Volume 3, Issue 9, September 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Securing the cloud using Decoy Information Technology to preventing them from distinguishing the Real Sensitive data from fake Worthless data

Etikala Aruna, Dr. Ch GVN Prasad, A. Malla Reddy

Hyderabad, A.P (INDIA)

Abstract: 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. Organizations use the Cloud in a variety of different service models (SaaS, PaaS, IaaS) and deployment models (Private, Public, Hybrid). There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.Cloud computing offers potential benefits including cost savings and improved business outcomes for Australian government agencies. However, there are a variety of information security risks that need to be carefully considered. Risks will vary depending on the sensitivity of the data to be stored or processed, and how the chosen cloud vendor (also referred to as a cloud service provider) has implemented their specific cloud services.

Key words: Data Security, Data locality, Data integrity, Data separation, Data access, Data confidentiality, Data breaches, Network Security, Authentication and authorization, Web application security, Identity management process

I. Introduction

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.

II. System Overview

2.1 Security Issues in Service Model:

Cloud computing having three delivery models through which services are delivered to end users. These models are SaaS, IaaS and PaaS which provide software, Infrastructure and platform assets to the users. They have different level of security requirements.

Security issues in SaaS:

Software as service is a model, where the software applications are hosted slightly by the service provider and available to users on request, over the internet. In SaaS, client data is available on the internet and may be visible to other users, it is the responsibility of provider to set proper security checks for data protection. This is the major security risk, which create a problem in secure data migration and storage. The following security measures should be counted in SaaS application improvement process such that Data Security, Data locality, Data integrity, Data separation, Data access, Data confidentiality, Data breaches, Network Security, Authentication and authorization, Web application security, Identity management process. The following are the basics issues through which malicious user get access and violate the data

security, store at the SaaS dealer such that Cross-site scripting, SQL Injection flaw, Cross-site request forgery, Insecure storage, Insecure configuration.

Security issues in PaaS

PaaS is the layer above the IaaS. It deals with operating system, middleware, etc. It provides set of service through which a developer can complete a development process from testing to maintenance. It is complete platform where user can complete development task without any hesitation.

In PaaS, the service provider give some command to customer over some application on platform. But still there can be the problem of security like intrusion etc, which must be assured that data may not be accessible between applications.

Security issues in IaaS

IaaS introduce the traditional concept of development, spending a huge amount on data centers or managing hosting forum and hiring a staff for operation. Now the IaaS give an idea to use the infrastructure of any one provider, get services and pay only for resources they use. IaaS and other related services have enable set up and focus on business improvement without worrying about the organization infrastructure.

The IaaS provides basic security firewall, load balancing, etc. In IaaS there is better control over the security, and there is no security gap in virtualization manager. The main security problem in IaaS is the trustworthiness of data that is stored within the provider's hardware.

2.2Cloud Computing Security Threats and solution

Top Seven Security Threats

Top seven security threats to cloud computing discovered by "Cloud Security Alliance" (CSA) are: i. Abuse and Nefarious Use of Cloud Computing.

Abuse and nefarious use of cloud computing is the top threat identified by the CSA. A simple example of this is the use of botnets to spread spam and malware. Attackers can infiltrate a public cloud, for example, and find a way to upload malware to thousands of computers and use the power of the cloud infrastructure to attack other machines.

Suggested remedies by the CSA to lessen this threat:

• Stricter initial registration and validation processes.
• Enhanced credit card fraud monitoring and coordination.
• Comprehensive introspection of customer network traffic.
• Monitoring public blacklists for one's own network blocks.

ii. Insecure Application Programming Interfaces.

As software interfaces or APIs are what customers use to interact with cloud services, those must have extremely secure authentication, access control, encryption and activity monitoring mechanisms - especially when third parties start to build on them.

Suggested remedies by CSA to lessen this threat:

• Analyze the security model of cloud provider interfaces.
• Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
• Understand the dependency chain associated with the API.

iii. Malicious Insiders.

The malicious insider threat is one that gains in importance as many providers still don't reveal how they hire people, how they grant them access to assets or how they monitor them. Transparency is, in this case, vital to a secure cloud offering, along with compliance reporting and breach notification.

