered user. The user personal information can be displayed without revealing the user detail. However any illegal activity is found, the user rights in the cloud server can be revoked. Author proposed work helps to Anonymous access, unlinkability and data transmission confidentiality.

C. An Efficient Public Auditing Protocol With Novel Dynamic Structure For Cloud Data

This paper is based on the efficient method of making the structure of the data. Author proposed public auditing scheme in which dynamic operation can be performed. Hashing can be performed in this method. Using Merkle Hash Tree the dynamic data operation can be performed. Ring signature stores the information of the user.

D. On A Relation Between Verifiable Secret Sharing Schemes And A Class Of Error-Correcting Codes

This paper explains about the Verifiable Secret Sharing Schemes. Using the metric author forms a set of codes known as set of error correcting codes. Then they consider the burst error interleaving codes introduces the efficient burst error correcting scheme. By this methods error correcting and secrete sharing of files can be performed.

E.Security And Privacy Of Ensitive Data In Cloud Computing: A Survey Of Recent Developments

This paper represents the Available technologies and a broad collection of Created and implementation of projects on cloud confidentiality and security. This paper are arranged based on the available works based on the cloud architecture ,Management of resources and cloud work management layers, along with the recollection of the developments that available in privacy preserving confidential data in cloud computing.

F. A Survey On Cloud Security Issues And Techniques

\

This paper explains about some of the security issues in cloud in various aspects like Insider attacks, Outsider attacks, Loss of control, data loss, multi tenancy, Network security, elasticity, and availability. It also consists of available security schemes and method for a securing cloud. This paper will deliver the idea about different security issues and tools to the researchers and professionals.

G. Security And Privacy Preservation Scheme Of Face Identification And Resolution Framework Using Fog Computing In Internet Of Things

ISSN: 2005-4238 IJAST

`

In this paper, used the face recognition in the three layer privacy in cloud computing using fog computing in internet of things. Using the face recognition the data present in the three layers are kept encrypted and secured. Only the authenticated person can open the data in the server. Face recognition is implemented in each layer. It helps to ensure security and privacy in the cloud computing.

H. A Secure Data Privacy Preservation For On-Demand Cloud Service

This paper describes about the portability issues in the cloud environment, the users can have their account information and details including respective cloud providers. Noisy disturbance in the valued data information of cloud, initiate a scheme to abort privacy leakage. Petri net models introduced as a modern tool for to do our own system that tells about concurrency and synchronization. The process is to develop the distributed theories as well as techniques. It is used to analyze the quantitative and logical processes.

Papers Study

[1] H. Li, W. Sun, F. Li, and B. Wang, "Secure and privacy-preserving data storage service in public cloud," J. Comput. Res. Develop., vol. 51, no. 7, pp. 1397–1409, 2014

Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.
[6] L. Xiao, Q. Li, and J. Liu, "Survey on secure cloud storage," J. Data Acquis. Process., vol. 31, no. 3, pp. 464–472, 2016.

Data Security and consumer data privacy are the key challenges in cloud computing era. The appropriateness and privacy of data stored in cloud may be compromised because of limited security for data owners. This paper presents an extensive survey on privacy preservation, data and storage security challenging issues in cloud computing. The Security of cloud data is further analyzed in terms of data integrity, access control and attribute based encryption. The survey analyzes each category of work in detail. A comparison table is also presented along with the strength and weakness of each approach.

ISSN: 2005-4238 IJAST

`

[13] J. Hou, C. Piao, and T. Fan, “Privacy preservation cloud storage architecture research,” J. Hebei Acad. Sci., vol. 30, no. 2, pp. 45–48, 2013.

We propose a novel privacy-preserving security solution for cloud services. Our solution is based on an efficient non-bilinear group signature scheme providing the anonymous access to cloud services and shared storage servers. The novel solution offers anonymous authenticationfor registered users. Thus, users' personal attributes (age, valid registration, successful payment) can be proven without revealing users' identity, and users can use cloud services without any threat of profiling their behavior. However, if a user breaks provider's rules, his access right is revoked. Our solution provides anonymous access, unlinkability and the confidentiality of transmitted data. We implement our solution as a proof of concept applicationand present the experimental results. Further, we analyzecurrent privacy preserving solutions for cloud services and group signature schemes as basic parts of privacy enhancing solutions in cloud services. We compare the performance of our solution with the related solutionsand schemes

[16] G. Feng, “A data privacy protection scheme of cloud storage,” vol. 14, no. 12, pp. 174–176, 2015.

