Intelligence based Defense System to Protect from Advanced Persistent Threat by means of Social Engineering on Social Cloud Platform

J. Vijaya Chandra¹, Narasimham Challa² and Sai Kiran Pasupuleti³

¹Department of CSE, KL University, Guntur - 522002, Andhra Pradesh, India
²Department of CSE, Sri Sivani College of Engineering, Chilakapalem, Andra Pradesh, India
³Department of CSE, KL University, Guntur - 522002, Andra Pradesh, India; vijayachandra.phd@gmail.com, narasimham_c@yahoo.com, psaikiran@kluniversity.in

Abstract

Advanced Persistent Threat is a specific design to survive until it reaches the target and creates backdoor for future Intrusion. The objective of this paper is, to design and implementation of a defense in depth system to protect social cloud against risks, threats and attacks. In this paper we discussed the policies and procedures of vulnerability management and intrusion detection system. We also focused on the steps involved in defense in depth system a layered architecture for prevention and protection from malicious users, masquerader and intruders. Where each layer restricts the intruder with deployed activities such as security monitoring, malicious site filtering, patches to remedy vulnerabilities, analysis of audit log files, Intrusion detection and prevention system and storage media management for protecting the cloud from advanced persistent threat. The different intrusion techniques using social engineering methods such as spear phishing or whale phishing are also discussed. A mathematical approach is given to secure the cloud computing using computational intelligence which is aimed to defense the attacks using Perron-Frobenius theorem and methods for public social network. In this paper we focused on the Defense in Depth model for a security layered strategy. We also discussed on the issues an audit communication or challenge to the cloud server data security. Defense System is the process of monitoring for and identifying unauthorized system access or manipulation and protecting the data from intruders. A clear description is given regarding the steps involved in the Advanced Persistent Attack and the measures or steps involved in Advanced Persistent Attack Defense System. The impact of security and privacy on cloud performance is calculated using cloud-sim tool, which supports simulating and modeling a large scale cloud infrastructure. An Experiment on intelligence based defense system using cloud analyst and simulator is given along with the result and conclusion.

Keywords: Advanced Persistent Attack, Cloud Computing, Cloud Security, Cloud Server, Defense in Depth, Defense System, Vulnerability

1. Introduction

One of the major characteristics and behavior of APT (Advanced Persistent Threat) is not to get caught, being stealthy and persistent nature. The major task is to protect cloud against the APT, using intelligence based defense system, to design and implement defense in depth system against the APT, and one should understand diversification of various types of viruses, exploitation of zero-day vulnerabilities and whale phishing attacks.

Phishing attempts focused at specific individuals or companies. These are targeted to collect information and resources desired to meet a specific collection requirement for monetary or espionage purposes. Water hole attack is a social engineering technique that is to victim an organization by observing the official websites for information gathering. Social engineering is a psychological tricks used by intruder to obtain sensitive information to access to system. It is the technique where an intruder uses brain more than the tools to obtain critical information from...
Intelligence based Defense System to Protect from Advanced Persistent Threat by means of Social Engineering on Social Cloud Platform

victims’ ignorance or lack of knowledge. Social cloud is a model as the resources are owned, provided and consumed by members of a social community. It needs to traverse network address translations which can handle non-static IP addresses and makes dynamic user management. Cloud based Social Networking is an application specific portal based on authentication and user experience which utilizes the web and storage services.

Security is the major factor in system functionality which approaches the functionality in terms of security controls. The risk is a function of threat that exploits vulnerabilities and in-light of counter measures we apply to protect our social cloud platform. Advanced Persistent Threats are stealthy, cautious, conscious, targeted and data focused which are quite different from general risks, threats and attacks. Uses social engineering methods are used to gather information about the target and sustains for a long period of time. Defense in Depth system is onion layer security architecture uses different tools that are categorized as host-based tools, network based tools, and data storage and retrieve tools to improve security postures.

Security Threats of Cloud Computing are increasing day by day due to the intruders who exploit the vulnerabilities of cloud architecture. Cloud Environment consists of computing resources in the form of virtual machines or instances, where multiple types of instances with different capabilities such as CPU speed, RAM size, I/O speed and network bandwidth to satisfy different application demands. The applications are automatically compose, configure and deploy in a cloud platform, where the deployment requirements of a web applications provided by the service provider, which includes security devices such as firewalls, load balancers, web servers, application servers, database servers and storage devices.

