INFLUENCE AND SECURITY INFLUENCE OF CLOUD COMPUTING IN E-COMMERCE AND INDUSTRIES

1.INTRODUCTION

E-commerce refers to the buying and selling of goods or services using the internet-commerce is often used to refer to the sale of physical products online but it can also describe any kind of commercial transaction facilitated through the internet. There has been a sudden increase of online shoppers with the advent of internet. People's live has made more convenient and accessible. Using E-commerce anyone can access any E-commerce website from anywhere without moving physically and users can easily choose products according to their wish. Business have widely recognized the advantages of investing in cloud computing technologies such as efficiency, reliability, improving availability and rising e-business costs [1]. Using the cloud computing platform an e-commerce enterprise can choose or rent IT products and services based on its demand so as to establish the technical architecture. Cloud computing helps to improve the security in e –commerce by providing a safer way to store the information. The wide range of cloud based e-commerce applications and integration platforms offers IT leader's a great flexibility when choosing a deployment models and suppliers. As a new IT concept cloud computing is being applied to many industries especially electronic commerce industry. This paper discusses the influence of cloud computing on traditional e-commerce from the perspective of technology and also the security measures of cloud computing.

2.INFLUENCE OF CLOUD COMPUTING IN E-COMMERCE

Cloud based e-commerce applications enable businesses to rapidly respond to market changes. Cloud computing provides so many benefits to the e-commerce industry. The major benefit that is provided by the cloud computing is the security of data. Cloud computing in e-commerce helps the business to look virtually big and operate extensively.

2.1. Scalability

The main advantage of cloud computing platform is that it is highly scalable. These systems are often referred to as "elastic systems". Cloud computing allows the e-commerce companies to upscale or downscale the services according to the customer demand and seasonal spikes. Cloud systems enable the use of resources according to requirements, when we need only few resources cloud facilitates low memory and vice versa

2.2 Reduced cost

Cloud computing reduces the cost of developing and maintaining IT infrastructure. we do not need to invest in hardware or software infrastructure according to the growth of the business. Cloud based e-commerce applications lower costs and faster deployments enable IT and business leaders to evaluate new opportunities without large upfront investments. [2] Cloud provides the facility of paying per use to reduce the cost.

2.3. Speed

For an e-commerce business speed is an important factor to make the customer satisfied. Good speed ensures higher conversations and helps the companies to get more customers. If a web page takes much time to load people will leave the webpage. Cloud systems provides a greater speed with greater band width, computational power and storage.

2.4 Security

Data security is the major benefit of cloud computing. Cloud computing allows the data to be stored in a virtual space. Data on physical servers can't overcome the hazards of the disasters. The data stored in virtual space is more secured than the data stored in physical servers.

2.5 Information Sharing

Cloud systems can show information in a smooth way. The increase in the ability to show information between clouds and communities of the cloud is the possible change going to happen in e-commerce platforms [3].

3.CLOUD COMPUTING DEPLOYMENT MODEL

It is important to select a type of cloud for a secure computing solution. There are four types of cloud deployment model.

3.1 Private Cloud

It is a cloud based infrastructure used by standalone organizations. It offers greater security, the data backup is done using a firewall and can be hosted internally or externally. The private cloud allows systems and services to be accessible within an organization. Private cloud provides the organizations greater control over data by permitting only authorized users. In private cloud resource sharing is highly secured.

3.2 Public cloud

Public clouds as the name indicates are available to the general public. Here datas are created and stored on third party servers. Public cloud deployment model can be used for businesses with low privacy concerns. Using public clouds, we can easily extend the cloud's capacity as per company requirement.

3.3Community cloud

The community cloud allows systems and services to be accessible by a group of organizations. Several organizations with similar backgrounds share the infrastructure and related resources of a community cloud. Community cloud facilitates data sharing and collaborations.