At present, there are a lot of mature encryption mechanisms and access control models for the protection of the data content in cloud environment. However, the research on the privacy protection of data attributes in cloud is still in the initial stage, which can be classified as two types: one is the privacy protection of data attributes during data transmission, including routing information, generation time, size and frequency, etc., the other is the privacy protection of data attributes as data storage, including relationships between attributes and distribution of attribute values. The current encryption mechanisms and access control models cannot solve the problem perfectly. In this paper, we try to analyze current protection schemes and algorithms for the protection of data attributes, and point out the future research directions.

[19] Z. Xia, X. Wang, X. Sun, and Q. Wang, “A secure and dynamic multikeyword ranked search scheme over encrypted cloud data,” IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 340–352, Feb. 2016.

Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. However, sensitive data should be encrypted before outsourcing for privacy requirements, which obsoletes data utilization like keyword-based document retrieval. In this paper, we present a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents. Specifically, the vector space model and the widely-used TF x IDF model are combined in the index construction and query generation. We construct a special tree-based index structure and propose a “Greedy Depth-first Search” algorithm to provide efficient multi-keyword ranked search. The secure kNN algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors. In order to resist statistical attacks, phantom terms are added to the index vector for blinding search results. Due to the use of our special tree-based index structure, the proposed scheme can achieve sub-linear search time and deal with the deletion and insertion of documents flexibly. Extensive experiments are conducted to demonstrate the efficiency of the proposed scheme.

ISSN: 2005-4238 IJAST

`

III. APPLICATIONS

Fog computing is an extended computing model based on cloud computing which is composed of a lot of fog nodes. These nodes have a certain storage capacity and processing capability. In our scheme, we split user's data into three parts and separately save them in the cloud server, the fog server and the user's local machine.

The security degree is an important metric to measure the quality of cloud storage system. Furthermore, data security is the most important part in cloud storage security and it includes three aspects: data privacy, data integrity and data availability. Ensuring data privacy and integrity has always been the focus of relevant researches. On another hand, data privacy is also the most concerned part of the users. From a business perspective, company with high security degree will attract more users. Therefore improving security is an crucial goal no matter in academia or business. In this section, we will detailedly elaborate how the Transport Layer Security framework protects the data privacy, the implementation details of work flow and the theoretical safety and efficiency analysis of the storage scheme. 4.1. Fog Computing Our scheme is based on fog computing model, which is an extension of cloud computing. Fog computing was firstly proposed by Ciscos Bonomi in 2011.In Bonomi's view, fog computing is similar to the cloud computing, the name of fog computing is very vivid. Compared to highly concentrated cloud computing, fog computing is closer to edge network and has many advantages as follows: broader geographical distributions, higher real-time and lowlatency. In considering of these characters, fog computing is more suitable to the applications which are sensitive to delay. On another hand, compared to sensor nodes, fog computing nodes have a certain storage capacity and data processing capability, which can do some simple data processing, especially those applications based on geographical location. Thus we can deploy CI on the fog server to do some calculating works. Fog computing is usually a three-level architecture, the upmost is cloud computing layer which has powerful storage capacity and compute capability. The next level is fog computing layer. The fog computing layer serves as the middle layer of the fog computing model and plays a crucial role in transmission between cloud computing layer and sensor network layer. The fog nodes in fog computing layer has a certain storage capacity and compute capability. The bottom is wireless sensor network layer. The main work of this layer is collecting data and uploading it to the fog server. Besides, the transfer rate between fog computing layer and other layers is faster than the rate directly between cloud layer and the bottom layer. The introduction of fog computing can relief the cloud computing layer, improving the work efficiency. In our scheme, we take advantage of the fog computing model, adopt three-layer structure. Furthermore, we replace the WSNs layer by user's local machine The framework can take full of cloud storage and protect the privacy of data. Here the cloud computing has attracted great attention from different sector of society. The three layer cloud storage stores in to the three different parts of data parts .If the one data part missing we lost the data information. In this proposed framework using the bucket concept based algorithms. In our system we using a bucket concept so reduce the data wastages and reduce the process timings. We are using a BCH (Bose–Chaudhuri– Hocquenghem) code algorithm. It's High flexible. BCH code are used in many communications application and low amount of redundancy. The Bucket Access manage resource represents the Access Control Lists (ACLs) for buckets inside Google Cloud Storage. ACLs let you specify who has access to your data and to what extent. The three layer cloud storage stores into the three different parts of data parts .If the one data part missing we lost the data information. In this propos
ed framework using the bucket concept based algorithms

IV. PROPOSED SYSTEM

Objectives Cloud computing promises to significantly change the way we use computers and access and store our personal and business information. With these new computing and communications

ISSN: 2005-4238 IJAST

`

technologies, arise new data security challenges. Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider. Propose a completely different approach to securing the cloud using decoy information technology connected to Fog computing. Proposing Enhanced A Three-Layer Privacy Preserving Cloud Storage using multi cloud servers and multi fog servers, an efficient, distributed and scalable data processing system through Multi Cloud Server Security.

