**Collusion Defender: Preserving Subscribers’ Privacy in Publish and Subscribe Systems**

**Abstract:**

 The Publish and Subscribe (pub/sub) system is an established paradigm to disseminate the data from publishers to subscribers in a loosely coupled manner using a network of dedicated brokers. However, sensitive data could be exposed to malicious entities if brokers get compromised or hacked; or even worse, if brokers themselves are curious to learn about the data. A viable mechanism to protect sensitive publications and subscriptions is to encrypt the data before it is disseminated through the brokers. State-of-the-art approaches allow brokers to perform encrypted matching without revealing publications and subscriptions. However, if malicious brokers collude with malicious subscribers or publishers, they can learn the interests of innocent subscribers, even when the interests are encrypted. In this article, we present a pub/sub system that ensures conﬁdentiality of publications and subscriptions in the presence of untrusted brokers. Furthermore, our solution resists collusion attacks between untrusted brokers and malicious subscribers (or publishers). Finally, we have implemented a prototype of our solution to show its feasibility and efﬁciency.

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 1 GB

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows XP/UBUNTU.
* Implementation : NS2
* NS2 Version : 2.28
* Front End : OTCL (Object Oriented Tool Command  Language)
* Tool : Cygwin (To simulate in Windows OS)