Intelligence based cloud security is an art of making computers to do smart things which parallels the remarkable ability of the human mind to reason and learn in an environment of uncertainty and imprecision which consists of several computing paradigms including neutral networks, fuzzy-set theory, appropriate reasoning and derivative free optimization methods. It is a knowledge based system

The Onion model of security is a layered strategy, where more layers of controls that are placed, to increase the amount of work required for an attacker to break down the defenses and reduce the risk of un-intended failure of technology. To defend the stealth virus and malicious attacks a pack of monitoring tools are used and implemented as an auto-executable file where the virtual scanning environment is created. A secured cloud can not only reduce the costs, it improves the speed access for resource sharing. Risk Management System should be control the internal security control environment that provides protection of consumer assets from unauthorized access by Intelligence based automatic system. The counter measures for the Advanced Persistent Threat is network monitoring, email protection, protection against the spread of malware, system and network configuration protection, spam filtering and other security awareness defense system methods. Advanced Persistent Attack is constantly changing attack procedure or technique and methods used to target and exploit an organization. Advanced Protection system refers to monitoring whether some unauthorized entity has attempted to gain access or has gained access to a protection system.

2. Related Work

Security management is the process of which security controls are implemented and security managers are subject to control.

1. Establish controls, classify data and determine which controls apply, assign responsibilities
2. Implement Controls
   • Block and scan E-mail file attachments
   • Lock Down application before a file is downloaded and it should be scanned perfectly to stop APT
   • Continuous monitoring of cloud using vulnerability testing tools
   • Periodic testing and scanning to control APT
3. Check and Assess whether controls are correctly implemented, applied and report results to stakeholders
4. Perform preventive and corrective actions appropriate.

Defense in depth is the security approach layered on other as known as onion model of security most commonly adopted in cloud computing. Where each layer is deployed with some activity such as Security Event Monitoring, Network Security System, Data Loss Prevention and Recovery System, Forensics Analysis, Email Security, Web Security, Intrusion Detection and Prevention System, Protection system from Risks, Threats.
and Attacks. A fundamental duty of intrusion detection is audit records, i.e., records of ongoing activities of the users that form a vital input for intrusion detection. But there will be some overlaps between the behavior of legitimate users and intruders. Cloud security concerns with anti-virus, identity management, access management and data loss prevention.

Authentication is a primary security service; the most common used procedure is verification of username and password, it is the processes of verifying who you are? Is that you say who you are? And Authorization is the processes of giving boundaries that is how much you can be accessed. Auditing consists of examination based on previous history in order to determine whether security violations took place. Audit data is recorded in audit log files, continuous monitoring and auditing procedures should be followed based on intelligence system.

Intrusion detection system is used to detect the outside attacks; it is a monitoring system that monitors network or system activities to identify malicious activities or policy violations and produces reports to a management station. IDS are in two types they are Network Intrusion Detection System and Host Based Intrusion Detection System. Intrusion Detection and Prevention System is primarily focuses on the identifying risks, threats and attacks, audits log records information, violated security policies are determined and prevents network based, host based, wireless and data storage risks, threats and attacks. Detections are Signature based, anomaly based and stateful protocol analysis. Where in Signature based, which compares known threat signatures to observed events to identify malwares. Anomaly based, which compares definitions of what activity is considered normal against observed events to identify significant deviations. Stateful protocol analysis, which compares predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations.

Security model in cloud computing is of CIA Triad, that is Confidentiality, Integrity and Availability. Confidentiality is the privacy policy of cloud computing so that data at transit or rest ensures confidentiality of data by preventing the unauthorized disclosure. Integrity is described as maintaining a software system in a predefined legitimate state. It addresses validating of the data origin, it detects the alteration of data and it determines whether the data origin has changed. Availability is concerned policy with denying illegitimate access to cloud computing resources and preventing external risks, threats and attacks.

### 3. Advanced Persistent Threat

Persistent is specially designed to serve long time, it stealth itself that means it kills-itself to hide from anti-virus or scanners and regenerate until goal reached. Attacks are unauthorized activities with malicious intent using specially crafted code or techniques.

Threats are classified into 6 steps they are

#### 3.1 Reconnaissance

Gathering of information about the target, looking for Specific areas that can be focused on to achieve long-term compromise with the minimal amount of energy or effort. This usually involves finding an individual that can be targeted to be used in intrusion.

