ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2015**

# Optimal Solution for Monitoring Data Objects with Trusted and Untrusted Agents

Maria Yesudas

M.Tech Student, Dept. of CSE, Viswajyothi College of Engineering and Technology, Vazhakulam, Kerala, India

**ABSTRACT:** Data misuse may be happened by entities like an organizations employees and business share holders who are allowed access to sensitive information and misuse their privileges. The users can be either trusted or un-trusted. The access of un-trusted parties to data objects, such as patient records should be viewed in an attempt to detect misuse. To find the data misuse, the data objects should be encrypted with digital signature. The digital signature is an encoded form embedded into a single file. The signature should contain current date and time and bank login user. However, monitoring data objects is resource intensive and time-consuming and may also cause disturbance or inconvenience to the involved employees. So that, the monitored data objects should be carefully choose. Two optimization issues are carefully designed for selecting specific data objects for monitoring, such that the detection rate is increased and the monitoring effort is reduced. In the first optimization problem, the goal is to select data objects for monitoring that are accessed by at most C trusted agents while ensuring access to at least k viewed objects by each un-trusted agent, both c and k are integer variable. As opposed to the first optimization problem, the goal of the second optimization problem is to select monitored data objects that maximize the number of monitored data objects accessed by un-trusted agents while ensuring that each trusted agent does not access more than d monitored data objects, d is an integer variable as well. After getting the specific data objects, it should be sent to un-trusted agents and can detect the guilty agents by using the digital signature.

**KEYWORDS**: un-trusted agents, Data misuse, guilty agents.

## I. INTRODUCTION

Data security means protecting data, such as a database, from destructive forces and from the unwanted actions of unauthorized users. A data misuse incident occurs when a privileged insider exploits his legitimate ability to access sensitive data for inappropriate purposes. Data leakage is a type of data misuse threat in which an authorized person publishes or publicly hands over confidential information, intentionally or unintentionally. For instance, a business partner may hand over sensitive information about firm customers to a competitor in exchange for money, or he may copy this information to a thumb drive that subsequently gets lost.

Today's business environment requires organizations to collaborate. It is not un-common for companies to outsource some of their tasks and services to subcontractors. For example, a cellular company may outsource customer-related services, advertising campaigns, information technology infrastructures, and more. In such environments, sharing secrets and sensitive information is inevitable. An attacker originating from a third-party partner usually seeks sensitive information assets of the company. In addition, many of the data loss incidents of the past decade were caused by un-trusted partners who failed to protect the data. Therefore, organizations must put significant effort into the protection of confidential information. Naturally, organizations tend to trust their own employees more than those of their partners, thus necessitating efficient security mechanisms to monitor the use of sensitive information and detect data misuse incidents.

## II. RELATED WORKS

A Data misuse is the process of accessing sensitive data by unauthorized party. The main aim of the system is to optimize the data misuse detection. There are different techniques for detecting the data misuse from untrusted agents. The goal of this literature survey is to find the different techniques and methods adopted for detecting data misuse.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2015**

1. Detection Of Guilty Agents For Data Misuse Detection

Agents within multi agent systems represent different stakeholders that have their own distinct and sometimes convicting interests and views. They would behave in a way so as to achieve their own objectives, even at the cost of others. Recent years have seen an increasing number of agents being developed to extend the sphere of human. Those agents, with their autonomous reasoning and decision-making capability, can engage in complex communications on behalf of their owners. There is no single-agent system. Agents usually live in a society of agents, which is known as multi agent system. Usually, agents in multi agents system represent various stakeholders, each with distinct interests and objectives. They try to pursue their own objectives, even at the cost of others. In the course of doing business, sometimes sensitive data must be handed over to supposedly trusted third parties. The data allocation strategies help the distributor intelligently give information to agents. Fake objects are added to identify the guilty part, to address this problem four instances are specified. Depending on which the data request is provided. Depending upon the type of data request, the fake objects are allowed.

2. Encryption Policies for Regulating Access to Outsourced Data

Recent access control methods assume that resources are under the hand of a trusted party which monitors each access request to verify if it is compliant with the specified access control policy. There are many scenarios where this approach is becoming no longer adequate. Many clear technologies in Web technology are creating a need for owners of sensitive information to manage access to it by legitimate users using the services of very honest but anxious third parties, that is, parties trusted with giving the required service but not authorized to read the actual data content. The solution puts forward a new approach that clubs cryptography with authorizations, thus enforcing access control through selective encryption. The most convincing and evolving solutions for these scenarios assume that the data owner encrypts data before sending them to the server for storage and gives the corresponding key to users authorized to access the data as shown in Figure 1. The goal of the solution is to translate an authorization policy to be enforced in an equivalent encryption policy regulating which data are encrypted with which key and regulating key release to the users. It is guided by the principles of releasing at most one key to each user, and encrypting each resource at most once. To achieve them, exploit a hierarchical organization of keys allowing the derivation of keys from other keys and public tokens. The aim is then to reduce the number of tokens to be generated and maintained.

