JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

PREVENTION OF DATA LEAKERS INSPARTIAL DOMAIN

K.Nandini[1],Dr.S.Chandrasekaran[2]K.Thiyagu[3],

[1]AssistantProfessor, Department of ComputerScienceandEngineering,PSVCollegeof Engineering and Technology, Krishnagiri.
[2]Head of the Department, Department of Computer Science and Engineering, PSV College of Engineering and Technology, Krishnagiri.
[3]Student, Department of Computer Science and Engineering,PSVCollegeof Engineering and Technology, Krishnagiri.

Abstract: The enterprise may outsource its data processing, and data must be given to various other companies. We call the owner of the original data the distributor and the supposedly trusted third parties the agents. And Our goal is to detect when the distributor’s sensitive data has been leaked by agents, or Other third-party and if possible to identify the agent that leaked the data. The project considers applications where the original sensitive data cannot be perturbed. Perturbation is very high and a very useful technique where the data is modified and made “low sensitive” before being handed to agents. For example, one ore more can add random noise to certain attributes, or one can replace exact values by ranges. However, in some cases it is important not to alter the original distributor’s data. For this project we are study unobtrusive techniques for detecting leakage of a set of objects or records in the data.

Specifically, we study the following scenario: After giving the set of objects to agents, the distributor discoverssomeofthosesameobjectsinanunauthorizedplace.thispointthedistributorscanassessthe likelihood that the leaked data came from one or more agents, as opposed having been independently gathered by Other mean. Finally, we also consider the option of adding “fake” or" Not real" objects to the distributed set. Such objects do not correspond to real entities but appear realistic to the agents. This Project is developed in Asp.net as front end and back end as SQL server.

KEYWORDS:
Symmetric Key,Fake Objects, Data Distributor,UnobtrusiveTechniques,E-mails.

INTRODUCTION

Theaimoftheprojectistotransferthedatainasecuremanner.Thisprojectwill eliminate the situation that the data is viewed by third person (i.e., hacking of data).In the course of doing business, sometimes sensitive data must be handed over to supposedly trusted third parties. Traditionally, leakage detection is handled by watermarking. In this project we use a technique called unobtrusive for detecting leakage of a set of objects or records. The main objective of our project is to detect the information leakage and to prevent it

A data distributor has given sensitive data to a set of supposedly trusted agents (third parties). Some of the data is leaked and found in an unauthorized place(e.g., on the web or somebody's laptop). We propose data allocation strategies (across the agents) that improvethe probabilityofidentifyingleakages.Insomecaseswecanalsoinject"realisticbutfake"data records to further improve our chances of detecting leakage and identifying the guilty party Our goal is to detect when the distributor's sensitive data has been leaked by agents,andif possible toidentifytheagentthatleakedthedata.Perturbationisaveryusefultechniquewherethedatais modifiedandmade"lesssensitive"beforebeinghandedtoagents.Theprojectisdevelopedusing ASP as its front end and SQL Server as its back end process should be time oriented ,The system will over come all the disadvantages of the existing system. It minimize the manual effect and time consumption will be minimum.

OBJECTIVES OF THE STUDY:

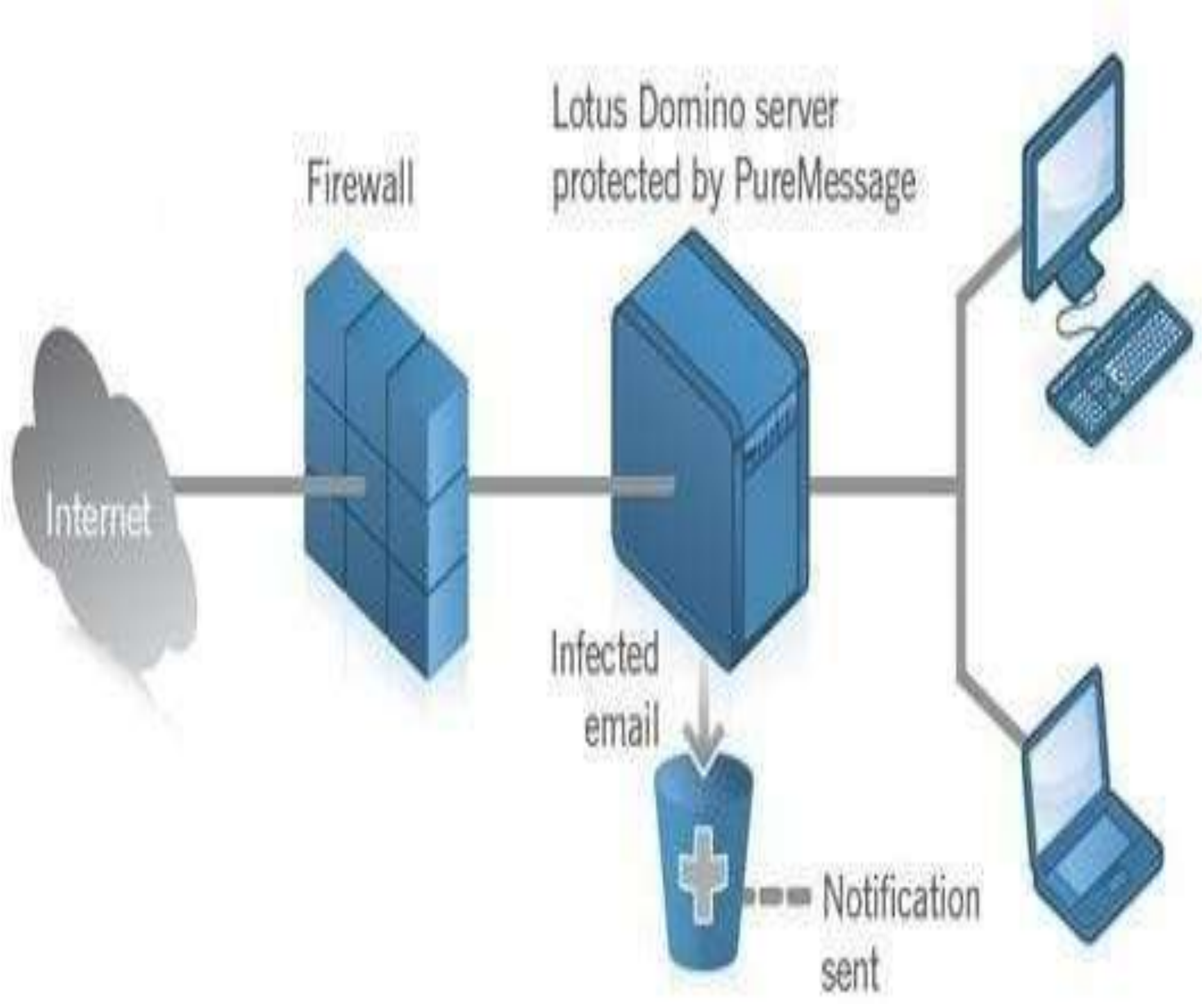
2 The main objective of our project is to detect the information leakage and to prevent it. A data distributor has given sensitive data to a set of supposedly trusted agents(third parties).Some of the datas leaked and found in an unauthorized place(e.g., on the web or somebody's laptop). We propose data allocation strategies (across the agents) that improve the probability of identifying leakages. In some cases we can also inject "realistic but fake" data records to further improve our chances of detecting leakage and identifying the guilty party.

FUTURE ENHANCEMENT:

In future it is a possible one to add new web pages without any problem with enhanced. As the technology use disgoo doneitis flexible or future enhancement and it is also possible to alter the front-end and back-end without any problem.