#### 3.2 Intrusion

Determining and finding some way to the organization to establish a foothold. This usually does not require exploitation and is most commonly achieved by convincing a user to open an attachment or click on a link they are not supposed to open.

#### 3.3 Whale Phishing

It is a Technique of an attacker, most probably uses an e-mail that appears to be from a well-known individual or a multi-national company offering a job or a business mail which seems to be related to you. It is from a criminal who wants to theft bank credit card details and other financial information. It is also for the company confidential information where you are working.

#### 3.4 Exploitation

Intruder steals and extracts the critical information off the cloud in a stealthy way. At this stage the intruder establishes persistence and total control of the cloud. This is usually done by installing customized tools to create a complete command and control communication in the cloud.

#### 3.5 Back Door

Establishment of backdoor ultimately what the APT wants to be able to communicate with the network they are targeted. After initial intrusion has been accomplished
a remote way in is established so the attacker can continue to move around the compromised cloud network.

3.6 Command and Control
An attacker wants to own the entire network and maintain for a long term access for both current and future use. This usually requires obtaining, cracking or hijacking admin, and privileged credentials. Advanced Persistent Threat is majorly classified into 6 types they are as follows

1. Infected with a virus by browsing a website
2. Targeted e-mail attack
3. Induction via downloaded files
4. Infected with virus via a medium (USB Stick)
5. Distributed Denial of Service attack and other Advanced Attacks.

Common features of Advanced Persistent Attack
1. Identifies HTTP protocol or other communication protocols or ports that are used by the target organization, and performs back door communications.
2. Spreads Infection within the compromised system that infects a network within an organization and then spreads infection to systems by exploiting vulnerabilities. Infects many more computers in the network so that it can more efficiently steal the information stored in the system.
3. Simultaneous updates and spread viruses in chores with the extended capability module downloaded from the command and control server. It spreads in the system with capability of carrying out an effective attack.
4. Information gathering, attack spreads to a closed system via a USB and spreads to the open system via social engineering methods and websites.

Advanced Persistent Threat is a hot and controversial term used among security professional, it is the combination of different threats such as zero-day threats, polymorphic threats and blended threats. A zero-day threat is a cyber-attack on an OS or application vulnerability that is the attack launches to the public awareness of the vulnerability from day zero. Polymorphic threat is that morphs – continuously changes and makes impossible to detect for traditional signature based security defenses to detect. A Blended threat employs multiple attack vectors it adopts stealthy procedures.

4. Defense System for Advanced Persistent Threat
Defense in depth is a protection procedure which challenges different attack methods through multi-layered such as application, data storage, web logic, network, logical and physical layered security architecture. Multi-layered defense like onion layer is more protected compared to single defense system. The concept of defense in depth originates from the military discipline. Defense in depth aims to stop or defend the intruders attack. In a computer network defense in depth not only intercepts intruder’s attacks on the network, but also provides time for a system auditor or administrator to identify the origin of problems and defends so that the chances of attackers invasion reduces and increases the attackers risk of detection, it also recovers the data losses and the success effects towards the protection of cloud data storage.

Defense in depth strategy continuously monitors the cloud and slows the attacker’s progress and provides the time to the defender but not totally provides security it acts as security barrier, it provides intrusion detection and protection system, virus protection and removal system, whale phishing detection and blocking system for secured electronic mails, malicious site filtering system for blocking malicious files download, vulnerability identification and patches to remedy, audit log analysis and finally USB-Media Management.

To protect the cloud computing environment from risks, threats and attacks, the security concerns are around the virtualization, it altered the relationship between operating system/software/application and hardware. Virtualization in cloud computing is minimizes risk by...
enhancing security through centralized IT management, easily update service packs and patches, easily restore servers/desktops. The virtual machine manager that manages the life cycle of virtual machines on a single node is called hypervisor. The new risk area is hypervisor itself; it is the prime target of intruder. All assets such as network, hardware and software should be managed; identity and access management is the primary security measure towards the cloud security that means right individuals should be accessed right resource at right time for right reason. Cloud computing security can be provided by using cryptographic techniques that is fully homomorphic encryption which is based on arbitrary processing. The data and information security can be provided to the confidential data to the cloud server by using cryptographic keys for encryption and decryption. Fully homomorphic encryption is implemented on a virtual platform as a Cloud server, a VPN network that links the Cloud with the customer, and then simulating using cloudsim tool. Security of cloud computing is based on onion layer security using fully homomorphic encryption concept of security which is to enable and provides confidentiality of data. Is concerned with protecting data at transit or at rest; also by preventing unauthorized disclosures and data losses. To secure clouds from malicious attacks malwares and stealth viruses a continuous layered base monitoring and defense system is developed using defense in depth for APT.

