International Journal of Pure and Applied Mathematics
Volume 116 No. 9 2017, 273-278
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

DATA LEAKAGE IN CLOUD COMPUTING

G.Michael
Assistant professor, Department of CSE,Bharath University, Chennai.
michel.cse@bharath.unive.ac.in

Abstract: In these days the gift digital world in general is determined by alternate of know-how (i.E).Transfer of data from one individual to a further individual which is sometimes called distributary method. The info is shipped from the distributor to the user are confidential so the info is dispensed best between the distributor and the depended on third parties. The info despatched via the distributor must be secured, confidential and need to no longer be reproduced as the data shared with the relied on third parties are exclusive and incredibly foremost. In some events the information disbursed by way of the distributor are copied through specific dealers who cause a large injury to the institute and this approach of losing the data is referred to as knowledge leakage. The information leakage have to be detected within the early stage with a purpose to look after the information type being open supply. The notion of enhancing the data itself to notice the leakage will not be a brand new method .The data should be detected from leaking by the use of adding false record`s in the information set and which improves probability of selecting leakages in the process. This challenge offers with protecting the information from being out sourcing by giving a distinctive inscription to the touchy knowledge in order that it can't be reproduced. Accordingly, the detection of knowledge from the distributor to retailers is mandatory.

Keywords: Data leakage, Data security, Fake records, Cloud environment, Unintended Leak, Intentional Leak, Malicious Leak.

1. Introduction

Each enterprise follows a further strategy which does no longer fit with any other company. The corporation's understanding safety will depend on workers by way of finding out the rules by way of training and realization-building sessions. However, protection need to go past worker capabilities and canopy the next areas comparable to a physical and logical security mechanism that is tailored to the wants of the corporation and to employee use then the procedure for managing updates and finally it needs an up-to-the-minute documented system[1,3].

Knowledge method protection is most commonly the subject of metaphors. It is usually in comparison with a sequence in the example that a process's protection stage is most effective as robust as the protection degree of its weakest hyperlink. All this goes to show that the hindrance of security have to be tackled at a global stage and need to incorporate the following factors like making users conscious of security problems then the logical safety, i.E. Safety on the data degree, especially organization knowledge[2,4], purposes and even running techniques and in addition merchandise utilized in Telecommunications safety corresponding to community applied sciences, company servers, access networks, etc.

This uncontrolled information leakage places trade in a inclined function. The dealers who get their hands on the sensitive information are often referred to as cyber criminals. Information leakage is done for his or her possess profits which outcome in loss of the enterprise. To overcome this drawback we tried a brand new inspiration of including false objects to the distributary knowledge to find the agent who are misusing the data and take detailed actions. The knowledge consists of 1 constrains and one fake object to fulfill the standards of the protection

1.1 Data Collection Method

Most often, qualitative study commonly emphasizes the human aspect to recognize their habits, abilities, altitudes and fears. The qualitative research involves qualitative information which are got via approaches reminiscent of surveys or interviews[8-9], on-web page observations, and focus agencies. Data are the empirical evidence or understanding one gathers cautiously in line with rules or techniques‟. We also determined that aim of knowledge collection approach is to receive answers from exceptional sources and this may occasionally let the researcher to explain, examine, and relate one characteristic to a further and exhibit that targeted characteristic exist in specified categories[10-11].

Case be taught is a qualitative strategy where the investigator explores a case in certain, and in depth data collection involving multiple sources of knowledge (corresponding to commentary, interviews, records, audio visual substances) and reports a case description and case founded topics.

Truly, there are two types of data collection methods; predominant and secondary. Fundamental knowledge assortment: This methods three exclusive types of techniques; interview, questioning, and remark. It is the most titanic process in all qualitative inquiry. It is first-hand information amassed by way of quite a lot of methods equivalent to statement, interviewing, mailing, and so forth[13].

Secondary knowledge collection: This has been collected and processed through different researchers for exclusive functions than what it is sued for. It is a very common practice to collect, approach, makes use of, and retailer data via organizations and businesses for the help of their operation. The secondary data are on the whole gathered from sources such as magazine, information paper, tv, web, studies, and study articles[12,14].