Existing System

Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider. Much research in Cloud computing security has focused on ways of preventing unauthorized and illegitimate access to data by developing sophisticated access control and encryption mechanisms. However these mechanisms have not been able to prevent data compromise. Many Concepts are introduced in Cloud computing security has focused on ways of preventing unauthorized and illegitimate access to data by developing sophisticated access control and encryption mechanisms. Traditional privacy protection schemes are usually based on encryption technology, but these kinds of methods cannot effectively resist attack from the inside of cloud server. In Traditional Methods all user related data is stored in a single cloud.

Existing system is a three-layer storage framework based on fog computing. As an extension to Traditional Method project has been extended with Enhanced security degree with combining local machine, fog server and cloud server.

Disadvantages of Existing System

- Many Concepts are introduced in Cloud computing security has focused on ways of preventing unauthorized and illegitimate access to data by developing sophisticated access control and encryption mechanisms.
- Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider.
- Much research in Cloud computing security has focused on ways of preventing unauthorized and illegitimate access to data by developing sophisticated access control and encryption mechanisms.
- However these mechanisms have not been able to prevent data compromise and data theft is usually occurring.

Proposed System

Propose a completely different approach to securing the cloud using decoy information technology to Fog computing. Providing an enhanced layer for Cloud Server to divided the data and store in multiple clouds. Technology to launch disinformation attacks against insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data. The decoys, then, serve two purposes: (1) validating whether data access is authorized When abnormal information access is detected, and (2) confusing the attacker with bogus information. The combination of these two security features will provide a high levels of security for the Cloud. No current Cloud security mechanism is available that provides this level of security. We design a cloud server with Application, Infrastructure and cloud plat form services. Cloud computing is a model for enabling convenient, ondemand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction. Future work could lead towards the development of a knowledge-based supplementary and aid system, which can provide

ISSN: 2005-4238 IJAST

`

decision support services for developers in designing a secure and performance efficient Fog infrastructure. Such a decision support system would require a large systematic knowledge acquisition of best practices, known security threats and their solutions, which can be formalized as either statistical-based system or rules, policies and facts. The system would also require an inference engine that can provide and explain suitable solution or advice, considering the given application scenario (current context) and available knowledge. A Fog platform is connected with both end-users and Cloud platform along with processing, storing and transmitting large volumes of data by consuming limited amount of resources. It is therefore of key importance that security measures are correctly adhered to overcome the potential limitations identified in this paper. Hence, the use of a decision support tool that is capable of advising security measures to developers can prevent the occurrence of vulnerabilities pro-actively and save the Fog platform from potential damage.

Advantages of Proposed System

- Cloud computing promises to significantly change the way we use computers and access and store our personal and business information.
- Enhances with Multi Clouds in Cloud Layer.
- With these new computing and communications technologies, arise new data security challenges.
- Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider.
- Propose a different approach for securing data in the cloud using offensive decoy technology.
- Propose a completely different approach to securing the cloud using decoy information technology, that we have come to call Fog computing.

Algorithm

Begin
1: for each session separated for every user do
2: Get different HTTP requests and activities of user (DB queries q, Storage S, Services r) in this session
3: for each different r do
4: Add user Request to File with sessions(UserID,Db Query, Storage, Services)
5: if r is not in set USER login then
6: exit else
7: Encrypt File (Db Query, Storage, Services)
encipher(String s, String key)
for I = 0 to s.length() do
char encyphered = s.charAt(i) + getShift(key, i) > 90 ? (char)((s.charAt(i) + getShift(key, i)) - 26) : (char)(s.charAt(i) + getShift(key, i))
log.append(encyphered);
next
8: Append session ID with Activity
9: decrypt (String s, String key)
For I = 1 to s.length() do
char decyphered = s.charAt(i) - getShift(key, i) < 65 ? (char)((s.charAt(i) - getShift(key, i)) + 26) :

ISSN: 2005-4238 IJAST

`

```
(char)(s.charAt(i) - getShift(key, i));
log.append(decyphered);
10: End
```

Application Modules

Cloud Computing

Cloud computing is a model for enabling convenient, ondemand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction. It divide into three type

1.Application as a service.
2.Infrastructure as a service.
3.Platform as a service.