## III. ARCHITECTURE

Data misuse may be performed by entities such as an organizations employees and business partners who are granted access to sensitive information and misuse their privileges. Assume that users can be either trusted or untrusted. The access of untrusted parties to data objects (e.g., client and patient records) should be monitored in an attempt to detect misuse. However, monitoring data objects is resource intensive and time-consuming and may also cause disturbance or inconvenience to the involved employees. Therefore, the monitored data objects should be carefully selected. Here, there are two optimization problems carefully designed for selecting specific data objects for monitoring, such that the detection rate is maximized and the monitoring effort is minimized.

Optimization algorithm 1 is defined to minimize the wasted monitoring effort of the organization that is, monitoring items that are accessed by trusted agents. The goal in optimization algorithm 2 is to find an assignment of monitored data objects that maximize the number of monitored data objects that are accessed by untrusted agents, the chances for revealing misuse incidents will grow by monitoring more of these data objects while ensuring that each trusted agents list does not contain more than a predefined number d of monitored data objects. A data misuse incident occurs when a privileged insider exploits his legitimate ability to access sensitive data for inappropriate purposes. Today's business environment requires organizations to collaborate. It is not uncommon for companies to outsource some of their tasks and services to subcontractors. In such environments, sharing secrets and sensitive information is inevitable. An attacker originating from a third-party partner usually seeks sensitive information assets of the company.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

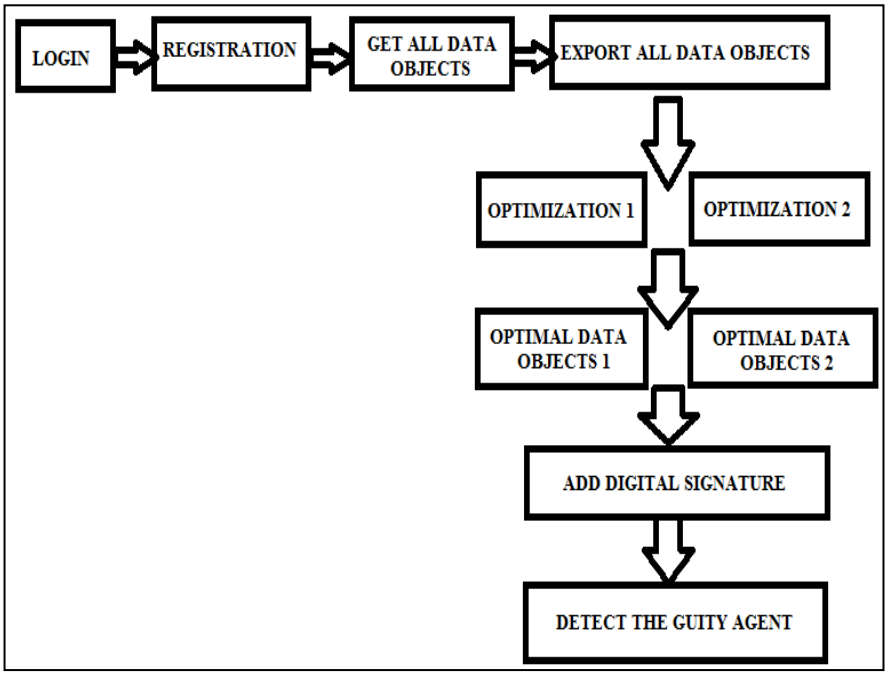


Figure 1: Block Diagram for Proposed System

System Overview:

The system will helps to find out the guilty agents, who are misusing the data. Optimal data objects are retrieved by the above mentioned algorithms. After that, digital signature should be added to that optimal data objects to find out the guilty agents. Digital signature will help to find who all are misusing the data. The two algorithms will help to find the optimal data objects for monitoring but cannot reduce the tendency to misuse the data objects. The proposed enhancement mainly includes a model for reducing the leakage. Here, a signature is added with the data objects and it can be accessed only through a decoder application. The decoder application can verify the signature on the data objects. This can be an enhanced steganographic model with signature implementation. This model reduces the data leakage. The trusted agents can have the decoder application through which only they can reproduce the data. The implemented optimization algorithm along with this signature embedding model can improve the overall efficiency of the system. This model combines the Data Protection, leakage detection and optimization. Even though lot of methods [1], [3], [7] are currently available for data leakage detection, here implements data leakage detection along with optimizing data misuses detection.

