SECURE INFORMATION HIDING APPROACH IN CLOUD USING EDGE DETECTION

Er. Mudasir Ahmed Muttoo, Assistant Professor*, Department of Computer Science and engineering,* SSM College of Engineering and Technology, Kashmir

Mrs.Yasmeen, H.O.D Assistant Professor, Department of Computer Science and engineering, SSM College of Engineering and Technology, Kashmir

Abstract: *The continuous development of cloud computing is giving way to more cloud services, due to which security of cloud services, especially data privacy protection, becomes more critical. This research work explores the basic features of data mining techniques in cloud computing and securing the data. The status of the development of cloud computing security, the data privacy analysis, security auditing, data monitoring and other challenges that the cloud computing security faces have been explored. The recent researches on data protection regarding security and privacy issues in cloud computing have partially addressed some issues. The implementation of data mining techniques through cloud computing encourages the users to extract meaningful hidden predictive information from virtually integrated data warehouse that reduces the costs of storage and infrastructure.*

Keywords: *Cloud Computing, data security, Knowledge Discovery*

I. INTRODUCTION

In this era of Internet, e-Commerce and social activities information and data are growing at a phenomenal rate. With the rapid growth of a variety of Internet services and applications, there are usually huge amounts of data; the need for quickly and efficiently manipulating the datasets in a scalable and reliable way is exceptionally high. Data mining applications and techniques are very much useful in the cloud computing model. Cloud computing denotes the new trend and practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Data mining in cloud computing is the process of extracting structured information from unstructured or semi-structured web data sources. The data mining in Cloud Computing allows organizations to centralize the management of software and data storage, with assurance of efficient, reliable and secure services for their users." The

implementation of data mining techniques through Cloud computing will allow the users to retrieve meaningful information from virtually integrated data warehouse that reduces the costs of infrastructure and storage [1]. Secure data transformation on internet has been a dream since the emergence of internet. Steganography [2] is one of the solutions to securely transmit data by hiding data in data. Data used to hide data in Steganography can be text or image.

II. DATA MINING

As we are into an information technology driven society, knowledge has proved to be an invaluable asset to any individual, organization or government. The business environment faced by all organizations has changed a lot with customers becoming more demanding in terms of their needs and in terms of products and services that they require. Since the format of the data is not predictable there comes a need to refine the data so as to get the most important and useful information in the company data warehouses.

Data mining, also known as knowledge discovery in databases, has been recognized as a promising research area to efficiently extract implicit, understandable, previously unknown and potentially useful information from large databases. Knowledge Discovery in Databases has become one of the most active and exciting research areas in the database community. In recent years, data mining has been used in all kinds of areas of science and engineering, for instance in bioinformatics, genetics, medicine and electrical power engineering. Also people from business find more and more applications for data mining, most applications are found in finance and insurance, retail, telecommunication and security. Keeping all the customer challenges in point of view companies mainly focuses on large amount of data that is supplied on daily basis. One of the prime motives of data mining is to "discover previously unknown relationships among the data, especially when we have different sources of database."

The KDD process includes an iterative sequence method [3], [4]:

- **Selection**: The KDD process includes selecting the data needed for data mining process & may be obtained from many different & heterogeneous data sources.

- **Preprocessing** includes finding incorrect or missing data. It also includes removal of noise or outliers, collecting necessary information to model or account for noise, accounting for time sequence information and known changes.

- **Transformation** is converting the data into a common format for processing. Some data may be encoded or transformed into more usable format. Data reduction, dimensionality reduction & data transformation method may be used to reduce the number of possible data values being considered.

- **Data Mining** is the task being performed, to generate the desired result.

- **Interpretation/Evaluation** is how the data mining results are presented to the users which are extremely important because the usefulness of the result is dependent on it.

III.   CLOUD COMPUTING

The Cloud computing has emerged as a new computing paradigm which aims to provide reliable, customized and dynamic computing environments for end-users. Many companies have begun to attempt to use cloud computing services. In cloud computing, the term "cloud" is used as a metaphor for the Internet and cloud computing is a type of distributed computing paradigm where different services such as servers, storage and applications collectively known as configurable computing resources are rapidly equipped and released with minimal management efforts.

Cloud computing allows individuals and businesses to use software's and hardware's that are managed and hosted by third parties at remote locations. The cloud computing model allows access to information and computer resources from anywhere provided a network connection is available.