Cloud computing exhibits the following key characteristics:

1. Agility improves with users' ability to re-provision technological infrastructure resources.
2. Cost is claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure. This is purported to lower barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation. The e-FISCAL project's state of the art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.
3. Virtualization technology allows servers and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another.
4. Multi tenancy enables sharing of resources and costs across a large pool of users thus allowing for:
5. Centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)
6. Utilization and efficiency improvements for systems that are often only 10–20% utilized.
7. Reliability is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
8. Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
9. Security could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.
10. Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

User Behavior Profiling

We monitor data access in the cloud and detect abnormal data access patterns User profiling is a well known Technique that can be applied here to model how, when, and how much a user accesses their

ISSN: 2005-4238 IJAST

`

information in the Cloud. Such 'normal user' behavior can be continuously checked to determine whether abnormal access to a user's information is occurring. This method of behavior-based security is commonly used in fraud detection applications. Such profiles would naturally include volumetric information, how many documents are typically read and how often. We monitor for abnormal search behaviors that exhibit deviations from the user baseline the correlation of search behavior anomaly detection with trap-based decoy files should provide stronger evidence of malfeasance, and therefore improve a detector's accuracy.

Decoy documents

We propose a different approach for securing data in thecloud using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data the decoys, then, serve two purposes:
(1) Validating whether data access is authorized when abnormal information access is detected, and
(2) Confusing the attacker with bogus information..

V.RESULTS

When we select one of the uploaded files from the list as an attacker, it will download but instead of original data duplicate data will be present there. These duplicate files called here as Decoy documents and the technology called as Decoy information technology. With the help of these decoy documents the attacker may get confused and may receive wrong information so that we can protect the data from the attackers even though they enter into the website.

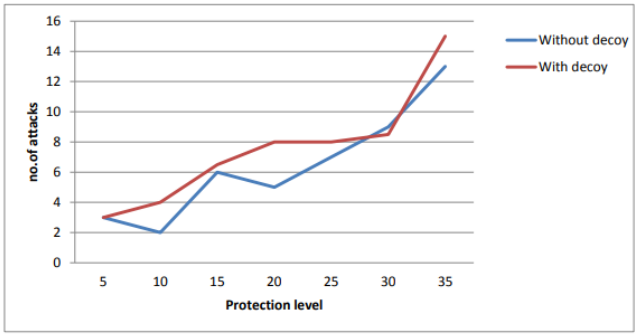

Fig. Attacking nature with respective to decoys

ISSN: 2005-4238 IJAST

`

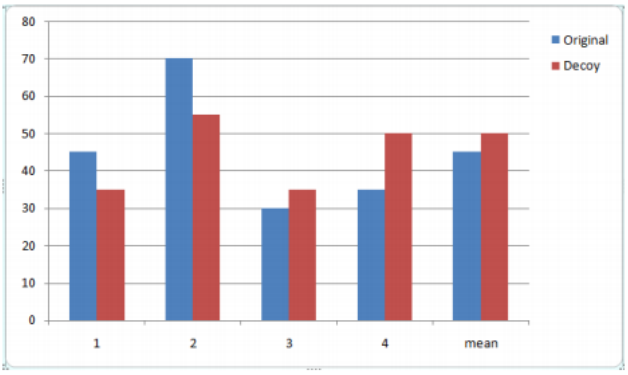

Fig.. Mean of protection towards the data

VI.CONCLUSION

The development of cloud computing brings us a lot of benefits. Cloud storage is a convenient technology which helps users to expand their storage capacity. However, cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in the separation of ownership and management of data. In order to resolve the matter of privacy protection in cloud storage, we have a tendency to propose a three layer privacy protective secure cloud storage methodology framework supported fog computing model and style. By allocating the magnitude relation of knowledge blocks keep in several servers fairly, we will make sure the privacy of knowledge in every server. On another hand, cracking the encryption matrix is not possible in theory. Besides, using hash transformation will shield the fractional info. Through the experiment take a look at, this theme will efficiently complete encryption and coding while not influence of the cloud storage efficiency. Cloud Computing makes the computer world has a wider range of uses and enhances user - friendliness by providing access through any type of internet connection. Even with this increased ease of use also some drawbacks. Confidentiality is to be considered very important and is a key issue for cloud memory. A variety of techniques that can be used in order to ensure confidentiality have been mitigated. This paper has discovered some confidentiality ways for avoiding the problems in confidentiality on unsecured data stores in cloud. There are still some approaches that are not addressed with in this paper. This paper makes difference in the methodologies in the literature is based on encryption methods, based on access control Mechanisms, keyword search schemes, query integrity and Adaptability schemes. The work is making efficient confidentiality-preserving memory

