ABSTRACT:

Privacy is one of the major concerns when publishing or sharing social network data for social science research and business analysis. Recently, researchers have developed privacy models similar to k-anonymity to prevent node reidentification through structure information. However, even when these privacy models are enforced, an attacker may still be able to infer one’s private information if a group of nodes largely share the same sensitive labels (i.e., attributes). In other words, the label-node relationship is not well protected by pure structure anonymization methods. Furthermore, existing approaches, which rely on edge editing or node clustering, may significantly alter key graph properties. In this paper, we define a $k$-degree-$l$-diversity anonymity model that considers the protection of structural information as well as sensitive labels of individuals. We further propose a novel anonymization methodology based on adding noise nodes. We develop a new algorithm by adding noise nodes into the original graph with the consideration of introducing the least distortion to graph properties. Most importantly, we provide a rigorous analysis of the theoretical bounds on the number of noise nodes added and their impacts on an important graph property. We conduct extensive experiments to evaluate the effectiveness of the proposed technique.
EXISTING SYSTEM:

Recently, much work has been done on anonymizing tabular microdata. A variety of privacy models as well as anonymization algorithms have been developed (e.g., k-anonymity, l-diversity, t-closeness). In tabular microdata, some of the nonsensitive attributes, called quasi identifiers, can be used to reidentify individuals and their sensitive attributes. When publishing social network data, graph structures are also published with corresponding social relationships. As a result, it may be exploited as a new means to compromise privacy.

DISADVANTAGES OF EXISTING SYSTEM:

- The edge-editing method sometimes may change the distance properties substantially by connecting two faraway nodes together or deleting the bridge link between two communities.
- Mining over these data might get the wrong conclusion about how the salaries are distributed in the society. Therefore, solely relying on edge editing may not be a good solution to preserve data utility.
PROPOSED SYSTEM:

We propose a novel idea to preserve important graph properties, such as distances between nodes by adding certain “noise” nodes into a graph. This idea is based on the following key observation.

In our proposed system, privacy preserving goal is to prevent an attacker from reidentifying a user and finding the fact that a certain user has a specific sensitive value. To achieve this goal, we define a $k$-degree-$l$-diversity (KDLD) model for safely publishing a labeled graph, and then develop corresponding graph anonymization algorithms with the least distortion to the properties of the original graph, such as degrees and distances between nodes.

ADVANTAGES OF PROPOSED SYSTEM:

- We combine $k$-degree anonymity with $l$-diversity to prevent not only the reidentification of individual nodes but also the revelation of a sensitive attribute associated with each node.
- We propose a novel graph construction technique which makes use of noise nodes to preserve utilities of the original graph. Two key properties are
considered: 1) Add as few noise edges as possible; 2) Change the distance between nodes as less as possible.

- We present analytical results to show the relationship between the number of noise nodes added and their impacts on an important graph property.

**SYSTEM ARCHITECTURE:**

**MODULES:**
- User Pane
- User Relationships
**MODULES DESCRIPTION:**

**User Pane**

User Pane is a block of information about a given user, like those typically found on a forum post, but can be used in other places as well. From core, it collects the user picture, name, join date, online status, contact link, and profile information. In addition, any module or theme can feed it more information via the preprocess system. All of this information is then gathered and displayed using a template file.

**User Relationships**

In this module we develop User Relationship module. Allows users to create named relationships between each other. It is the basic building block for a social networking site, or any site where users are aware of one another, and communicate.
Content Access

This module allows you to manage permissions for content types by role and author. It allows you to specify custom view, edit and delete permissions for each content type. Optionally you can enable per content access settings, so you can customize the access for each content node.

Protection of structural information

Our privacy preserving goal is to prevent an attacker from re-identifying a user and finding the fact that a certain user has a specific sensitive value.

SYSTEM CONFIGURATION:-

HARDWARE CONFIGURATION:-

✓ Processor - Pentium –IV
✓ Speed - 1.1 Ghz
✓ RAM - 256 MB(min)
✓ Hard Disk - 20 GB
✓ Key Board - Standard Windows Keyboard
✓ Mouse - Two or Three Button Mouse
SOFTWARE CONFIGURATION:-

- Operating System : Windows XP
- Programming Language : JAVA/J2EE
- Database : MYSQL
- Java Version : JDK 1.6 & above.
- IDE : Netbeans 7.2.1