Suggested remedies by CSA to lessen this threat:

• Enforce strict supply chain management and conduct a comprehensive supplier assessment.
• Specify human resource requirements as part of legal contracts.
• Require transparency into overall information security and management practices, as well as compliance reporting.
• Determine security breach notification processes.

iv. Shared Technology Vulnerabilities.

Sharing infrastructure is a way of life for IaaS providers. Unfortunately, the components on which this infrastructure is based were not designed for that. To ensure that customers don't thread on each other's "territory", monitoring and strong compartmentalization is required.

Suggested remedies by CSA to lessen this threat:

• Implement security best practices for installation/configuration.
•Monitor environment for unauthorized changes/activity.
• Promote strong authentication and access control for administrative access and operations.
• Enforce service level agreements for patching and vulnerability remediation.
• Conduct vulnerability scanning and configuration audits.

v. Data Loss/Leakage.

Be it by deletion without a backup, by loss of the encoding key or by unauthorized access, data is always in danger of being lost or stolen. This is one of the top concerns for businesses, because they not only stand to lose their reputation, but are also obligated by law to keep it safe.

Suggested remedies by CSA to lessen this threat:
•Implement strong API access control.
• Encrypt and protect integrity of data in transit.
• Analyze data protection at both design and run time.
• Implement strong key generation, storage and management, and destruction practices.
• Contractually demand providers to wipe persistent media before it is released into the pool.
• Contractually specify provider backup and retention strategies.

vi. Account, Service & Traffic Hijacking.

Account service and traffic hijacking is another issue that cloud users need to be aware of. These threats range from man-in-the-middle attacks, to phishing and spam campaigns, to denial-of service attacks.
Suggested remedies by CSA to lessen this threat:
• Prohibit the sharing of account credentials between users and services.
•Leverage strong two-factor authentication techniques where possible.
• Employ proactive monitoring to detect unauthorized activity.
• Understand cloud provider security policies and SLAs.

vii. Unknown Risk Profile.

Security should be always in the upper portion of the priority list. Code updates, security practices, vulnerability profiles, intrusion attempts – all things that should always be kept in mind ,Suggested remedies by CSA to lessen this threat:
• Disclosure of applicable logs and data.
•Partial/full disclosure of infrastructure details (*e.g.*, patch levels, firewalls, etc.).
•Monitoring and alerting on necessary information.

III. System Analyses

MODULE DESCRIPTION:

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 is converted to operational expenditure. This is purported to lower 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 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 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 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 is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
8. Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
9. 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 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 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.

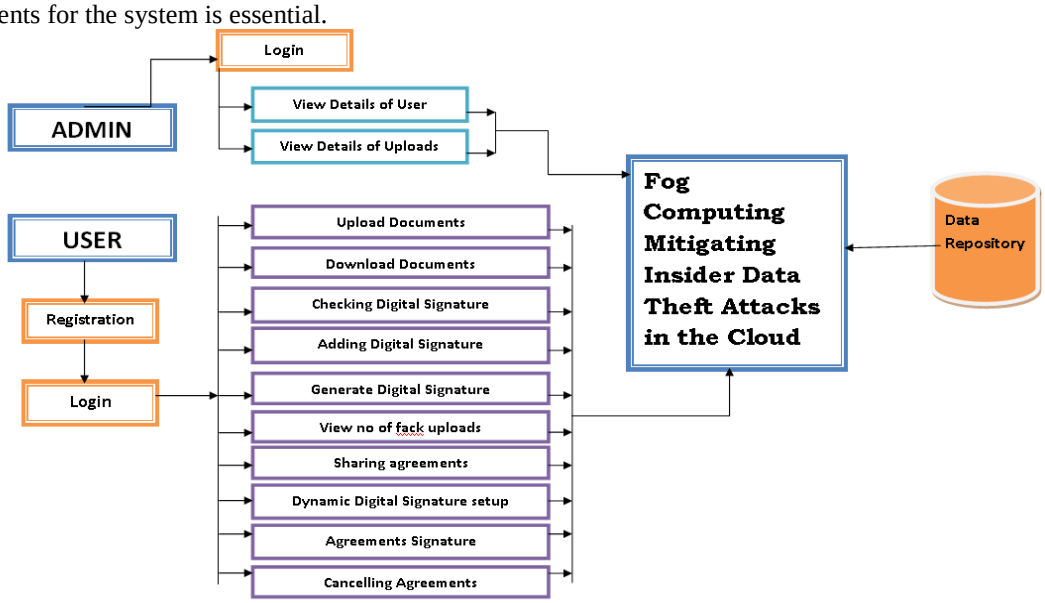
Decoy documents:

We propose a different approach for securing data in the cloud 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

IV. Feasibility Report

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.