For this study, interviews, observations, records, and reviews were commonly used as a type of knowledge collection. Primary data are captured from the organization internal expertise base (real time data or empirical information) as considered one of our researcher is working for the organization on knowledge Loss Prevention assignment and an extra researcher have labored in conducting interview questions in to gather the assignment important points with admire to thesis outline. Both closed and open ended questions have been used throughout the interviews, and the interviews were performed in e mail process. Along with this, protection journals, DLP books corresponding to (data Leak Prevention - ISACA), and are used in amassing the info

1.2 Classification of Data Leakage

The expertise leakage into three levels because of this a report containing exclusive data can also be labeled as unintended leak, intentional leak, and malicious leak[15,16].

1.2.1 Unintended Leak:

1. Attach document
2. Zip and send

1.2.2 Intentional Leak:

The intentional leakage in general happens when a person tries to ship a exclusive report without conscious of enterprise coverage and subsequently sends in any case. This is probably carried out when a consumer bypassing the protection ideas and regulations or devices without looking to acquire personal benefits. For example, when an worker renames a document folder and partially copies the data from it.

1.2.3 Intentional Leak

1. Document renames
2. Document type change
3. Partial data copy
4. Remove keyword

1.2.4 Malicious Leak

Malicious leakage most likely brought about when a person intentionally trying to sneak the personal knowledge past the protection rules.

1.2.5 Malicious Leak

1. Character encoding
2. Print screen
3. Password protected
4. Self extracted archive
5. Hide data
6. Policies or product.

For instance, when an worker sneaks a private knowledge from enterprise procedure and sends them through e-mail and even cause vulnerability to the method.

2.1 Dataleakage prevention

- My DLP
- Watermarking method
- Novel system for Hindering the info Leakage
- Impeding information Leakage procedure (IDL)

2.2 Data leakage prevention using my DLP

My DLP is open source all-in-one facts loss prevention software that runs with multi-website online configurations on network servers and endpoint computers. My DLP development mission has made its source code available underneath the terms of the GNU General Public License. My DLP is one of the first loose software tasks for records loss prevention. My DLP permits you to screen, inspect and save you all outgoing personal data without the hassle. With painless deployment and configuration, easy to use policy interface and extraordinary overall performance IT administrators and protection officers are capable of

fight data leakage. With My DLP you may; 1. Block or quarantine outgoing exclusive information from your enterprise community thru mail and net. Archive suspicious files. 2. Monitor removable tool usage for your employer and block or quarantine personal documents copied into those devices including USB memory sticks or clever telephones. 3. Block or quarantine print jobs which comprise confidential information. 4. Discover exclusive information on network storages, databases, workstations and laptops on your company.

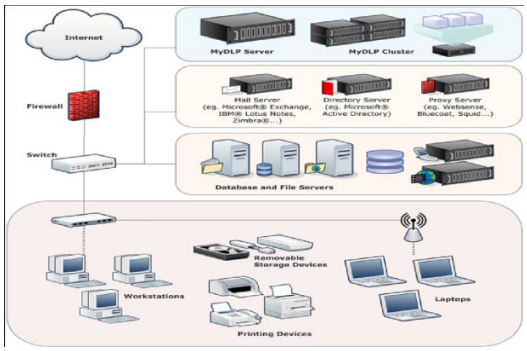

Figure 1. (My DLP)

2.3 Watermarking the data.

A Watermark is a sign this is securely, imperceptibly, and robustly embedded into unique content consisting of an picture, video, or audio signal, generating a watermarked signal and it describes records that can be used for evidence of possession or tamper proofing.

It affords an effective watermarking approach geared for the relational facts. This approach ensures that some bit positions of a number of the attributes of a number of the tuples comprise unique values. The tuples, attributes inside a tuple, bit positions in an characteristic, and precise bit values are all algorithmically decided underneath the manage of a personal key recognised handiest to the proprietor of the statistics. This bit pattern constitutes the watermark. Only if one has get right of entry to to the personal key then it's miles possible to discover the watermark with a few excessive chance.

In Digital Media along with video, audio, picture, text, the information are without problems copied and easily dispensed thru the internet. While sharing secured facts as provided some traditional statistics like Stock market information, Consumer Behavior statistics (Wal-Mart), Power Consumption information, Weather facts the Database outsourcing is a commonplace exercise. So the Watermarking affords an powerful way for proof of authorship by means of signature and the facts because the identical object and additionally it offers an effective manner of tamper proofing by way of integrity records is used and embedded in the records.

