International Journal of Computational Research and Development (IJCRD)
Impact Factor: 4.775, ISSN (Online): 2456 - 3137
(www.dvpublication.com) Volume 1, Issue 2, 2016

ENHANCED SECURITY MECHANISM AGAINST MALICIOUS ATTACKS FROM INTRUDERS IN CLOUDS

N. Abhishek*, M. Rakesh Chowdary & A. Yashwanth Reddy*****
Assistant Professor, Department of Computer Science and Engineering, Sree Dattha Group of Institutions, Hyderabad, Telangana

Cite This Article: N. Abhishek, M. Rakesh Chowdary & A. Yashwanth Reddy, "Enhanced Security Mechanism against Malicious Attacks from Intruders in Clouds", International Journal of Computational Research and Development, Volume 1, Issue 2, Page Number 148-151, 2016.

Abstract:
Cloud computing is architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce.som and Microsoft etc. Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability. Some logical and trial results prove the effectiveness of this new security infrastructure to safeguard mobile cloud services.

Key Words: Security Issues, Cloud Security, Cloud Architecture, Data Protection, Cloud Platform & Grid Computing

1. Introduction:

Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud service providers (CSP's) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. CSPs and ISPs (Internet Service Providers) both offer services. Cloud computing is a model that enables convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications that can be rapidly provisioned and released with minimal management effort or service provider's interaction. In general cloud providers offer three types of services i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). There are various reasons for organizations to move towards IT solutions that include cloud computing as they are just required to pay for the resources on consumption basis. In addition, organizations can easily meet the needs of rapidly changing markets to ensure that they are always on the leading edge for their consumers [1]. Cloud computing appeared as a business necessity, being animated by the idea of just using the infrastructure without managing it. Although initially this idea was present only in the academic area, recently, it was transposed into industry by companies like Microsoft, Amazon, Google, Yahoo! and Salesforce.com. This makes it possible for new startups to enter the market easier, since the cost of the infrastructure is greatly diminished. This allows developers to concentrate on the business value rather on the starting budget.

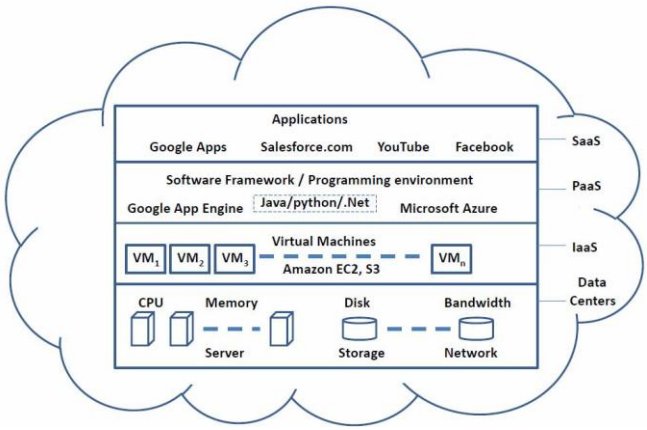

Figure 1: High Level View of Cloud Computing Architecture

The clients of commercial clouds rent computing power (virtual machines) or storage space (virtual space) dynamically, according to the needs of their business. With the exploit of this technology, users can access heavy applications via lightweight portable devices such as mobile phones, PCs and PDAs.

We propose a hierarchically designed security constructed. A trust chain is established between mobile devices, the cloudlet net, and remote cloud platforms. Predictive security analytics are processed at the backend cloud for virus signature scanning and update with automated malicious filtering and removal. We emphasize real-time filtering or removal of malicious attacks or fast response to intrusions with the help of trusted remote clouds.

2. Literature Survey:

The security of these questions has received limited formal scan, almost all of which pace smart-phone. Stuart Schechter and Cormack Harley deals with User-selected passwords are subject to arithmetical guessing thrust, a form of reference thrust, in which an thrust sorts the password reference by rely, or previously-observed, popularity and guesses the most popular passwords first. Password-health meters provide auspices based on rules orient to those used to erect password custom, but the hazard classic under which they give this 'strength' is dim.

Thus, most online tenacity meters will deem a string of 32 random lowercase letters a 'weak' password. Alain Mayer, Fabian Monroe, Michael K. Reiter deals with, in this papers us far advance the theory and practice of graphical passwords. We take as a main benchmark the need to gauge graphical passwords' security relative to that of extols passwords. We design two graphical password schemes that we believe to be more secure than extols passwords. Throughout this paper we focus on dotted passwords that are repeatable by the user. This divide our work from all works on dotted pattern notice of which we are aware where it success for the device to notice an input as being necessarily.