This web-base doneis created effectively in a user-friendly manner and any new systemthatisdevelopedinfuturemustbeincorporatedorupdatedwithoutanyproblem.Sothis will support enhancements in future. Our future work includes the investigation of agent guilt models that capture leakage scenarios that are not studied n this paper. For example,

what is the appropriate model for cases where agents can collude and identify fake users A preliminary discussion of such a model is available in future. Another open problem is the extension of our allocation strategies so that they can handle online fashion (the presented)



SYSTEM ARCHITECTURE

SYSTEM IMPLEMENTATION:

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, c system will work and be effective.Theimplementationstageinvolvescarefulplanning,investigationoftheexistingsyste m and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

FEATURES OF C#:

- C#. Net [2] has flexibility, allowing one or more language to interoperate to provide the solution. This Cross Language Compatibility allows to do project at faster rate.
- C#. Net has Common Language Runtime, that allows all the component to converge into one intermediate format and then can interact.
- C#.Net has provide excellent security when your applications executed in the system
- C#.Net has flexibility, allowing us to configure the working environment to best suit our individual style. We can choose between a single and multiple document interfaces, and we can adjust the size and position in go the various IDE elements.
- C#.NethasIntelligencefeaturethatmakethecodingeasyandalsodynamichelpprovides very less coding time.
- The working environment in C#.Net is often referred to as Integrated Development Environment because it integrates many different functions such as design, editing, compiling and debugging within a common environment. In most traditional development tools, each of separate program, each with its own interface.
- The C#.Net language is quite powerful if we can imagine a programming task and accomplished using C#.Net
- After creating a C#. Net application, if we want to distribute it to others we can freely distribute any application to anyone who uses Microsoft windows. We can distribute our applications on disk, on CDs, across networks, or over an intranet or the internet.
- Toolbars provide quick access to commonly used commands in the programming environment. We click a button on the tool bar once to carry out the action represented by that button. By default, the standard toolbar is Displayed when we start Visual Basic. Additional toolbars for editing, form design, and debugging can be toggled on or off from the toolbars command on the view menu.
- Many parts of C# are context sensitive. Context sensitive means we can get help on these parts directly without having to go through the help menu. For example, to get help on any keyword in the C# language, place the insertion point on that keyword in the code window and press F1.
- C# interprets our code as we enter it, catching and highlighting most syntax or spelling errors on the fly. It’s almost like having an expert watching over our shoulder as we enter our code.

FRONT-END: ASP.NET:

FEATURESOF.NET:

- Microsoft .NET is a set of Microsoft software technologies for rapidly building and integrating XML Web services, Microsoft Windows-based applications, and Web solutions. The. NET Framework is a language- neutral platform for writing programs that can easily and securely interoperate. There's no language barrier with .NET: there are numerous languages available to the developer including Managed C++, C#, Visual Basic and Java Script. The .NET framework provides the foundation for components to interact seamlessly, whether locally or remotely on different platforms. It standardizes common data types and communications protocols so that components created in different languages can easily interoperate.
- ".NET" is also the collective name given to various software components built upon the .NET platform. These will be both products (Visual Studio.NET and Windows.NET Server, for instance) and services (like Passport, .NET My Services, and so on).

CONCLUSION:

In a perfect world there would be no need to hand over sensitive data to agents that may unknowingly or maliciously leak it. And even if we had to hand over sensitive data, in a perfect world we could watermark each object so that we could trace its origins with absolute certainty. However, in many cases we must indeed work with agents that may not be 100% trusted, and we may not be certain if a leaked object came from an agent or from some other source, since certain data cannot admit watermarks

REFERENCE

1. User Inter faces in C#: Windows Forms and Custom Controls by Matthew MacDonald.
2. Applied Microsoft® .NET Frame work Programming(Pro-Developer)by Jeffrey Richter.
3. Practical .Net2 and C#2: Harness the Platform, the Language, and the Frame work by Patrick Smacchia.
4. Data Communications and Networking, by Behrouz A Forouzan.
5. Computer Networking: A Top- Down Approach, by James F.Kurose.
6. Operating System Concepts, by Abraham Silberschatz.
7. R. Agrawal and J. Kiernan. Watermarking relational databases.In VLDB '02: Proceedings of the 28th international conference on VeryLarge Data Bases, pages155–166. VLDB Endowment, 2002.