INTRODUCTION:

Internet security problems are still a big challenge as there are many security events occurred, such as Internet worms, Spam and phishing attacks etc. Botnet, a well-organized distributed network attack, consists of a large volume of bots, which generates huge volumes of spam or launching Distributed Denial-of-Service (DDoS) attacks to victim hosts. This new emerging botnet attack makes Internet security status even worse. To address these problems, a practical Collaborative Network Security Management System is proposed with well deployed collaborative UTM (Unified Threat Management) and traffic probers. Such distributed security overlay network with a centralized Security Center leverage Peer-to-Peer communication protocol used in UTM’s collaborative module and virtually interconnect them to exchange Network events and security rules. Also security functions for UTM are retro fitted to share security rules.

OBJECTIVES:

The main objective of our work is to provide that a practical solution to collect data trace and analyze these data in parallel in a Cloud Computing platform. We propose to use cloud storage to keep huge traffic data and processing it with cloud computing platform to find the malicious attacks. As we already operate Collaborative Network Security Management System which has big data output. A workable case, phishing attack forensic analysis is presented and the required computing and storage resource are investigated. We have concluded that this phishing filter functions can be effectively scale to analyze a large volume of trace data for phishing attack detection with Cloud computing. The results also show that this solution is economical for large scale forensic analysis for traffic.
METHODOLOGY:

Collaborative network security management system (CNSMS) deployed in multisite is shown in below figure. During the system operating the collaborative mechanism runs as we accepted to share security events and rules set and new rules set are enforced on demands as instructed by security center. Operating reports from each NetSecu node and prober been collected and send back to security center.

MODULE DESCRIPTION:

1. Traffic prober.
2. Collaborative UTM.
4. Forensic analysis for fishing attack.

1. COLLABORATION DIAGRAM

![Collaboration Diagram]

2. ARCHITECTURE DIAGRAM

![Architecture Diagram]

Fig1. The deployment of Collaborative Network Security Management System in Multisite
RESULTS AND CONCLUSION:

The Collaborative Network Security Management System is very useful to counter measure distributed network attacks. Its operation resulted in big data outputs, such as network traffics, security events, etc. We use cloud computing systems to explore the large volume of collected data from CNSMS to track the attacking events. Traffic archiving is implemented in collaborative UTM to collect all the network trace data and the cloud computing technology is leveraged to analyze the experimental data in parallel. Phishing attack forensic analysis as a workable case is presented and the required computing and storage resource are also evaluated by using real trace data. All phishing filtering operation is cloud-based and operated in parallel, and the processing procedure is also evaluated. The results show that the proposed scheme is practical and can be generalized to forensic analysis of other network attacks in the future.

FUTURE ENHANCEMENTS:

From the end user’s point of view this work has explained whether the availability is preserved so that they can get an access to their own data. From the trusted third parties’ view, this work has explained whether they can gain the authority to get access to the evidence. And finally, for service providers’ point of view this work has summarized whether they able to guarantee the safety of the data.

The discussion above is basically on the security problems when digital forensics analysis is embedded into cloud computing environments. In the future, these security problems can be transferred as a solution in order to have a secured network. There must be some ways to have an improved security by migrating the cloud services. Three proposed ways are a progression of connectivity, the flat corporate network and the social engineering path. This may be one of the future works in the cloud computing field.