5. Mathematical Analysis

Let us consider the Social Network as a Graph, where \( G = (V, E) \) and a sub-graph \( H \) of \( G \) is a pair \( (W, F) \), where \( W \subseteq V \) and \( F \subseteq E \), and each edge in \( F \) has both endpoints in \( W \). We now define the following collection of sub-graphs \( B_k(G) \): We say that a sub-graph \( H \) of \( G \) belongs to \( B_k(G) \) if:

1. Each edge of \( H \) belongs to at least \( k \) distinct triangles in \( H \), and
2. Each node of \( H \) has at least one incident edge in \( H \). We observe that \( B(G) \) is a non-empty set, Since the Sub graph consisting of no nodes and no edges satisfies Conditions (i) and (ii) and hence belong to \( B_k(G) \).

The Graph of \( n \) vertices the maximum number of edges in any \( n \) vertex unordered and undirected graph with exactly \( n(n-1)/2 \) edges is a complete graph. A graph can be represented in a matrix form by using the adjacency matrix or the incidence matrix of the graph. Connectivity defines how nodes are connected in a sequence of edges in a graph.

Two nodes \( V_i \) and \( V_j \) are connected via an edge, therefore \( V_i \) is adjacent \( e(V_i, V_j) \). Two edges \( e_1(a,b) \) and \( e_2(c,d) \) are incident when they share one endpoint that is

\[
e_1(a,b) \text{ is incident to } e_2(c,d) \equiv (a = c) \lor (a = d) \lor (b = c) \lor (b = d)
\]

The Degree Centrality is the number of links incident upon a node that is the number of ties that a node has, Degree is often interpreted in terms of immediate risk of node for catching whatever is flowing through the network. If the network is directed, then we usually define two separate measures of degree centrality, namely in-degree and out-degree. In-degree is a count of the number of ties directed to the node, and out-degree is the number of ties that the node directs to others.

For a graph \( G := (V, E) \) with \( n \) vertices, the degree centrality \( CD(v) \) for vertex \( V \) is:

\[
CD(v) = \frac{\text{deg}(v)}{n - 1}
\]

Calculating degree for all nodes \( V \) is graph takes \( \theta \) \((V2) \) in a dense adjacency matrix representation of the graph, and for edges \( E \) in a graph takes \( \theta \)\((E) \) in a sparse matrix representation.

The definition of centrality can be extended to graphs. Let \( V^* \) be the node with highest degree centrality in \( G \). Let \( X := (Y, Z) \) be the \( n \) node connected graph that maximize the following quantity with \( y^* \) being the node with highest degree centrality in \( X \).

\[
H = \sum_{j=1}^{\mid V \mid} C_D(y^*) - C_D(y_j)
\]

Then the degree centrality of the graph \( G \) is defined as follows:

\[
C_D(G) = \frac{\sum_{j=1}^{\mid V \mid} [C_D(v^*) - C_D(v_j)]}{H}
\]

Where \( H \) is maximized when the graph \( X \) contains one node that is connected to all other nodes and all other nodes are connected only to this one central node (a star graph). In this case
Intelligence based Defense System to Protect from Advanced Persistent Threat by means of Social Engineering on Social Cloud Platform

\[ H = (n - 1) \left( 1 - \frac{1}{n-1} \right) = n - 2 \]

So the degree of centrality of G reduces to

\[ \sum_{i=1}^{[\nu]} [C_D(\nu^i) - C_D(\nu_i)] \]

\[ C_D(G) = n - 2 \]

A more sophisticated version of the same idea is that so called *Eigen vector centrality*. Where degree centrality gives a simple count of the number of connections a vertex has, Eigen vector centrality acknowledges that not all connections are equal. In general, connections to people who are themselves influential will lend a person more influence than connections to less influential people who are themselves influential will lend a person more influence than connections to less influential people. If we denote centrality of vertex i by \( x_i \) then we can allow for this effect for making \( x_i \) proportional to the average of centralities of i’s network neighbors.