The main goal of cloud computing is to combine the distributed resources to achieve higher throughput, high resource utilization and be able to solve large scale computation problems. The cloud computing has many potential advantages in comparison to traditional IT model. But the major barrier for the adoption of cloud computing are the security concerns. Security control measures in cloud are similar to ones in traditional IT environment.

Cloud service delivery is divided among three service models- Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)

IV.   SECURITY OF DATA IN CLOUD

Security is a key barrier to the broader adoption of cloud computing. The real and perceived risks of providing, accessing and controlling services in multitenant cloud environments can slow or hinder the migration to services by IT organizations [12]. Although cloud computing

promises lower costs, rapid scaling, easier maintenance, and service availability anywhere, anytime, a key challenge is how to ensure and build confidence that the cloud can handle user data securely. To make the cloud computing be adopted by users and enterprise, the security concerns of users should be rectified first to make cloud environment trustworthy.

The development of new services bring along new opportunities and challenges. At present, almost all IT enterprises are involved in cloud storage by services provision. But while provision of services, we must take into account the problems emerging from the storage operations in cloud. When the data store on personal devices, users have the highest privilege to operate on them and ensure its security. But once the users choose to put data into cloud, they lose their control over the data [9].The user's authentication and authorization is needed to access the data so as to prevent stealing other user's data through service failure or intrusion.

The data in the cloud may be divided into the data in IaaS environment and the data in PaaS or SaaS environment related to cloud based applications. The data stored in the cloud storages is similar with the ones stored in other places and needs to consider three aspects of information security: confidentiality, integrity and availability. The common solution for data confidentiality is data encryption. To ensure the effect of encryption, the use of both encryption algorithm and key strength are needed to be considered. As the cloud computing environment encompasses large amounts of data transmission, storage and handling so there also needs to consider processing speed and computational efficiency of encrypting large amounts of data. In such cases, symmetric encryption algorithm is more suitable than asymmetric encryption algorithm. The major issue about data encryption is key management. The major issue considered in key management is as who will be responsible for key management. Ideally, the data owners are responsible for managing the key. As the cloud providers need to maintain keys for a large number of users, key management become more complex and difficult [6].

V. STEGANOGRAPHY

Steganography is the process of hiding the one information into other sources of information like text, image or audio file, so that it is not visible to the natural view. There are varieties of steganographic techniques available to hide the data depending upon the carriers we use. In steganography the message is kept secret without any changes but in

cryptography the original content of the message is differed in different stages like encryption and decryption. Steganography supports different types of digital formats that are used for hiding the data. These files are known as carriers. The main file formats that are used for steganography are text, images, audio, video, protocol. Images are the most popular cover objects used for steganography.

VI. MOTIVATION

The major concerns of users or companies, which put their information on the cloud is they are having no idea what's happening to it. When they will have audit of when their information is approached, who access the data increase to strengthen the confidence that their information is being handled properly. Cloud repository purposes an on-demand information service model, and its reputation increasing because of its scaling down and less repair capital properties. Even, safety measure involvement arises when information repository is overcome to third-party cloud companies. This is essential to able cloud users to check their integrity of the important information on cloud, if the information has corrupted or attacked [9]. Cloud infrastructure is multi-holder, with various applications which are sharing physical framework. That gives aid of much capable resource using. Even there is no physical barriers between them, it is necessary to create and maintain balance safety measure controls to lesser the effect of malwares to distribute via cloud [14].Companies taking cloud services need to understand the involvement for maintaining the confidentiality of owners or other critical business information. The major attention is how the physical location of information affects its use. Ensure only specific users and devices can see sensitive information. One of the biggest concerns for companies coming to contact with cloud computing is confidentiality. In fully-managed public cloud service, confidentiality and aloofness risks are often likely to change accordingly to the provider's aloofness policy.

VII. PROPOSED SCHEME

The paper aims to:

1) Implement secure cloud system using CloudSim simulator and java Eclipse

2) Collection and preprocessing of data for mining

3) Encrypt the dataset into an image and securely migrate that image to cloud

4) Apply data mining in cloud and secure the generated mining report.