System Architecture:

V. Sample Code

Creating Edit form

Include the following code in a JSP page (editjsdata.jsp) this is for my example

```
<%
        // creating local variables
    String email= request.getParameter("email");
    // connecting with DB
    java.sql.Connection mycon=DB.MyDBBean.getDataBaseConnection();
    // preparing SQL java string version
    String q="select * from jsdata where email=' "+email+" ' ";
    // creating Statement OBject
    java.sql.Statement stmt=mycon.createStatement();
    // invoking executeQuery() ---------  ResultSet Object
    java.sql.ResultSet rs= stmt.executeQuery(q);
    // rs contains list of rows returned by your sql query
    String tname=null, tphn=null, tqual=null;
    if(rs.next())
```



```
                {
                 tname=rs.getString(2);
          tphn=rs.getString(4);
          tqual=rs.getString(5);
       %>
<form action="EditJsActionServlet" method="POST">
       <table border="0">
          <tbody>
             <tr>
                <td>Your email is :</td>
                <td>
                   <%=email%>
                   <input type="hidden" name="email" value="<%=email%>">
                </td>              </tr>              <tr>                 <td>Your Name is :</td>
                <td>
                   <input type="text" name="n" value="<%=tname%>" />
                </td>                                 </tr>              <tr>
                <td>Your Phone Number is :</td>                 <td><input type="text" name="phn" value="<%=tphn%>"
/></td>              </tr>
             <tr>                 <td>Your Qualification is</td>
                <td><input type="text" name="q" value="<%=tqual%>" /></td>
             </tr>              <tr>                 <td><input type="submit" value="Edit MY Data" /></td>
                <td></td>              </tr>
          </tbody>       </table>
        </form>
       }       else
                {
       %>
       <h1>Email id is not available</h1>
       <%
       }%>
```

Edit Action Logic

This is a servlet code for edit your data

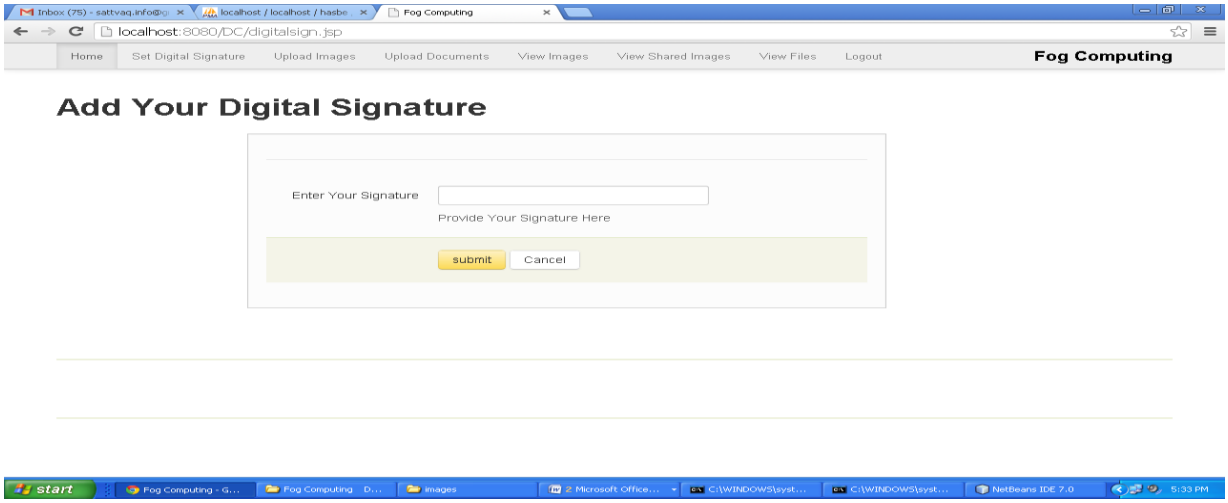
```
try {
                          // creating local variable
          String e=null, n=null, p=null,q=null;
            e= request.getParameter("e");
             n= request.getParameter("n");
               p= request.getParameter("p");
                 q= request.getParameter("q");
                          // creating Connection Object
                 java.sql.Connection mycon= DB.MyDBBean.getDataBaseConnection();
                 // creating SQL query -- Update for 3 with where for email
                                   String q1="update jsdata set name='"+n+"',phone='"+p+"',qualification='"+q+"' where
email='"+e+"'";
                          // creating STMT Object
                 java.sql.Statement stmt= mycon.createStatement();
                          // invoking executeUpdate() int

                 int i= stmt.executeUpdate(q1);
                                  if(i>0)                          {
                 // RD
                                  javax.servlet.RequestDispatcher rd= request.getRequestDispatcher("viewalljsdetails.jsp");

                    rd.forward(request, response);
                          }               else
                 {
javax.servlet.RequestDispatcher rd= request.getRequestDispatcher("viewalljsdetails.jsp");
                                  rd.forward(request, response);
```