\[ x_i = \frac{1}{\lambda} \sum_{j=1}^{n} A_{ij} x_j \]

Where \( \lambda \) is a constant. Defining the vector of centralities \( x = (x_1, x_2, \ldots) \), we can rewrite this equation in matrix form as

\[ \hat{\lambda} x = Ax \]

And hence we see that \( x \) in an Eigen vector of the adjacency matrix with eigen value \( \lambda \). Assuming that we wish the centralities to be non-negative, it can be shown using the Perron-Frobenius Theorem that \( \lambda \) must be the largest Eigen vector of the adjacency matrix and \( \lambda \) the corresponding Eigen vector. Let \( A \) be the irreducible non-negative \( m \times m \) matrix with period \( h \) and spectral radius \( \rho(A) = r \). Then the permutation matrix \( P \) such that

\[ PAP^{-1} = \begin{bmatrix}
0 & A_1 & 0 & 0 & \ldots & 0 \\
0 & 0 & A_2 & 0 & \ldots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & 0 & \ldots & A_{h-1} & 0 \\
A_h & 0 & 0 & \ldots & 0 & 0 \\
\end{bmatrix} \]

The blocks along the main diagonal are zero of square matrix. Where the Perron-Frobenius eigen value satisfies the in-equalities.

\[ \min_i \sum_j a_{ij} \leq r \leq \max_i \sum_j a_{ij} \]

All primitive matrices are non-negative matrix where \( a_{ij} \) are non-negative members and \( A \) said to be primitive, if for some integer \( m_0 \), \( A^{m_0} \) is a positive matrix that is \( a_{ij}^{(m_0)} \geq 0 \), where \( a_{ij}^{(m_0)} \) represents the \((i, j)\) the entry of \( A^{m_0} \)

\[ M = \begin{bmatrix}
0 & 1 & 0 & 0 & \ldots & 0 \\
0 & 0 & 1 & 0 & \ldots & 0 \\
0 & 0 & 0 & 1 & \ldots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & \ldots & \ldots & \ldots & \ldots & 1 \\
1 & 1 & 0 & 0 & \ldots & 0 \\
\end{bmatrix} \]

The Eigen vector centrality crops up in vast array of fields. Social community network structure use versions of Eigen vectors centrality and other methods to measure connection between players in social groups. Eigen vector centrality has been used to study social networks and Perron-Frobenius theorem is used to understand the concept of social networks and error detection and correction method.

### 6. Experimental Analysis to APT Defense System

CloudSim Tool Kit plays a great role in modeling and simulating cloud environment. Virtualization is capable of associating system/software and physical hardware on which it is running. It can be used at servers, storage, network and enables resource sharing and utilization. A Virtual Cloud Environment is modeled by using data center’s capabilities as a network of virtual services which includes hardware, database, user-interface and application logic, so that users are able to access and deploy applications from anywhere in the Internet driven by the demand and Quality of Service (QoS) requirements. Simulation tools open up the possibility of evaluating the practical assumption in a controlled environment where we can replicate results based on hypothesis. CloudSim has capabilities to do experimentation on risks, threats and attacks on cloud computing infrastructure and application services. It also provides capability to do experimentation on defense system to protect from attacks.

CloudSim supports virtual development of cloud application service models deployed within a Virtual Machine.
Modeling the Cloud consists of Cloud Information Service (CIS) is the first entity to be created, it is the registry, where the entire resources available are created, such as Data Centers, Hosts and Virtual Machines. The data center is created and register with the CIS, the properties of data centers are created and configured, and it models the core infrastructure level services, where the set of hosts are composed and responsible for managing Virtual Machines. A host has hardware configuration and particular bandwidth. It has pre-configured capability, memory storage and scheduling policy for allocating processing cores to virtual machines. The job of broker is to submit the task acts as intermediate between datacenter, cloud lets and CIS. Cloud Let models cloud based application services which are commonly deployed in data centers, every application has a pre-assigned instruction length, and speed is measured in Million Instruction Per Second (MIPS). Cloud Let Scheduler determines how the available CPU resources of virtual machines are divides among cloud lets. Two types of cloud based optimization polices are offered such as space-shared and time-shared. Virtual scheduler determines how processing cores of the host are allocated to virtual machines. Auditing is the process of registering all events related to access to the protected system resources in the system log. The auditing subsystem of contemporary operating system allows us to differentiate events of interest and monitoring tools provide the possibility of detecting and registering important security related events as a log files.