The proposed methodology is as:

- Request for Data mining report

- Select an image to hide the data mining request

- Encrypt the dataset into an image using edge detection method

- Find the edges of the selected image

- Use these edges as a Pixel keys pattern

- Randomized the pixels and generate the sequence of pattern positions to hide the request

- Convert the request into bits and replace them with the pattern positions

- Send this encrypted image to cloud storage

- Hidden dataset in an image is decoded at the cloud.

- Data mining is performed i.e. from the collections of files and data-sets the mining report is generated.

- For the security purpose, again the mining report is encoded into an image and that image is send to user end

- At user end, image is decoded, and the desired secure mining report is generated.

The proposed solution is to be implemented in CloudSim simulator and Java Eclipse.

The Eclipse Platform [15] is designed and built to meet the following requirements

- Support the construction of a variety of tools for application development.

- Support an unrestricted set of tool provider s, including independent software vendors (ISVs).

- Support tools to manipulate arbitrary content types (e.g., HTML, Java, C, JSP, EJB, XML, and GIF).

- Facilitate seamless integration of tools within and across different content types and tool providers.

- Support both GUI and non-GUI-based application development environments.

- Run on a wide range of operating systems, including Windows and Linux

- Capitalize on the popularity of the Java programming language for writing tools.

VIII. CONCLUSION

In an emerging discipline, like cloud computing, security needs to be analyzed more frequently. With advancement in cloud technologies and increasing number of cloud users,

data security dimensions will continuously increase. Cloud computing security needs consider both technology and strategy, including: audit, compliance and risk assessment. Both the Service providers and the clients must work together to ensure safety and security of cloud and data on clouds. Mutual understanding between service providers and users is extremely necessary for providing better cloud security. In our paper we are laying stress on the security issue in the cloud.

ACKNOWLEDGMENT

REFERENCES

[1] Ruxandra-Ştefania PETRE (2012), **"***Data mining in Cloud Computing"* Database Systems Journal vol. III, no. 3/2012

[2] Sneha Arora and Sanyam Anand, **"***A New Approach for Image Steganography using Edge detection method***",** International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 1, Issue 3, May 2013

[3] Sadie Creese, Paul Hopkins, Siani Pearson, Yun Shen, "Data Protection-Aware Design for Cloud Computing", HP Laboratories

[4] "Introduction to Cloud Computing", Dialogic Corporation

[5] Ranjita Mishra, Sanjit Kumar Dash (2011), "A Privacy Preserving Repository for Securing Data across the Cloud", 978-1-4244-8679-3/11/2011 IEEE

[6] YashpalsinhJadeja, KiritModi (2012), "Cloud Computing - Concepts, Architecture and Challenges", 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET]

[7] Deyan Chen, Hong Zhao (2012), "Data Security and Privacy Protection Issues in Cloud Computing",International Conference on Computer Science and Electronics Engineering

[8] 1T.V.Mahendra 2N.Deepika 3N.Keasava Rao, "Data Mining for High Performance Data Cloud using Association Rule Mining", Volume 2, Issue 1, January 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[9] K.Ganeshkumar H.Vignesh Ramamoorthy, S.Sudha D.Suganya Devi, "An Encrypted Technique with Association Rule Mining in Cloud Environment", National Conference on Advancement of Technologies – Information Systems & Computer Networks (ISCON – 2012)

[10] Henry C. H. Chen and Patrick P. C. Lee (2012), "Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage", 2012 31st International Symposium on Reliable Distributed Systems, IEEE Computer Society

[11] Raghu Yeluri, Enrique Castro-Leon, Robert R. Harmon, James Greene (2012), "Building Trust and Compliance in the Cloud for Services", 2012 Service Research and Innovation Institute Global Conference, 978-0-7695-4770-1/12/2012 IEEE

[12] Engr: Farhan Bashir Shaikh and SajjadHaider(2011), "Security Threats in Cloud Computing",IEEE

[13] Lingjuan Li, Min Zhang, "The Strategy of Mining Association Rule Based on Cloud Computing", 2011 International Conference on Business Computing and Global Informatization

[14] B. KAMALA, "A Study On Integrated Approach Of Data Mining And Cloud Mining", International Journal of Advances In Computer Science and Cloud Computing, ISSN: 2321-4058 Volume- 1, Issue- 2, Nov-2013

[15] Jain Nitin, Meshram Sachin and Dubey Shikha (2012) *"Image Steganography Using LSB and Edge – Detection Technique"*, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July.