Data Leakage Detection of Guilty Agents and Security Strategies using Encryption Algorithm and MAC Address

[1]Krishna Murari, [2]Mr. Mahesh kumar,
[1]PG Student M.tech CSE, [2]Associate Professor GITAM,
[1]Computer Science Engineering,
[1]Ganga institute of Technology and Management, kablana , haryana, India

Abstract : There are a unit of several websites that publish data and supply access of knowledge on the network. All that internet sites has many alternative web application programs that contains potential data or knowledge that got to be protected. In many organizations, business scenarios and company outsource its data to the other company or organization or agents, all these agents are known as trusted third party agents. The knowledge owner provides the confidential knowledge to the sure third party agents and their risk that any of that sure agent will leak the potential data. It is obligatory to notice the guilty agent, who leaks the data to unauthorized agents. For identification of leaked data in existing system uses watermarking technique and data allocation strategies with adding fake objects. However, it has deficiency is that watermarking data can be modified or change. In projected system uses AES algorithmic rule for coding of requested knowledge. As a result, unauthorized party is unable to view or access the confidential data. One more technique used for up probabilities of police work guilty agent is raincoat (Media Access Control) address.

***IndexTerms* –AES algorithm, Guilty Agent, Watermarking.**

I. INTRODUCTION

Any organisation company, or business, all have their confidential data. And all these data consisting of customer details, patient records, credit card details, finance information. All these kind of data must be protected from unauthorized access. Sometimes company has to share that data to the trusted third party agents for surveying, improving, research etc. At that time security of that data is a major question. If any agent from them will leak the confidential data, it leads a greatest financial loss.

So, it's a desire to supply the confidentiality of the information and determine the guilty agents, which are from the trusted agents, who leak the data to unauthorized person.

For rising the possibilities of characteristic guilty agents, another new technique has been proposed.

This technique can use the Mack and IP address and AES formula.

The MAC address improves the chances of identifying guilty agents. And AES algorithm will encrypt the requested data by the agents.

1.OBJECT

- ✓ A information distributor has given sensitive data to a group of purportedly trusty agents (third parties). Some of the data is leaked and found in an unauthorized place (e.g., on the web or somebody's laptop).
  The distributor should assess the chance that the leaked information came from one or additional agents, as opposed to having been independently gathered by other means.
- ✓ We propose information allocation ways (across the agents) that improve the chance of distinctive leakages.
- ✓ These ways don't suppose alterations of the discharged information (e.g., watermarks).
- ✓ In some cases we can also inject? Realistic but fake?

- ✓ Data records to additional improve our probabilities of sleuthing leak and distinctive the cause. Our goal is to detect when the distributor?
- ✓ sensitive information has been leaked by agents, and if possible to identify the agent that leaked the data.
- ✓ A data distributor has given sensitive data to a set of supposedly trusted agents (third parties).
- ✓ Some of the info is leaked and located in Associate in Nursing unauthorized place (e.g., on the web or somebody's laptop).

  The distributor must assess the likelihood that the leaked data came from one or more agents, as opposed to having been independently gathered by other means. We propose data allocation strategies (across the agents) that improve the probability of identifying leakages. These methods do not rely on alterations of the released data (e.g., watermarks). In some cases we will conjointly inject "realistic however fake" information records to additional improve our probabilities of sleuthing leak and distinctive the cause.

1.2 EXISTING SYSTEM

conventional, watermarking is used to handle leakage detection , e.g., in each distributed copy a unique code is embedded. The leaker can be identified If that copy is later discovered in the hands of an unauthorized party.

Disadvantages of Existing Systems

In some cases Watermarks are often terribly helpful, but again, involve some modification of the initial information. Furthermore, if the data recipient is malicious ,watermarks can sometimes be destroyed. E.g. A hospital could provide patient records to researchers UN agency can devise new treatments. Similarly, a corporation could have partnerships with alternative firms that need sharing client information. Another enterprise could source its processing, thus information should run to numerous alternative firms. We decision the owner of the info the distributor and also the purportedly trusty third parties the agents.

2. PROPOSED SYSTEM

- Our major goal is to detect when the distributor's sensitive data has been leaked by agents, and if possible to identify the agent that leaked the data.
- Perturbation is a useful technique, in which the data is modified and made "less sensitive" before being handed to the agents.
- We develop unobtrusive techniques for sleuthing leak of a group of objects or records.
- We can develop such a model for assessing the "guilt" of agents and leakage can be avoided.
- We also present an algorithms for distributing objects to agents, in such a way that enhance our chances of identifying a leaker.
- Lastly, we can also consider the option of adding "fake" objects to the distributed set. Such objects don't correspond to real entities however seem realistic to the agents.
- In proposed system, for the entire set without modifying any individual members the fake objects can be acts as a type of watermark. If it seems associate in Nursing agent was given one or additional pretend objects that were leaked, then the distributor can be more confident that agent was guilty.

Problem Setup and Notation

A distributor owns a set T=of valuable data objects.

The distributor needs to share a number of the objects with a group of agents U1,U2,?

Un, however doesn't would like the objects be leaked to alternative third parties.

The objects in T may be of any sort and size, e.g., they could be tuples in a relation, or relations in a database.

An agent Ui receives a set of objects, determined either by a sample request or a particular request:

1. Sample request
2. Explicit request

3. CONCLUSIONS

From the study of the data leakage, we study the various possibility that an agent may be responsible for data leakage using some techniques. We analyzed that distributing data may enhance the chances of detecting the agents effectively specially when there is a large overlap in the data that agents must receive. Our objective was to verify the results of algorithms that finding the guilt agent among company. Hence, we can conclude that if the distributor wants to completely satisfy an agent before allocating any object to other agents our technique must be used in order to improve the chances of identifying the leaker. Our future work Organizational culture if improperly or hurriedly implemented. Careful planning and preparation, communication and awareness training are paramount in deploying a successful program.

4 ACKNOWLEDGEMENT

For all the efforts behind the paper work, I first & foremost would like to express my sincere appreciation to the staff of Dept. of Computer Sci.& Engg., for their extended help & suggestions at every stage of this paper. It is with a great sense of gratitude that I acknowledge the support, time to time suggestions and highly indebted to my guide associate Professor Mr. Mahesh Kumar and Dr. Neetu Sharma (HOD). Finally, I pay sincere thanks to all those, who indirectly and directly helped me towards the successful completion of the this paper.

5.REFERENCES

[1] J.J.K.O.Ruanaidh, W.J.Dowling, and F.M.Boland," Watermarking Digital Images For Copyright Protection", IEE Proc.Vision,Signal and Image Processing,vol.143,no.4,pp.250-256,1996.

[2] F.Hartung and B.Girod,"Watermarking of Uncompressed and Compressed Video," Signal Processing, vol.66, no.3,pp.283-301,1998.

[3] S.Czerwinski, R.Fromm,and T.Hodes,"Digital Music Distribution and Audio watermarking," http://www.Scientificcommons.org/43025658,2007.

[4] S.Jajodia, P.Samarati, M.L.Sapino,and V.S. Subrahmanian,"Flexible Support For Multiple Access ControlPolicies,"ACMTrans.DatabaseSystems vol.26.no.2.pp.214-260,2001.

[5] Data Leakage: Affordable Data Leakage Risk Management by Joseph A. Rivela Senior Security Consultant P.P (4-6)