Steps involved in defense in depth and auditing the cloud for continuous monitoring to secured data storage are

1. Key Generation
2. Tag Generation
3. Data Integrity
4. Periodic Sampling Batch Audit
5. Audit for Dynamic Operations
6. Distributive Secured Data Storage

6.1 Key Generation

An Intelligence based system used to generate key KG that initialize the public and secret parameters by a pair of keys (pk, sk), where pk is verifying key is a public key and sk is signing key is private key. Signature Generation algorithm SG inputs a data file F and signing key sk that is SG(F, sk) and to generation proof algorithm GP run by the cloud server to generate proof of data storage correctness and verification proof algorithm VP is used to verify or audit the data storage, inputs data file F, a verifying key pk and SG. At the receiving end, verification is performed, it is either accepts or rejects. The receiver generates a quantity q that is a function of the public key components, the sender’s public key and the hash of the incoming message. If this quantity matches the r component of the signature, then the signature is validated. Data recovery is possible from data disasters by computing discrete logs such as to recover k from r, or x from s. It is also possible that nearly all the calculations are mod q and hence are much faster to recover and save at last step.

The structure of this function is such the receiver can recover r using the incoming message and signature, the public key of the user and the global public key. It is certainly not obvious that such a scheme would work.

1. Having received F and signature (r, s)
2. To verify a signature, recipient computers,
   \[ W = s - 1 \pmod{q}, \]
   \[ U_1 = (H(M).W) \pmod{q} \]
   \[ U_2 = (r \cdot w) \pmod{q}, \]
   \[ q = (gu_1 \cdot yu_2 \pmod{p}) \pmod{q} \]
3. If q = r then signature is verified.

6.2 Tag Generation

It is a technique used to produce an identity. It is a term associated with piece of information, where one party proves the identity of another party.

6.3 Data Integrity

When data is stored, it is often protected by access controls, and the server may also be physically protected. Sensitive data can be further protected by encrypting files where accuracy and consistency is maintained. The data stored in data ensures the integrity of data at transit or at storage, as it specify means to recover from detectable errors; it includes control policies and decisions.

6.4 Periodic Sampling Batch Audit

It allows multiple auditing tasks simultaneously, and reduces the computational cost due to aggregating multiple verifications at a time.

6.5 Audit for Dynamic Operations

In Cloud Computing the data may be updated frequently by the cloud users, hence the security and privacy is
possible only when the audit is done for the dynamic operations such as deletions, insertions and modifications, a continuous monitoring and dynamic auditing process is adopted in cloud for security. It secures a standardized, scalable, dynamic, virtualized and secure physical infrastructure with levels of redundancy to ensure high levels of availability with dynamic computing infrastructure.

### 6.6 Distributive Secured Data Storage

The Data Stored in data is secured by adopting distributive data storage all over the world; the data is stored in large data centers and server farms at multiple locations and linked via inter-networks providing distributed computing. The open and distributive service system of cloud computing became an attractive target to intruders. In cloud computing every component is available through internet, so there is high chances of security breaches that are the risks, threats, vulnerabilities and attacks by intruders and hackers. The Social networking becomes more popular, so cyber attackers using social media for identification of their target. Cloud storage enables users to store data remotely and retrieve on requirement of the cloud users.

### 7. Experimental Results and Discussion

The Experiment is done at i7 processor system with 8 Gb ram and 1Tb hard disk capacity using the cloud simulation by taking 10 sample data blocks, comparing on auditing time between batch auditing and the individual auditing with sample data comparison of server computing time and auditing computing time in microseconds. In the Experiment we consider the major factors such as time and space optimization techniques, with storage and communication. As the Cloud is pay as you use model, users have to pay both storage cost and bandwidth cost, frequently auditing increases the cost that is data transfer charge, at our comparisons it is found that when storage cost is optimized (reduced) the bandwidth cost is increased.