Because pattern respect schemes require the storage of the plain-text password on the device, the password is vulnerable to an attacker who captures and probes the device. In contrast, because graphical passwords are retable, our schemes can derive a secret key. Graphical input resource enable the user to duple the position of inputs from the mortal order in which those inputs occur, and we show that this duple can be used to generate password schemes with in fact larger (memorable) password spaces. In order to evaluate the security of one of our schemes, we devise a novel way to capture a subset of the great passwords that, we believe, is itself a contribution. In this work we are primarily motivated by devices. Samuli Hemminki, Petteri Nurmi, Sasu Tarkoma deals with we present novel accelerator based techniques which can be used single, or in conjunction with other sensors for portage mode expose on smart phones. We focus on accelerator as they are well-suited to overcome the above mention limitations. First, accelerators have very low power consumption, enabling continuous transportation behavior monitoring. Second, accelerator measure user's going directly and therefore do not depend on any external signal sources. Third, accelerator contains highly detailed information about phone movement, enabling fine-grained distinction of different motorized transportation modalities. Mike Just deals with this paper reports on an experimental survey into user chosen questions. We collected questions from a large mate of students, in a way that encouraged participants [2] to give practical data. The questions allow us to consider possible modes of attack and to judge the near effort needed to crack a question, according to a new model of the knowledge of the attacker. Using this model, we found that many members were likely to have chosen questions with low decay answers, yet they believed that their challenge questions would stay attacks from a new arrival. Though by asking multiple questions, we are able to show a marked improvement in security for most users. In a second stage of our experiment, we applied existing advantage to measure the worth of the questions and answers. Although having youthful memories and choosing their own questions, users made errors more often than desirable.

3. Proposed System:

All cloudlets are Wi-Fi-enabled. Each cloudlet server has a surrounded Wi-Fi entree socket. Therefore, each cloudlet could connect to many mobile devices within the Wi-Fi range. The cloudlets are organized by whichever wired or wireless links to form the net. All cloudlets activate fundamentally as gateways at the edge network of the Internet. Remote clouds are assumed accessible through the Internet backbone.

3.1 Platform as a Service (PaaS):

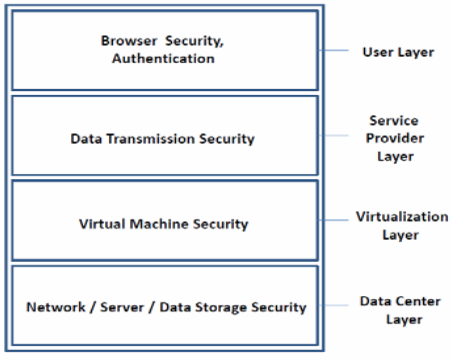

Figure 2: High Level Security Architecture of Cloud Computing

"PaaS is the delivery of a computing platform and solution stack as a service without software downloads or installation for developers, IT managers or end-users. It provides an infrastructure with a high level of integration in order to implement and test cloud applications. The user does not manage the infrastructure (including network, servers, operating systems and storage), but he controls deployed applications and, possibly, their configurations. Examples of PaaS includes: Force.com, Google App Engine and Microsoft Azure.

3.2 Infrastructure as a Service (IaaS): Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. In general, the user does not manage the underlying hardware in the cloud infrastructure, but he controls the operating systems, storage and deployed applications. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Examples of IaaS includes Amazon Elastic Cloud Computing (EC2), Amazon S3, GoGrid. There are also four different cloud deployment models namely Private cloud, Public cloud, Hybrid cloud and Community cloud. Details about the models are given below. Private cloud: Private cloud can be owned or leased and managed by the organization or a third party and exist at on premises or off-premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems [3].

3.3 Public Cloud: A cloud infrastructure is provided to many customers and is managed by a third party and exists beyond the company firewall. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources. These clouds are fully hosted and managed by the cloud provider and fully responsibilities of installation, management, provisioning, and maintenance. Customers are only charged for the resources they use, so under-utilization is eliminated. Since consumers have little control over the infrastructure, processes requiring powerful security and regulatory compliance are not always a good fit for public clouds. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used. Public cloud providers such as Google or Amazon offer an access control to their clients. Examples of a public cloud include Microsoft Azure, Google App Engine.

3.4 Hybrid Cloud: A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other. These clouds would typically be created by the enterprise and management responsibilities would be split between the enterprise and the cloud provider. In this model, a company can outline the goals and needs of services. A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments, as well as those that are secondary to the business, such as employee payroll processing. The major drawback to the hybrid cloud is the difficulty in effectively creating and governing such a solution. Services from different sources must be obtained and provisioned as if they originated from a single location, and interactions between private and public components can make the implementation even more complicated. These can be private, community or public clouds.

3.5 Cloud Providers: Includes Internet service providers, telecommunications companies, and large business process outsourcers that provide either the media (Internet connections) or infrastructure (hosted data centers) that enable consumers to access cloud services. Service providers may also include systems integrators that build and support data centers hosting private clouds and they offer different services (e.g., SaaS, PaaS, IaaS, and etc.) to the consumers, the service brokers or resellers.