2.4 Novel technique for hindering the data leakage

The actual trouble is that the hazard of records loss does no longer growth with cloud computing, it increases whilst personnel leverage their very own gadgets, including clever phones and drugs that show up to leverage cloud for lower back-quit offerings. This is going to be a steady match for maximum in agency IT over the following several years. Users won't surrender their private gadgets at paintings, and they don't need to hold around telephones and drugs. Thus, those in corporation IT want to get higher at dealing with those gadgets, and accordingly keep data at ease. While cloud computing is often the scapegoat of those searching out "statistics leaks," facts has genuinely been leaking for some time. Cloud or no cloud. USB drives were around for years, and plenty of the information that walked out of organizations changed into on those forms of drives, as well as stolen laptops. So, at the same time as it's cool to kick the cloud inside the face[19,20], IT has larger troubles to cope with. The threat of records loss is an exception to the availability dialogue on the previous slide. Users can be able to tolerate an occasional carrier interruption, but non-recoverable facts losses can kill a commercial enterprise. Most cloud computing services use dispensed and replicated international report structures which are designed to insure that hardware screw ups will no longer result in any everlasting information loss, however I consider there's nonetheless value in doing a traditional off website backup of 1's facts, whether that facts is in use by means of traditional servers or cloud computing servers. When seeking out answers, ensure you find ones that backs up data from the cloud[21.22].

Cloud computing sincerely makes experience if your own protection is susceptible, lacking functions, or below common. Ultimately, if the cloud provider's security people are higher than cloud users, the internet-offerings interfaces don't introduce an excessive amount of new vulnerability, and the cloud company goals at the least as high as you do, at protection goals, then cloud computing has higher protection. However, a few issues cannot be tackled with conventional hardware and software program. There are some drawbacks in conventional techniques in computing obligations must be, properly-defined, pretty predictable and computable in reasonable time. Thus, the change computing could be introduced along with DNA based computing, Bio-computing, neural

networks and Quantum computing. This sort of computing are worried inside the subject of system optimization, Robotics and telecommunications. Obviously, those computing could have a few complesity like:

- Compromises between unique desires
- Some natural mechanisms are not well understood
- Well-defined issues cannot be solved in higher way
- Computing Sometimes fails

Thus the implementation of swarm intelligence inside the cloud computing is undertaken in this paper. The swarm intelligence indicates the biological computing by using the conduct of social insects. This paper introduces a singular method, Impeding Data Leakage Technique (IDL) that's worn to hamper the facts leakages in the cloud services the usage of the swarm intelligence, no longer to prevent it however it might halt the outflow of records to make a cozy carrier. IDL approach includes an included swarm intelligence approach recognised to be Ant Colony Optimization (ACO) and Artificial Bee Colony (ABC). The ACO and ABC techniques are included to assemble an obstruct scheme of statistics leakage in cloud computing. The entire server behaviors might be knobbed by using the ACO and the patron behaviors might be dealing with the ABC.

2.5 Impeding data leakage technique (IDL)

The method Impeding Data Leakage (IDL) is extended to avert the outflow of the records throughout conversation inside the cloud services. The facts might be leaked due to the intrusion happens within the environment. A Secure cloud is always a dependable supply of data accordingly shielding the cloud is a totally essential project for protection experts who are in rate of the cloud. Some of the methods by means of which a cloud may be included are Protection of information, making sure information is available for the users, turning in excessive overall performance for the users, using Intrusion Detection System on Cloud to screen any malicious activities, to make certain the utility used by the consumer is safe to apply, the cloud server must offer a help gadget for the user, consumer must be capable of recover any lack of facts inside the cloud. The intruder might attack the information at some stage in the communication route from the server to the cloud users. The lack of manage could ends in the statistics outflow inside the conversation channels

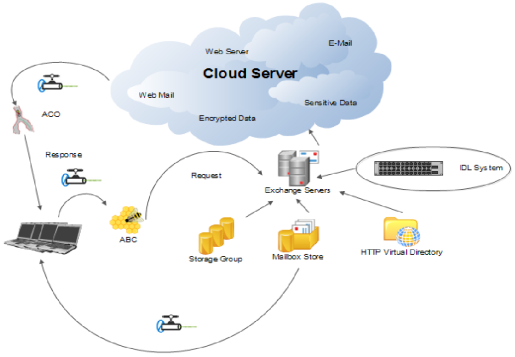

Figure 2. (cloud server)