### 8. Conclusion and Future Work

The cloud security and privacy are the major factors using cryptography, which offers authentication of the genuine users and auditing for fully, ensure the cloud users the continuous and periodically check for data and information storage protection from vulnerabilities and unauthorized information leakage. Batch auditing provides more secure and high performance where multiple delegated auditing tasks from different users can be performed simultaneously by the auditor in data and privacy preserving manner. In this work, we proposed a batch auditing scheme to build a cloud storage service and for future work audit free data storage at cloud computing is proposed. The proposed feature makes compulsion invalid, and ensures secure cloud data sharing with a fine-grained access control mechanism. Our proposed scheme provides a possible way to fight against immoral interference such as intruders, masquerader, misfeasor and clandestine users with the right of privacy. We hope more schemes can be created to protect cloud user privacy. Vulnerability is one of the major problem due to insecure cryptography and un-safe data protection and portability that the cloud computing is facing. It is known that an external auditor is required to monitor continuously without knowing the data content in cloud storage, many storage nodes are filled with the security mile stones for auditing of data storage in cloud computing, more and more data security audit applications are developed in this secured cloud computing environment. The auditors devote most of their monitoring time in scalable public storage auditing for processing a large volume of data. So the Complexity of security and privacy are important to improve the performance of the Cloud storage.

### 9. References

1. Caton S, Haas C, Chark K, Bubendorfer K. Social Cloud: Cloud Computing in Social Networks. IEEE Transactions on Services Computing. 2014 Jul-Sep; 7(3):359–72.
2. Vijaya CJ, Narasimham C, Mohammed AH. Data and Information Storage Security from Advanced Persistent
3. Vijaya CJ, Narasimham C, Sai Kiran P, Thirupathi RK, Krishna RV. Numerical Formulation and Simulation of Social Networks using Graph Theory on Social Cloud Platform. Global Journal of Pure and Applied Mathematics. 2015; 11(2):1253–64.

4. Sood AK, Enbody RJ. Targeted Cyberattacks: A Superset of Advanced Persistent Threats. IEEE Security and Privacy. 2013 Jan-Feb; 11(1):54–61.

5. Jian L, Kun H, Hong R, Huimei W, Ming X. Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage. IEEE Transactions on Information Forensics and Security. 2015 Jul; 10(7):1513–28.

6. Lifei W, Haojin Z, Zhenfu C, Xiaolei D, Weiwei J, Yunlu C, Athanasios V. Security and privacy for storage and computation in cloud computing. Information Sciences. Elsevier. 2014 Feb 10; 258:371–86.

7. Leu FY, Tsai KL, Hsiao YT, Yang CT. An Internal Intrusion Detection and Protection System by using Data Mining and Forensic Techniques. IEEE Systems Journal. 2015 Apr 21; 99:1–2.

8. Manjusha R, Ramachandran R. Secure Authentication and Access System for Cloud Computing Auditing Services using Associated Digital Certificate. Indian Journal of Science and Technology. 2015 Apr; 8(57):220–7.

9. Vukalovic J, Delija D. Advanced Persistent Threats - detection and defense. 38th International Convention on Information and Communication Technology. Electronics and Microelectronics (MIPRO); 2015 May 25–29. p. 1324–30.

10. Skopik F, Friedberg I, Fiedler R. Dealing with advanced persistent threats in smart grid ICT networks. Proceedings of the Innovative Smart Grid Technologies Conference (ISGT)-2014; 2014 Feb 19-22. p. 1–5.

11. Mirza NAS, Abbas H, Khan FA, Al Muhtadi J. Anticipating Advanced Persistent Threat (APT) counter measures using collaborative security mechanisms. Proceedings of the International Symposium on Biometrics and Security Technologies (ISBAST)-2014; 2014 Aug 26-27. p. 129–32.

12. Shengjian L, Ping Z, Huyuan S. Research on Defense In-depth Model of Information Network Confrontation. Proceedings of the Fourth International Conference on Computational and Information Sciences (ICCIS)-2012; 2012 Aug 17-19. p. 267–70.

13. Groat S, Tront J, Marchany R. Advancing the defense in depth model. Proceedings of the International Conference on System of Systems Engineering (SoSE)-2012; 2012 Jul 16–9. p. 285–90.

14. Divyambika R, Umamakeswari A. Protection of Virtual Machines during Live Migration in Cloud Environment. Indian Journal of Science and Technology. May 2015; 8(59):333–9.

15. Buyyya R, Ranjan R, Calheiros RN. Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities. Proceedings of the 7 High Performance Computing and Simulation Conference (HPCS09). IEEE Computer Society; 2009 Jun.

16. Chi P-W, Lei C-L. Audit-Free Cloud Storage via Deniable Attribute-based Encryption,” IEEE Transactions on in Cloud Computing. 2015 Apr 21; 99:1–1.