Digital Signature:

Digital signatures are the public-key prime units of message authentication. Likewise, a digital signature is a method that binds a person or entity to the digital content data. This binding can be independently verified by receiver as well as any third party. Digital signature is a cryptographic value which can be calculated from the data and a secret key known only by the signer. In real world, the receiver of message needs assurance that the message belongs to the sender and he or she should not be capable to repudiate the creation of that message. This requirement is very critical in business applications, since likelihood of a dispute over exchanged data is very high.

It should have a public-private key pair. Generally, the key pairs used for encryption/decryption and signing or verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key values. Since digital signature is created by 'private' key of signer and no one else can have this the signer cannot repudiate signing the data in future. By putting public-key encryption to digital signature scheme, it can

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2015**

create a cryptosystem that can provide the four essential elements of security namely Privacy, Authentication, Integrity, and Non-repudiation.

Generate Public and Private Keys

In order to be able to create a digital signature, we need a private key. Its corresponding public key will be needed in order to verify the authenticity of the signature. A key pair is generated by using the KeyPairGenerator class. In this, we will generate a public/private key pair for the Digital Signature Algorithm (DSA). We can also generate keys with a 1024-bit length.

Generating a key pair requires several steps:

- Key Pair Generator Creation:
  The way to get a KeyPairGenerator object for a particular type of algorithm is to call the getInstance static factory method on the KeyPairGenerator class. This method has two forms, both of which have a String algorithm first argument; one form also has a String provider second argument.

  KeyPairGenerator keyGen = KeyPairGenerator.getInstance("DSA", "SUN");

  This method has two forms, both of which have a String algorithm first argument and a String provider as second argument.

- Key Pair Generator Initialization:
  The next step is to initialize the key pair generator. All key pair generators share the concepts of a keysize and a source of randomness. The KeyPairGenerator class has an initialize method that takes these two types of arguments.The key size for a DSA key generator is the key length (in bits), which will set to 1024. The source of randomness must be an instance of the SecureRandom class that provides a cryptographically strong random number generator(RNG).

  SecureRandom random = SecureRandom.getInstance("SHA1PRNG", "SUN");
  keyGen.initialize(1024, random);

  The key size for a DSA key generator is the key length in bits set to 1024. The source of randomness must be an instance of the SecureRandom class that provides a cryptographically strong random number generator(RNG). An example requests an instance of SecureRandom that uses the SHA1PRNG algorithm, as provided by the built-in SUN provider.

- The Pair of Keys Generation:
  The final step is to generate the key pair and to store the keys in PrivateKey and PublicKey objects.

  KeyPair pair = keyGen.generateKeyPair();
  PrivateKey priv = pair.getPrivate();
  PublicKey pub = pair.getPublic();

## IV. PERFORMANCE EVALUATION

The Performance of the system is evaluated by the two optimization algorithm. Both the algorithms give optimal data objects with minimum time. But by comparing them, we can see that Optimization 2 algorithm performs well and gives better result than Optimization 1. Optimization 1 will give optimal solution in which it may or may not satisfy all the constraints. But, Optimization 2 will give optimal solution only when it satisfies all the constraints. So, we can conclude that Optimization 2 performs well when compared to Optimization 1. Empirical evaluation showed that the proposed algorithms reached a significantly greater ability to identify the source of leakage (compared with simple allocation algorithms), even in cases where there was a large overlap between the objects that the agents received. In

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2015**

Optimization 1 algorithm shown in Figure, the optimal data objects generated are Value Added Details and Contact details. This result is not obtained by satisfying all the constraints or conditions. The algorithm 1 will favour data objects with a lower ratio, where the optimal ratio is zero - that is, no trusted agent accesses the data object and at least one untrusted agent accesses it. Additionally, the algorithm 1 ignores data objects that are not accessed by any of the untrusted agents. The algorithm also ignores data objects that are accessed by more than c trusted agents and therefore do not satisfy the second type of constraints. Here, in Optimization 2 algorithm shown in Figure 4.2, the optimal data objects generated are Account Details, Card Details and Contact Details. This result is not obtained by satisfying all the constraints or conditions. As opposed to Optimization