The cloud provider is greater cozy than the other computing offerings, however in this case it is able to purpose some information loss all through transmission. Thus, this context constructs a method to completely hinder the facts loss, recognised to be IDL. The time period “Impede” publicizes that completely halts the records loss and stops the communique channels. The foremost goal of this paper is to avoid the leakage through redirecting the paths primarily based on the swarm intelligence techniques (ABC & ACO). The consumer requests are exceeds to the cloud server with the possible and responsible routes in the cloud surroundings. In this nation, the requests are analyzed and the conversation route is built by means of the use of the method of swarm intelligence regarded to be Artificial Bee Colony (ABC). The transmission route is generated by using the ABC most effective if the possible routes to the cloud server are responsible in confirm and also the accountable routes are evaluated that there is probably any incidence of records leakage, if outflow happens then next accountable direction is selected for the request transmission. After transmitting requests, the cloud server responses to the purchaser requests the usage of Ant Colony Optimization (ACO). The server responses are transferred via optimized direction to the client, as same as ABC the optimized course restrains any leakage of information and if leakage takes place the ACO chooses the subsequent optimized path to transfer the statistics. ACO and ABC swarm intelligence strategies is based totally at the concept of stigmergy. Stigmergy is a mechanism of conversation by means of modifying the environment. Ant Colony Optimization and Artificial Bee Colony use artificial stigmergy. This kind method used for fixing issues which can be expressed as finding properly paths thru graphs.

2. Conclusion

The information leakage detection in information system is obtained through following primary strategies

like watermarking on distinctive data. This facts leakage issue can be dealt with in a couple of approaches which should be studied later. When the information is watermarked it secures the statistics from being open source and helps to find out the cybercriminal by means of the use of the fake items located a tone of kind positions of records this is to be sent.

References

[1]R. Sion, M. Atallah, and S. Prabhakar, ―Rights Protection forRelational Data,‖ Proc. ACM SIGMOD, pp. 98-109, 2003.

[2]R.AgrawalandJ.Kiernan,Watermarking relational databases‖. In VLDB '02: Proceedings of the 28th international conference on Very Large Data Bases, pages 155–166. VLDB Endowment, 2002.

[3]Hartun and kutter,Watermarking technique for multimedia data‖2003.

[4]Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.

[5]Kaliyamurthie K.P., Parameswari D., Udayakumar R., QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, v-6, i-SUPPL5, pp-4648-4652, 2013.

[6]Brintha Rajakumari S., Nalini C., An efficient cost model for data storage with horizontal layout in the cloud, Indian Journal of Science and Technology, v-7, i-, pp-45-46, 2014.

[7]Brintha Rajakumari S., Nalini C., An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, v-7, i-, pp-44-46, 2014.

[8]Khanna V., Mohanta K., Saravanan T., Recovery of link quality degradation in wireless mesh networks, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4837-4843, 2013.

[9]Khanaa V., Thooyamani K.P., Udayakumar R., A secure and efficient authentication system for distributed wireless sensor network, World Applied Sciences Journal, v-29, i-14, pp-304-308, 2014.

[10]Udayakumar R., Khanaa V., Saravanan T., Saritha G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, v-16, i-12, pp-1781-1785, 2013.

[11]Khanaa V., Mohanta K., Saravanan. T., Performance analysis of FTTH using GEPON in direct and external modulation, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4848-4852, 2013.

[12]Kaliyamurthie K.P., Udayakumar R., Parameswari D., Mugunthan S.N., Highly secured online voting system over network, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4831-4836, 2013.

[13]Thooyamani K.P., Khanaa V., Udayakumar R., Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, v-20, i-12, pp-2464-2470, 2014.

[14]R.Kalaiprasath, R.Elankavi, Dr.R.Udayakumar, Cloud Information Accountability (Cia) Framework Ensuring Accountability Of Data In Cloud And Security In End To End Process In Cloud Terminology, International Journal Of Civil Engineering And Technology (Ijciet)Volume 8, Issue 4, Pp. 376–385, April 2017.

[15]R.Elankavi, R.Kalaiprasath, Dr.R.Udayakumar, A fast clustering algorithm for high-dimensional data, International Journal Of Civil Engineering And Technology (Ijciet), Volume 8, Issue 5, Pp. 1220–1227, May 2017.

[16]R. Kalaiprasath, R. Elankavi and Dr. R. Udayakumar. Cloud. Security and Compliance - A Semantic Approach in End to End Security, International Journal Of Mechanical Engineering And Technology (Ijmet), Volume 8, Issue 5, pp-987-994, May 2017.