3.4 Hybrid Cloud

A hybrid cloud is a mixture of public and private cloud in which the critical activities are performed using private cloud where non critical activities are performed using public cloud. Hybrid cloud enhances security and flexibility.
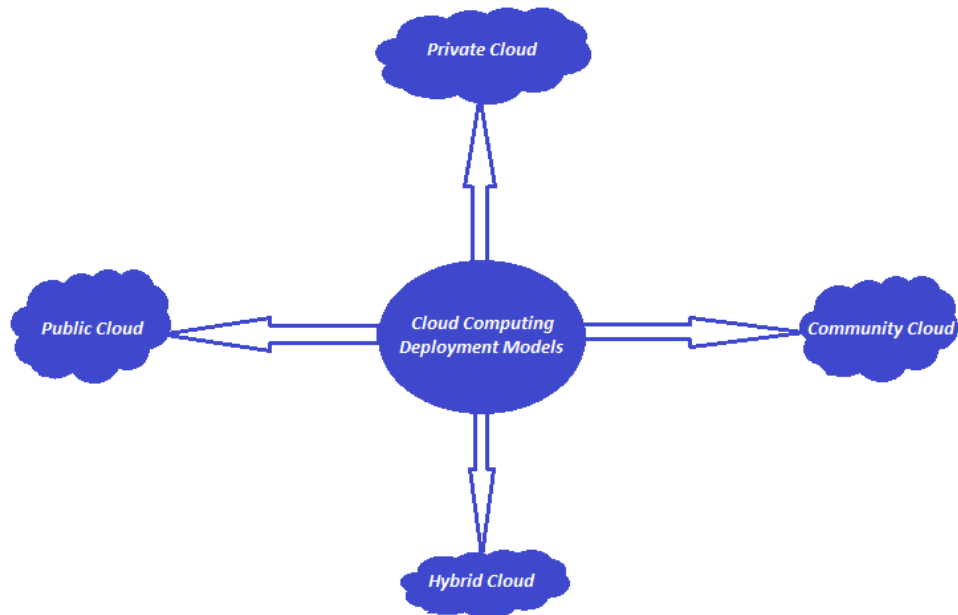
Figure 1: Cloud Computing Deployment Models

4.CLOUD COMPUTING SERVICE MODELS

E-commerce companies are experiencing burden on their IT infrastructure as they struggle to meet growing customer expectations for fast, reliable, and secure services. In order to the increase the processing power and storage capabilities of their IT systems companies needs to invest a lots of money. Cloud computing offers three service models to satisfy the business requirements.

4.1. SaaS(Software as a Service)

Software-as–a-Service (SaaS) model allows to provide software application as a service to the end users using internet. In SaaS software application is maintained by the vendor. The license to the software may be subscription based or usage based. SaaS offers shared data model, so multiple users can share single instance of infrastructure. It is not required to hard code the functionality for individual users. Here all users run the same version of the software. SaaS has proved to be beneficial in terms of scalability, efficiency and performance. There is no requirement for complex software packages at client side and no risk of configuration at client side. SaaS has the Low distribution cost among all service models. When you want an application to run smoothly and reliably with minimal input from the user SaaS is the best option. Big Commerce is an example of SaaS e-commerce platform. Big Commerce provides a complete shopping software without worrying about the coding and hosting of the software.

4.2. IaaS(Infrastructure as a Service)

Infrastructure as a service is also known as hardware as a service. It is a computing infrastructure managed over the internet. In IaaS resources are available as services. Services are highly scalable, dynamic and flexible. For efficient storage of files it provides back-end storage. It provides load balancing capability at the infrastructure layer. IaaS allows the same physical infrastructure to be shared among different users.it provides services based on pay as per use basis, so the users are required to pay for what they have used. Using IaaS users do not worry about the software upgradation and trouble shoot issues related to hardware components. IaaS provides fails to provide 100% security for the data.it offers portability, interoperability with legacy applications.

4.3. PaaS(Platform as a Service)

Platform as a service offers development, deployment tools and run time environment for applications.PaaS provides browser based development environment, which allows the developer to create database and edit application code either using point and click tools or API's.Built in security ,scalability and web service interfaces are the important features of PaaS.We can easily integrate other application on same platform with PaaS.Applications outside the platform can be connected using web services interface.PaaS infrastructure includes servers, storage and networking.PaaS supports complete web application life cycle. PaaS development tools can reduce the coding time for an application.
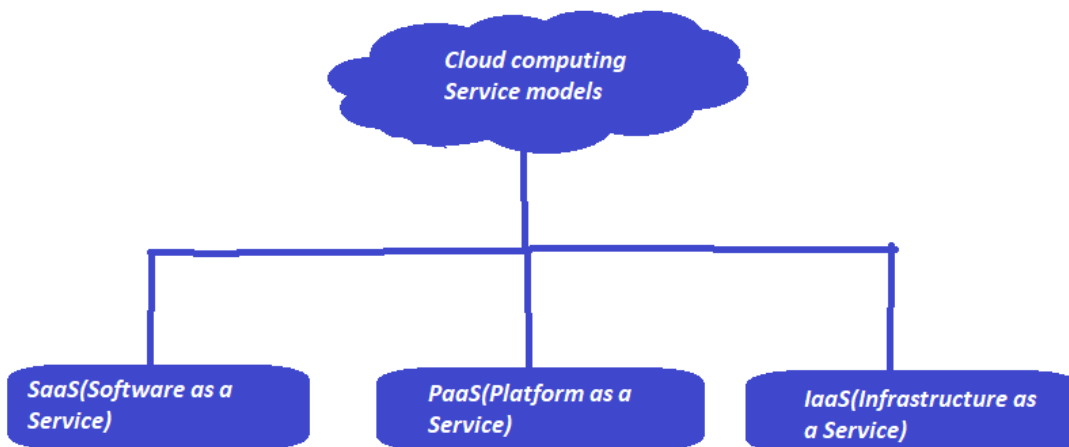

