Review on Food Court goes Smart with Cloud: Opportunities and Threats

Shreyas Rajguru[1], Vasudha Mathur[2], Sandeep Yadav[3], Prof. P. R. Jaiswal[4]

[1, 2, 3, 4] Vishwakarma Institute of Information Technology, Pune, Maharashtra, India

[1]shreyasrajguru@gmail.com

[2]vasudha.mathur92@gmail.com

[3]19sandeep.yadav@gmail.com

[4]pawan.jaiswal@viit.ac.in

ABSTRACT

Total customer satisfaction is the key factor for success of any business. In a restaurant, there are disadvantages associated with the waiter service like late delivery or improper service manners. One improving aspect would be to remove the middle man, i.e. the waiter, while giving the order so that the order is directly sent to the chef. This would be beneficial as the precious time of customer will not be wasted on unnecessary tasks like waiting for the waiter to get free. On a larger scale, this idea could be applied to an agglomeration of restaurants such as all the restaurants registered to an independent food ordering website. All the information such as menus of different restaurants or customer preference history must be stored in a database, stored centrally on a cloud, which would make this technique possible. A software system that increases operational efficiency through use of an internal wireless communications system and a statistical data processing unit can be proposed. The main domain is of Cloud and Android application. Moreover, since Cloud is a broad term, the key aspects of the cloud that would be utilized in such a system would be cloud storage as well as cloud security. Here the system would come under the wing of Software as a Service (SaaS). This paper elaborates on the above mentioned concepts that would be essential to realize the proposed system. This paper will also shed light on the specifications and the problems associated with such a system.

Keywords - Cloud, Android, cloud storage and cloud security.

1. INTRODUCTION

We are implementing a project which will improve the interaction between the customer and the restaurant owner also providing additional features to both the stakeholders. Our implementation will include an android mobile application which will be backed by a cloud data server. Using the android application the customer will not only be able to make the orders but also he/she can track his/her order history. A single customer profile will be maintained across wide range of restaurants. This project comes under the domain of cloud computing providing SAAS feature of the cloud.

2. OPPORTUNITIES AND THREATS

The customer can use the application services to place order only when he is within the predefined premises of the restaurant where in the user can use the application to connect to the cloud data storage. If not, the customer is made available with features like creating an account, or reading the prominent features as well as reviews of the registered restaurants.

Thus, the customer and the restaurant data have to be stored in a database which would be hosted on a cloud, thus, cloud storage is a required feature on which light must be shed before implementing such a system. Moreover, as a convention it is thought that the most serious drawback of the cloud is its low

security. Therefore, along with cloud storage a robust security concept must be examined which would provide the cloud storage with the protection that it needs. This would allow the stakeholders to put faith in the system.

We'll talk about storage, sharing and protection in cloud, which would be required for the customer and restaurant data, in the next couple of pages.

3. CLOUD STORAGE[1]

3.1 Public Cloud

These services range from simple building blocks, such as online file storage, to business software applications, such as Salesforce.com. Public cloud services are open to anyone with a credit card and an Internet connection. An example of a public cloud service is Amazon's Simple Storage Service or S3. It is the largest public online storage service in the world, though many other companies also offer public storage services. There are two key advantages to public cloud services:

- The cost is all operating expense and is much easier to account for. There is no capital cost involved.
- One can get unlimited storage
- Initialization can be quick.

3.2 Private Cloud

Private clouds do not offer the benefit of quick provisioning and low capital costs that public clouds do. Private clouds are Internet-accessible services for the use of, and maintained by, a business or an organization. But they do have some important advantages.

- Quicker recovery: Most important is that when the data is needed it can be retrieved much faster than is typically possible over the Internet from the public cloud storage.
- Quicker startup: Initial data copies can be made in your office using a high-speed local area network instead of the days and sometimes weeks that can take to copy data across the Internet on a public cloud.
- Control and peace of mind: You know where your data is at all times, typically residing in your own network.

4. CLOUD SECURITY

4.1 Cloud Security Challenges (threats)

In the private and public cloud, perimeter boundaries blur and control over security diminishes as applications move dynamically and organizations share the same remotely located physical hardware with strangers. However, in traditional datacenters, IT managers put procedures and controls in place to build a hardened perimeter around the infrastructure and data they want to secure. This configuration is relatively easy to manage, since organizations have control of their servers' location and utilize the physical hardware entirely for themselves.

4.1.1. Data Privacy

The public nature of cloud computing poses significant implications to data privacy as well as confidentiality. Cloud data is often stored in plain text, and few companies have an absolute understanding of the sensitivity levels their data stores hold. Data breaches are embarrassing and costly. In fact, a recent report by the Cloud Security Alliance lists data loss and leakage as one of top security concerns in the cloud. Recent laws, regulations and compliance frameworks compound the risks; offending companies can be held responsible for the loss of sensitive data and may face heavy fines over data breaches. Business impacts aside, loose data security practices also harm on a personal level. Lost or stolen medical records, credit card numbers or bank information may cause emotional and financial ruin, the repercussions of which could take years to repair. Sensitive data stored within cloud environments must be safeguarded to protect its owners and subjects alike.

