**Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud**

**ABSTRACT**

Cloud computing promises to significantly change the way we use computers and access and store our personal and business information. With these new computing and communications paradigms arise new data security challenges. Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider. We propose a different approach for securing data in the cloud using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions, we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user’s real data. Experiments conducted in a local file setting provide evidence that this approach may provide unprecedented levels of user data security in a Cloud environment.

**EXISTING SYSTEM**

Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider. Much research in Cloud computing security has focused on ways of preventing unauthorized and illegitimate access to data by developing sophisticated access control and encryption mechanisms. However these mechanisms have not been able to prevent data compromise.

**PROPOSED SYSTEM**

We propose a completely different approach to securing the cloud using decoy information technology, that we have come to call Fog computing. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data. The decoys, then, serve two purposes: (1) validating whether data access is authorized

when abnormal information access is detected, and (2) confusing the attacker with bogus information.

**MODULE DESCRIPTION**:

1.      **Cloud Computing.**

2.      **User Behavior Profiling:**

3.      **Decoy documents.**

**cloud computing**

                        Cloud computing is a model for enabling convenient, ondemand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction.    It divide into three type

1.Application as a service.

2.Infrastructure as a service.

3.Platform as a service.

                   Cloud computing exhibits the following key characteristics:

**1. Agility** improves with users' ability to re-provision technological infrastructure resources.

**2. Cost** is claimed to be reduced and in a public cloud delivery model [capital expenditure](http://en.wikipedia.org/wiki/Capital_expenditure) is converted to [operational expenditure](http://en.wikipedia.org/wiki/Operational_expenditure). This is purported to lower [barriers to entry](http://en.wikipedia.org/wiki/Barriers_to_entry), as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a [utility computing](http://en.wikipedia.org/wiki/Utility_computing) basis is fine-grained with usage-based options and fewer IT skills are required for implementation. The e-FISCAL project's state of the art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.

**3.**[**Virtualization**](http://en.wikipedia.org/wiki/Virtualization) technology allows servers and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another.

**4.**[**Multi tenancy**](http://en.wikipedia.org/wiki/Multitenancy) enables sharing of resources and costs across a large pool of users thus allowing for:

**5. Centralization** of infrastructure in locations with lower costs (such as real estate, electricity, etc.)

**6.      Utilization and efficiency** improvements for systems that are often only 10–20% utilized.

**7.**[**Reliability**](http://en.wikipedia.org/wiki/Reliability_(computer_networking)) is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for [business continuity](http://en.wikipedia.org/wiki/Business_continuity) and [disaster recovery](http://en.wikipedia.org/wiki/Disaster_recovery).

**8.**[**Performance**](http://en.wikipedia.org/wiki/Computer_performance) is monitored and consistent and loosely coupled architectures are constructed using [web services](http://en.wikipedia.org/wiki/Web_services) as the system interface.

**9.**[**Security**](http://en.wikipedia.org/wiki/Computer_security) could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security [audit logs](http://en.wikipedia.org/wiki/Audit_log) may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

**10.**[**Maintenance**](http://en.wikipedia.org/wiki/Software_maintenance) of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

**User Behavior Profiling:**

                    We monitor data access in the cloud and detect abnormal data access patterns User profiling is a well known Technique that can be applied here to model how, when, and how much a user accesses their information in the Cloud. Such ‘normal user’ behavior can be continuously checked to determine whether abnormal access to a user’s information is occurring. This method of behavior-based security is commonly used in fraud detection applications. Such profiles would naturally include volumetric information, how many documents are typically read and how often. We monitor for abnormal search behaviors that exhibit deviations from the user baseline the correlation of search behavior anomaly detection with trap-based decoy files should provide stronger evidence of malfeasance, and therefore improve a detector’s accuracy.

**Decoy documents.**

                            We propose a different approach for securing data in thecloud using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user’s real data. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data  the decoys, then, serve two purposes:

(1) Validating whether data access is authorized when abnormal information access is detected, and

(2) Confusing the attacker with bogus information..

**H/W System Configuration:-**

**Processor               -    Pentium –III**

Speed                                -    1.1 Ghz

RAM                                 -    256  MB(min)

Hard Disk                          -   20 GB

Floppy Drive                     -    1.44 MB

Key Board                         -    Standard Windows Keyboard

Mouse                                -    Two or Three Button Mouse

Monitor                              -    SVGA

**S/W System Configuration:-**

Operating System            :Windows95/98/2000/XP

Application  Server          :   Tomcat5.0/6.X

Front End                          :   HTML, Java, Jsp

 Scripts                                :   JavaScript.

Server side Script             :   Java Server Pages.

Database                            :   Mysql