REFERENCES

[1] J. Shen, D. Liu, J. Shen, Q. Liu, X. Sun, A secure cloudassisted urban data sharing framework for ubiquitouscities,Pervasive and Mobile Computing (2017), http://dx.doi.org/10.1016/j.pmcj.2017.3.013

[2] Fu, J., Liu, Y., Chao, H.-C., Bhargava, B., & Zhang, Z. (2018). Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing.IEEE Transactions on Industrial Informatics, 1–1.doi:10.1109/tii.2018.2793350

[3] P. Mell and T. Grance, “The NIST definition of cloud computing,” Nat.Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.

ISSN: 2005-4238 IJAST

`

[4] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A survey ofmobile cloud computing: Architecture, applications, and approaches,” Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587–1611, 2013.

[5] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, “Joint virtual machine and bandwidth allocation in

software defined network (sdn) and cloud computing environments,” in Proc. IEEE Int. Conf. Commun., 2014,pp. 2969–2974.

[6] H. Li, W. Sun, F. Li, and B. Wang, “Secure and privacypreserving data storage service in public cloud,” J.

Comput. Res. Develop., vol. 51, no. 7,pp. 1397–1409, 2014.

[7] Y. Li, T.Wang, G.Wang, J. Liang, and H. Chen, “Efficient data collection in sensor-cloud system with multiple mobile sinks,” in Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf., 2016,pp. 130–143.

[8] L. Xiao, Q. Li, and J. Liu, “Survey on secure cloud storage,” J. Data Acquis. Process., vol. 31, no. 3, pp. 464–472, 2016.

[9] R. J. McEliece and D. V. Sarwate, “On sharing secrets and reed-solomon codes,” Commun. ACM, vol. 24, no. 9, pp. 583–584, 1981.

[10] J. S. Plank, “T1: Erasure codes for storage applications,” in Proc. 4th USENIX Conf. File Storage Technol., 2005, pp. 1–74.

[11] R. Kulkarni, A. Forster, and G. Venayagamoorthy, “Computational intelligence in wireless sensor networks: A survey,” IEEE Commun. Surv. Tuts.,vol. 13, no. 1, pp. 68–96, First Quarter 2011.

[12] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, “A privacypreserving and copy-deterrence content-based image retrieval scheme in cloud computing,” IEEE Trans. Inf. Forensics Security, vol. 11, no. 11,pp.2594–2608, Nov. 2016.

[13] J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, “A secure cloudassisted urban data sharing framework for ubiquitouscities,” Pervasive Mobile Comput., vol. 41, pp. 219–230,

2017.

[14] Z. Fu, F. Huang, K. Ren, J.Weng, and C.Wang, “Privacypreserving smart semantic search based on conceptual graphs over encrypted outsourced data,” IEEE Trans. Inf. Forensics Security, vol. 12, no. 8, pp. 1874–1884,Aug. 2017.

[15] J. Hou, C. Piao, and T. Fan, “Privacy preservation cloud storage architecture research,” J. Hebei Acad. Sci., vol. 30, no. 2, pp. 45–48, 2013.

[16] Q. Hou, Y. Wu, W. Zheng, and G. Yang, “A method on protection of user data privacy in cloud

ISSN: 2005-4238 IJAST

`

storage

platform," J. Comput. Res. Develop., vol. 48, no. 7, pp. 1146–1154, 2011.

[17] P. Barham et al., "Xen and the art of virtualization," ACMmSIGOPS Oper.Syst. Rev., vol. 37, no. 5, pp. 164–177, 2003.

[18] G. Feng, "A data privacy protection scheme of cloud storage," vol. 14, no. 12, pp. 174–176, 2015.Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multikeyword fuzzy search over encrypted outsourced

data with accuracy improvement," IEEE Trans. Inf. Forensics Security, vol. 11, no. 12, pp. 2706–2716, Dec.

2016.

ISSN: 2005-4238 IJAST