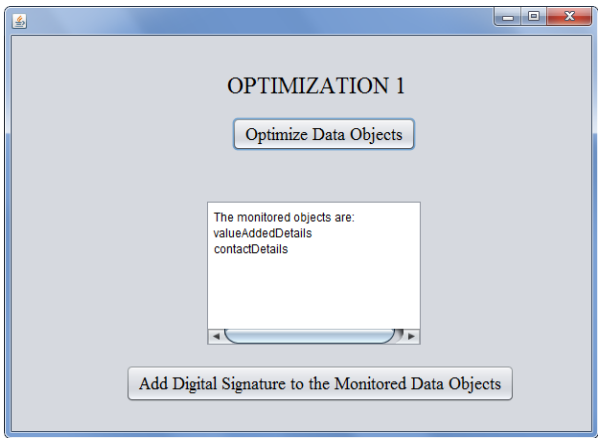


Figure 2: Optimization 1

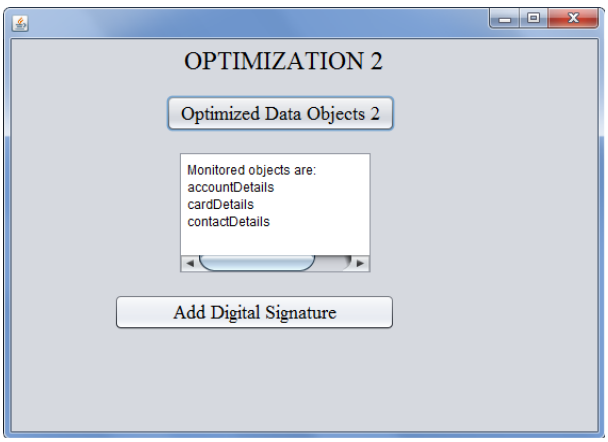


Figure 3: Optimization 2

problem 1, the goal in Optimization problem 2 is to find an assignment of monitored data objects that maximize the number of monitored data objects that are accessed by untrusted agents, the chances for revealing misuse incidents will grow by monitoring more of these data objects while ensuring that each trusted agents list does not contain more than a predefined number d of monitored data objects. Applying the selection approach represented by Optimization problem 2 will be preferred over Optimization problem 1 in cases where it is important to limit the number of monitored objects in a trusted agents list when the monitoring process interrupts the agent's ongoing work, or when there are many trusted agents and only a few untrusted agents. In doing so, it would help to achieve a balance and a level of fairness by constraining the amount of disruption or inconvenience experienced by the same trusted agent while providing the organization the opportunity for in-depth investigation of data objects accessed by the untrusted agents.

## V. CONCLUSION AND FUTURE WORK

A data misuse incident occurs when a privileged insider exploits his legitimate ability to access sensitive data for inappropriate purposes. Various techniques are studied for detecting data misuse or leakage. All the techniques which discussed above have some advantages when compared to other. Using fake objects prevent most of the data misuse events. Recently, encrypting the data is used. Honey tokens are also used to detect the leakage. But, they found to be more costly when compared to other. So, a different method for selecting specific data objects to efficiently monitor and detect data misuse incidents performed by insiders. In the addressed scenario, trusted and untrusted agents are authorized to access a predefined list of data objects out of a shared data object collection. This method suggests monitoring only a subset of data objects that are selected in such a way that the monitoring effort is minimized while the detection rate is maximized. This technique will help for optimal selection of data objects for monitoring. It will take less time when compared to other methods and provides more efficient results.

## REFERENCES

[1] Umamaheswari, S.,Geetha, \Detection Of Guilty Agents For Data Misuse Detection ", National Conference on Innovations in Emerging Technology (NCOIET), January 2010 pp. 23-26

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2015**

[2] Sabrina de Capitani Di Vimercatti and Sara Foresti, \Encryption Policies for Regulating Access to Outsourced Data ", ACM Transactions on Database Systems, Vol. 35, No. 2, Article 12, April 2010.
[3] Jonathan White Brajendra Panda, \Insider Threat Discovery Using Automatic Detection of Mission Critical Data Based On Content ", 2010 Sixth International Conference on Information Assurance and Security (IAS),23-25 Aug. 2010, pp. 56 - 61
[4] Amir Harel, Asaf Shabtai, \M-Score: Estimating the Potential Damage of Data Leakage Incident by Assigning Misuseability Weight ", Insider Threats '10: Proceedings of the 2010 ACM workshop on Insider threats ,October 8, 2010, Chicago, Illinois, USA.
[5] Ma'ayan Gafny, Asaf Shabtai, \Detecting Data Misuse by Applying Context Based Data Linkage ", Insider Threats '10: Proceedings of the 2010 ACM workshop on Insider threats, October 2010.

## BIOGRAPHY

Maria Yesudas was born in Kerala, India on March 27, 1990. She did her Bachelor of Technology in Computer Science and Engineering from Toc H Institute of Science and Technology, Arakkunnam, Ernakulam, Kerala, India in the year 2012. She is currently pursuing her Master of Technology in Computer Science and Engineering from Viswajyothi College of Engineering and Technology, Vazhakulam, Kerala.

Her field of interest lies in areas of security Right from the time she had been doing her bachelor's degree her focus was on building applications for security.