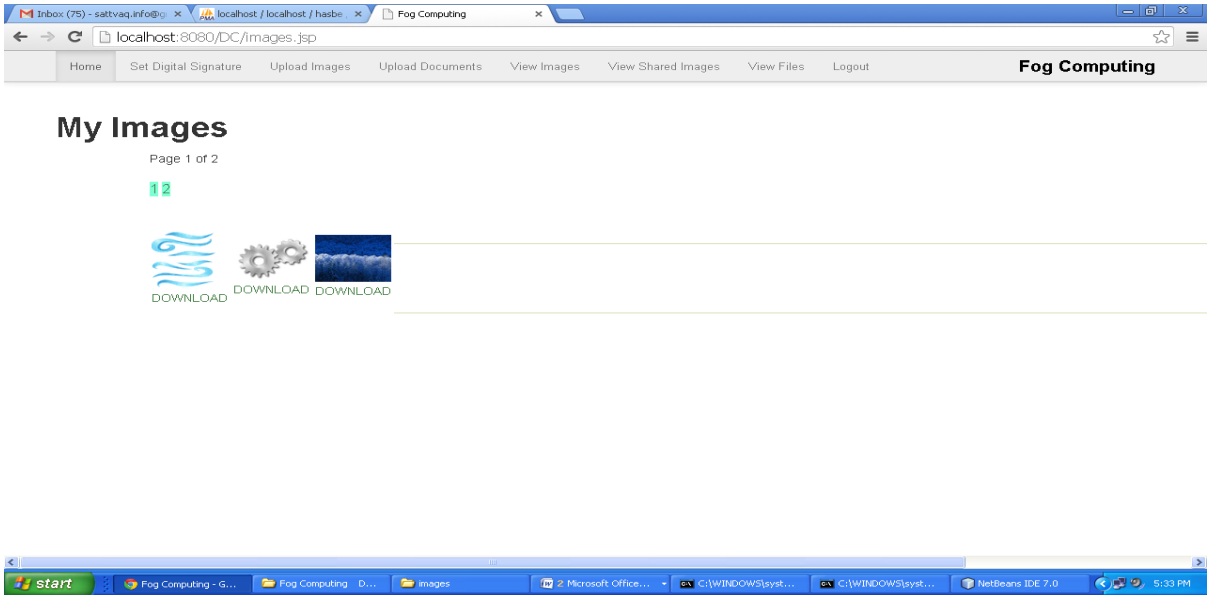


```
                    }
} catch (Exception e) {
                out.print(e);
    }
```

VI. System Implementation Screen Shots:

Screen shots:





VII. System Testing

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

Invalid Input : identified classes of invalid input must be rejected.

Functions : identified functions must be exercised.
Output : identified classes of application outputs must be exercised.
Systems/Procedures: interfacing systems or procedures must be invoked.
Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.
System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

VIII. Conclusion & Future Enhancements

In this paper documents stored in the Cloud alongside the user's real data also serve as sensors to detect illegitimate access. Once unauthorized data access or exposure is suspected, and later verified, with challenge questions for instance, we inundate the malicious insider with bogus information in order to dilute the user's real data. Such preventive attacks that rely on disinformation technology, could provide unprecedented levels of security in the Cloud and in social networks.