3.6 Cloud Service Brokers: Includes technology consultants, business professional service organizations, registered brokers and agents, and influencers that help guide consumers in the selection of cloud computing solutions. Service brokers concentrate on the negotiation of the relationships between consumers and providers without owning or managing the whole Cloud infrastructure. Moreover, they add extra services on top of a Cloud provider's infrastructure to make up the user's Cloud environment.

3.7 Cloud Resellers: Resellers can become an important factor of the Cloud market when the Cloud providers will expand their business across continents. Cloud providers may choose local IT consultancy firms or resellers of their existing products to act as "resellers" for their Cloud-based products in a particular region. Cloud Consumers: End users belong to the category of Cloud consumers. However, also Cloud service brokers and resellers can belong to this category as soon as they are customers of another Cloud provider, broker or reseller. In the next section, key benefits of and possible threats and risks for Cloud Computing are listed.

3.8 Inter-Cloudlet Protocol: We define a new *Inter-Cloudlet Protocol (ICP)* for communiqué among the cloudlets in the net. This ICP protocol supports collective interruption detection and load matching operations, which are clear to mobile users. We use multiple cloudlets, each installed with an *intrusion detection system*

(IDS). Each cloudlet has a database containing a white list of friendly users. This protocol specifies the steps needed to locked inter-cloudlet communications and load matching within the cloudlet net.

3.9 Access to Servers & Applications: In traditional datacenters, administrative access to servers is controlled and restricted to direct or on-premise connections which are not the case of cloud data centers. In cloud computing administrative access must be conducted via the Internet, increasing exposure and risk. It is extremely important to restrict administrative access to data and monitor this access to maintain visibility of changes in system control. Data access issue is mainly related to security policies provided to the users while accessing the data. In a typical scenario, a small business organization can use a cloud provided by some other provider for carrying out its business processes. Some organization will have its own security policies based on which each employee can have access to a particular set of data. The security policies may entitle some considerations wherein some of the employees are not given access to certain amount of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users [4]. Most companies are storing their employee information in some type of Lightweight Directory Access Protocol (LDAP) servers. In the case of SMB companies, a segment that has the highest cloud application adoption rate, Active Directory (AD) seems to be the most popular tool for managing users. With cloud application, the software is hosted outside of the corporate firewall. Many times user credentials are stored in the cloud application providers databases and not as part of the corporate IT infrastructure. This means SaaS customers must remember to remove/disable accounts as employees leave the company and create/enable accounts as come onboard. In essence, having multiple cloud application products will increase IT management overhead. For example, cloud application providers can provide delegate the authentication process to the customer's internal LDAP/AD server, so that companies can retain control over the management of users. Large enterprises, the management of user's account as the adoption of single sign on (SSO) or each employee will be dispatched some different accounts to access different systems. Thus, multi-authentication for each employee might be very often to be confronted in an enterprise. Those accounts that come along with each individuals might be the same or different. Therefore, how could the administrator well manage those user's identification accounts and the corresponding passwords or achieve the state of SSO is another important issue. Nevertheless, the application of SSO for identification and authentication does have serious information security risk. In addition, the management of authorized access privilege is also a critical key point [5].

3.10 Data Transmission: Encryption techniques are used for data in transmission. To provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. SSL/TLS protocols are used here. In Cloud environment most of the data is not encrypted in the processing time. But to process data, for any application that data must be unencrypted. In a fully homomorphism encryption scheme advance in cryptography, which allows data to be processed without being decrypted. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud provider. Man-in-the-middle attacks is cryptographic attack is carried out when an attacker can place themselves in the communication's path between the users. Here, there is the possibility that they can interrupt and change communications.

4. Conclusion:

We use the cloudlet net to perform cooperative interruption discovery among several cloudlets. This results in important gain in collective intrusion detection rate. We unload very large Tweet dataset to the AWS cloud for Map Reduced sifting of malicious hidden in large tweet dataset. Fast filtering of spams from huge dataset can help malicious perusing and signature groups from new unknown outbreaks. We review below the major study findings of these studies.

5. References:

1. Bahar, Md. Ahsan Habib and Md. Manowaru l Islam, "Safety construction for mobile cloud computing," International Journal of Scientific Knowledge, pp. 11-17, July 2013.
2. M. Cai, K. Hwang, Y. K. Kwok, S. Song, and Y. Chen, "Collaborative Internet Worm Containment", IE EE Security and Privacy, May/June 2005, pp.25-33.
3. D. Chen, and Hong Zhao, "Data Security and Confidentiality Defense Issues in Cloud Computing.
4. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.
5. Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing" Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.