4.1.2. Multi-Tenancy

Cloud computing users share physical resources with others through common software virtualization layers. These shared environments introduce unique risks into a user's resource stack. For example, the cloud consumer is completely unaware of a neighbor's identity, security profile or intentions. The virtual machine running next to the consumer's environment could be malicious, looking to attack the other hypervisor tenants or sniff communications moving throughout the system. Because the cloud consumer's data sits on common storage hardware, it could become compromised through lax access management or malicious attack. In a joint paper published in November 2009 by MIT and UCSD entitled "Hey,

You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," the authors exhibited the possibility of a side-channel attack in a cloud environment in which an attacker would be able to implant some arbitrary code into a neighbor's VM environment with little to no chance of detection. In another scenario, a security bulletin from Amazon Web Services reported that the Zeus Botnet was able to install and successfully run a command and control infrastructure in the cloud environment.

4.1.3. Data Remanence

Although the recycling of storage resources is common practice in the cloud, no clear standard exists on how cloud service providers should recycle memory or disk space. In many cases, vacated hardware is simply re-purposed with little regard to secure hardware repurposing. The risk of a cloud tenant being able to gather pieces of the previous tenants' data is high when resources are not securely recycled. Resolving the issue of data remanence can frequently consume considerable negotiating time while establishing service agreements between an enterprise and a cloud service provider.

4.1.4. Data Control And Mobility

Moving data from static physical servers onto virtual volumes makes it remarkably mobile, and data stored in the cloud can live anywhere in the virtual world. Storage administrators can easily reassign or replicate users' information across data centers to facilitate server maintenance, HA/DR or capacity planning, with little or no service interruption or notice to data owners. This creates a number of legal complications for cloud users. Legislation like the EU Privacy Act forbids data processing or storage of residents' data within foreign data centers. Careful controls must be applied to data in cloud computing environments to ensure cloud providers do not inadvertently break these rules by migrating geographically sensitive information across political boundaries. Further, legislation such as the US Patriot Act allows federal agencies to present vendors with subpoenas and seize data (which can include trade secrets and sensitive electronic conversations) without informing or gaining data owners' consent.

4.2 Cloud Security Solutions[2]

The system's patented key-management technology combined with industry standard encryption should allow businesses to control access to sensitive data stores and operate safely in public and private clouds. The system should alleviate data security and privacy risks associated with deploying information into any cloud computing environment.

4.2.1. Custody Of Encryption Keys

The system will help users control data access with the option of isolating the physical storage of keys away from the cloud infrastructure provider. This will stop infrastructure administrators from accessing data or keys and gives customers the freedom to move data from one provider to another without the fear of vendor lockin. The system's on-premise solution will give customers even more control by keeping keys within their trusted environment and controlling custody at all times. Further, if a regulatory agency presents vendors with subpoenas and seizes data without informing or getting consent from data owners, the encrypted volumes remain useless without the encryption keys.

4.2.2. Easy Deployment

With a simple agent installed on the virtual machine image, the system should be able to ensure that data in the cloud environment is tamper proof, protected through encryption at the kernel level. Communication between the agent and the system management server must be secure, thus avoiding the risk of any man-in the- middle attacks to gain access to the encryption keys.

4.2.3. Granular Control

The system's unique policy-based approach to key management and data access will allow users to determine exactly which server gets access to secure data. Virtual servers spinning up in the cloud consumer's environment must first authenticate to the system key server with credentials that have been encrypted. Based on the defined policies, information provided back to the key management server will then be vetted, ensuring the cloud environment is safe to release the keys into. Along with detailed key management policies, the system will offer role-based access to the administrators, with specific permission levels ranging from full access, key approval, to audit logging only.

4.2.4. Industry Standard Encryption

The system would use industry standard AES encryption to make data unreadable and unusable to those without the encryption key. Rendering the data useless greatly reduces the risks associated with data theft, exposure to unauthorized parties or data seizure through judicial subpoena. The system's ability to encrypt data will add additional benefits to the cloud consumer when changing vendors or terminating storage agreements. Any encrypted data remaining on vendor storage devices will be unrecognizable and secure.

4.2.5. Reporting

The system will accommodate the frequent need to view system configuration settings by providing a full audit trail of key approvals occurring on the management server. The system can also offer detailed logging and reporting for any actions performed within the system and any key approvals. All events and changes, whether they come from an administrator or the system itself, will be logged and can be called upon for a full detailed audit trail.

4.2.6. Secure Key Management

With the system, cloud consumers can have exclusive control of the encryption keys, and therefore control of their own data. The encryption key management will not be hosted by the cloud service provider, but rather by the cloud consumers themselves. This will provide the cloud consumers the ability to take advantage of the cloud services, but still maintain full control of the encryption keys within their environments.

5. CONCLUSION

This paper elaborates on the concepts, i.e. cloud storage and cloud security, answers to which would be essential in order to realise the food ordering system. We would also like to conclude by summing up the paper as well as its features which will enable the customer to place order by sitting at a single place. The important things about the system are that it will save user time and eliminate the need of middleperson (i.e. waiter). It makes the life of the user easy by giving him/her a chance to sit back on the table and make all orders. It is user friendly software that is portable, reusable and flexible. In future it will be an important system that will be used in most of the restaurants.

REFERENCES

[1] Robin Harris, What Every Business Should Know About Cloud Storage May 2012, Chief Analyst At TechnoQWANLLC, White Paper

[2] Trend Micro Virtualization Security (July 2010), Addressing Data Security Challenges In Cloud, White paper.