FutureEnhancements:

As we done in our proposed system, this security model can applicable only for a single cloud ownership system. If the cloud owner has a more than one clouds to operate then this proposed system can't pplicable for providing security, therefore in the future enhancement we can enhance our application to manage a cloud environment which has more then one cloud architecture.Cloud computing is the future for organizations. The considerable benefits that provide will make eventually all the organizations artially or totally move their processes and data to the Cloud. A lot of effort will be put in return to provision the appropriate security to make business on cloud environments. Although virtualization is already established, virtualization in the Cloud is still an immature area. The focus of future works should aim to harden the security of virtualization in multi-tenant environments. Possible lines of research are the development of reliable and efficient virtual network securities to monitor the communications between virtual machines in the same physical host. To achieve secure virtualized environments, isolation between the different tenants is needed. Future researches should aim to provide new architectures and techniques to harden the different resources shared between tenants.

The hypervisor is the most critical component of virtualized environments. If compromised, the host and guest OSs could potentially be compromised too. Hypervisor architectures that aim to minimize the code and, at the same time, maintain the functionalities, provide an interesting future research to secure virtualized environments and the Cloud, especially to prevent against future hypervisor root kits.

References

[1] Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March 2010. [Online]. Available:https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
[2] M. Arrington, "In our inbox: Hundreds of confidential twitter documents," July 2009. [Online]. Available: http://techcrunch.com/2009/07/14/in-our-inbox-hundreds-ofconfidential- twitter-documents/
[3] D. Takahashi, "French hacker who leaked Twitter documents o TechCrunch is busted," March 2010. [Online]. Available: http://venturebeat.com/2010/03/24/french-hacker-wholeaked- twitter-documents-to-techcrunch-is-busted/
[4] D. Danchev, "ZDNET: french hacker gains access to twitter's admin panel," April 2009. [Online]. Available: http://www.zdnet.com/blog/security/french-hacker-gains-access-totwitters- admin-panel/3292
[5] P. Allen, "Obama's Twitter password revealed after french hacker arrested for breaking into U.S. president's account," March 2010. [Online]. Available: http://www.dailymail.co.uk/news/article-1260488/Barack- Obamas-Twitter-password-revealed-French-hacker-arrested.html
[6] F. Rocha and M. Correia, "Lucy in the sky without diamonds: Stealing confidential data in the cloud," in Proceedings of the First International Workshop on Dependability of Clouds, Data Centers and Virtual Computing Environments, Hong Kong, ser. DCDV '11, June 2011.
[7] M. Van Dijk and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing," in Proceedings of the 5th USENIX conference on Hot topics in security, ser. HotSec'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 1–8. [Online]. Available: http://dl.acm.org/citation.cfm?id=1924931.1924934
[8] J. Pepitone, "Dropbox's password nightmare highlights cloud risks," June 2011.
[9] M. Ben-Salem and S. J. Stolfo, "Modeling user search-behavior for masquerade detection," in Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection. Heidelberg: Springer, September 2011, pp. 1–20.
[10] B. M. Bowen and S. Hershkop, "Decoy Document Distributor: http://sneakers.cs.columbia.edu/ids/fog/," 2009. [Online]. Available: http://sneakers.cs.columbia.edu/ids/FOG/.

Authors:

Mrs. Etikala Aruna, , Education Details: B.Tech-- IT(Information Technology) 2004-2008,JNTUH University. Experience Details: Worked As Process Associate In Six Sigma Technologies, West Marred Ally, Feb,2009-Nov,2011.Studying M.Tech-- CSE(Computer Science And Engineering)2011-2013, Sri Indoor College Of Engineering And Technology, JNTUH University. Aruna.etikalas@gmail.com

Mr. Dr. Ch GVN Prasad , M.Tech,Ph.D(Experience-- 20 years ; 12 years IT industry (8 years in National Informatics Centre, Govt. of India, as Scientist and Software Analyst in AT&T in US)and 11 years Teaching as Professor and HOD of CSE dept). He Is Currently Working As Professor In Department Of Computer Science & Engineering In Sri Indu College of Engg & Tech.
prasadch2042@gmail.com

Mr. A. Malla Reddy , M.Tech(Ph.D) India,(Experience-- 5 years). He Is Currently Working As Associate Professor In Department Of Computer Science & Engineering In Sri Indu College of Engg & Tech. mallareddyadudhodla@gmail.com