Figure 2: Cloud Computing Service Models

5.DATA SECURITY AND PRIVACY IN CLOUD COMPUTING

One of the major concerns regarding the security and privacy in cloud computing is the protection of data. The easy accessibility to the clouds functions allows users to effortlessly work on their computing tasks and access their data simply via the internet. The meaning of security is plentiful. Security is the combination of confidentiality, the prevention of unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information and availability, the prevention of unauthorized withholding of information. Following are the security mechanisms used in cloud.

5.1 Encryption

Data is coded in a readable format by default. When this data is transmitted over a network it is vulnerable to unauthorized and malicious access. Encryption mechanism is used to preserve the confidentiality and integrity of data. It is used for encoding data into a protected and unreadable format. Encryption technology uses a standard algorithm called a cipher to transform original data into encrypted data referred to as cipher text. When encryption is applied to plain text data, the data is paired with a string of characters called an encryption key, a secret message that is established by and shared among organized parties. The encryption key is used to decrypt the cipher text back into its original plain text format. A malicious service agent is unable to retrieve data from an encrypted message. The retrieval attempt may further be revealed to the cloud service customer.

5.2 Hashing

This mechanism is used when non reversible form of data needs to be protected. Once hashing has been applied to a data, it is locked and no key is provided for the data to be unlocked. Hashing technology is commonly used for storage of passwords. Hashing technology can be used to derive a hashing code from a message. The hashing code is a fixed length code and smaller than the original message.

The message sender can then utilize the hashing mechanism to attach hashing code to the message. A hashing function is applied to protect the integrity of a message that is encrypted and altered by a malicious service agent before it is forwarded. The firewall can be configured to determine that the message has been altered, thereby enabling it to reject the message before it can proceed to the cloud service.

5.3 Digital signature

The digital signature mechanism is used for providing data authenticity and integrity through authentication and non-repudiation. a digital signature is assigned with the message before transmission, which is then rendered invalid. If the message experiences any subsequent unauthorized modifications. A Digital signature provides evidence that the message relived is same as the one created by its rightful sender. Both hashing and encryption technologies are used for the creation of digital signature.

5.4. Public key Infrastructure

It is a common approach used for managing asymmetric key. Public key infrastructure exists as a system of protocols, data formats, rules and practices that enable large scale systems to securely use public key infrastructure. The main purpose of this system is to associate public keys with their corresponding key owners this is known as public key identification. The public key infrastructure mechanism is primarily used to counter the insufficient authorization threat. Public key infrastructure relies on the use of digital certificates it is digitally signed data structure which bind public keys to certificates owner identities. It is a method for implementing asymmetric encryption, managing cloud consumer and cloud provider identity information.

5.5. Identity and Access Management(IAM)

The identify and access management mechanism contains the components and policies necessary to control and track user identities and access privileges for IT resources. IAM consist of four components.

(1) Authentication: Username and password are the most common form of user authentication credentials managed by the IAM system. It can also support digital signatures, digital certificates, biometric hardware and locking user accounts to registered IP or MAC addresses.

(2) Authorization: The authorization component defines the correct granularity for access controls and oversees the relationships between identities.

(3) User Management: The user management program is responsible for creating new user identities and access groups, resetting passwords and managing privileges.

(4) Credential Management: The

(5) credential management system establishes identifies and access control rules for defined user accounts, which mitigates the threat of the insufficient authorization.

6.CONCLUSION

It is clear that cloud computing is essential for E-Commerce industry as it provides many opportunities for E-Commerce industry. The application of advanced cloud computing in E-commerce helped to handle shortage of resources and man power. Although there are many security mechanisms available in the cloud systems, some problems such as platform security, technical standards, regulatory and other services are not well resolved yet in practice.

7.REFERENCES

[1] Arya M Nair. "cloud computing in e-commerce". IRJET, Volume:07.

[2] Tim weaver and Gene Alvarez." The top four impacts of cloud computing on E-Commerce". G00258146.

[3]" The impact of cloud computing on E-Commerce Industry". Idea mine.