Borneo International Journal eISSN 2636-9826; Vol. 5 (3); 2022; 14-26
Published by *Majmuah Enterprise*
www.majmuah.com

Comparative Study on Cloud Computing Implementation and Security Challenges

K. T. KHANISHA THANASEGARAN, MOHAMAD FADLI BIN ZOLKIPLI

School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA
Email: khanishathanasegaran@gmail.com, m.fadli.zolkipli@uum.edu.my | Tel: +601110872917, +60177247779 |

Received: December 17,2022
Accepted: December 19, 2022
Online Published: December 21, 2022

Abstract

As a concept, cloud computing can be defined as an innovative paradigm that enables users to access computing resources when they require them, such as network, storage, servers, applications, and services, based on a pay-as-you-go model. Cloud computing refers to the sharing of resources among consumers. As well as providing computing infrastructure, cloud computing also provides users with a platform for developing their own applications on top of this platform. As a result, capital expenditures on the development of applications are reduced because of the software development process. The cloud service allows users to access resources from any location at any time with an internet connection at any time. Although Cloud Computing provides a few advantages, there are some security challenges that must also be overcome. The purpose of this paper is to compare and discuss the implementation of cloud computing in various sectors such as e-health, e-commerce, banking, and the construction industry. This paper also discusses the security challenges of cloud computing in various aspects from various perspectives.

Keywords: cloud computing, cloud service, advantages, implementation, security challenges

1. Introduction

In the fast-growing field of Information Technology, cloud computing has proved to be a huge boon. With it, the concept of virtualization of resources as services is introduced, which covers resources such as networks, storage, servers, applications, and services, as well as network applications. It is possible to access the cloud service wherever there is an internet connection, so it can be accessed from anywhere. To facilitate the disbursement of computing resources, a cloud is set up that can host them on demand for the users when they require them. Only the amount of cloud consumption that is consumed by the users will be charged to them. As a result, small and medium sized businesses can reduce their capital expenditures for deploying the necessary resources on site, which is beneficial for them (George & Rajakumari, 2019).

In the past few years, there has been a steady increase in the adoption of cloud computing. According to a report published in the Economic Times, over 88 percent of the Indian companies have already adopted cloud services. People have witnessed a significant change in their lives over the past few years because of cloud computing, which has transformed the way they listen to music, share photos, and conduct business. There will, however, be potential risks associated with the introduction of cloud computing, and they are like those associated with any other development of a technology. A significant obstacle to cloud computing adoption is the security concerns that are associated with it. According to organizations like ENISA, the Cloud Security Alliance (CSA), the National Institute of Standards and Technology, and cloud service providers like IBM and Amazon, approximately 80% of cloud services currently in use meet strict data security and privacy requirements. Today, there are more than 20,000 types of cloud services available (Yan, Hao, Cheng & Zhou, 2018).

Underlying this model is the ability for customers to access a pool of configurable computing resources whenever and wherever they desire (for example, networks, servers, storage, applications, and services). Provisioning and releasing these resources can be done rapidly and with minimal management effort. There are five essential characteristics of the cloud model, three service models, and four deployment models that can be utilized to maximize its benefits (Mell & Grance, 2011). During the past few years, cloud computing has developed to the point where more and more governments, organizations, and businesses are adopting cloud computing. As cloud computing becomes more and more important for the continued success of businesses, it may be necessary for businesses to adopt this technology before their competitors do so. As it stands, security is a key component of the success of cloud computing, and it would be a good idea to give more attention to the privacy and security issues involved in cloud computing.

2. Overview of Cloud

2.1 Cloud Service Models

There are different types of cloud computing, but the term cloud computing covers the general concept of providing various kinds of services over the internet, such as data storage, processing, analytics and other services, without relying on local hardware. Businesses have access to the provider's services via the Internet and use third-party services to help them with their computing tasks. It is also important to note that cloud services can be differentiated by the manner in which they are billed, their functionality, and their business model. There are five cloud service models as follow:

2.1.1 Software as a Service (SaaS)

Cloud computing services and applications are being delivered over the Internet through Software-as-a-Service (SaaS). In order to free from the hassle of maintaining and managing complicated software and hardware, users simply access the software via the Internet rather than installing and maintaining it by themselves. Since it eliminates the need to install and run applications on their own computers and in data centers, it eliminates the expense of buying, installing, and maintaining hardware and software. On a pay-as-you-go basis, cloud service providers offer software as a service that can use when needed. It is possible to run most SaaS applications straight from a browser without having to download or install anything in order to run the applications. A SaaS application is sometimes referred to as a web-based application, a hosted application, or an on-demand application.

The advantages are as follow:
i. Cost-Effective: The only thing users have to pay for is what they use.
ii. Reduced time: It is usually possible to access SaaS apps directly from a browser without installing any software or downloading any files. Software deployments can be sped up by reducing the time spent installing and configuring.
iii. Accessibility: Whenever and wherever users want, users can access app data.
iv. Automatic updates: Updates are automatically performed by SaaS providers rather than customers purchasing new software.
v. Scalability: On-demand services and features are available to users.

2.1.2 Platform as a Service

The Platform as a Service cloud computing service offers developers an environment to build applications and services that can be accessed from the internet. It is a type of cloud computing service that offers a platform for developers. Users can access these PaaS services from their web browsers simply by launching a web browser, and the services are hosted on the cloud. Hardware and software are hosted on the infrastructure of PaaS providers so that they can provide the service. Because of this, PaaS provides users with the opportunity to develop and run new applications without installing hardware or software themselves. Thus, it is possible to develop and deploy users' application independent of the hardware in which it is deployed. Consumer do not have the control or responsibility over the underlying infrastructure of the cloud service, such as the network, servers, operating systems, or storage. It is possible to control which applications are deployed, as well as the environment where they are hosted if users have access to the application settings. Take for instance an annual day event that someone would like to hold, he/she would have two options, either he/she could create a venue or he/she could rent a venue, but both options exist if he/she want the function to be the same.

The advantages are as follow:

i. Simple and convenient for users: Users can access most IT services via a web browser from anywhere, and it provides much of the infrastructure.
ii. Cost-Effective: By eliminating the need to purchase hardware and software on-premises, the service charges per-use for the services provided.
iii. Efficiently managing the lifecycle: With it, users can build, test, deploy, manage, and update web applications throughout the entire lifecycle.
iv. Efficiency: As a result, applications can be developed more efficiently with higher-level programming and reduced complexity.

2.1.3 Infrastructure as a Service

A service model called Infrastructure as a Service (IaaS) provides computer infrastructure as a service on an outsourced basis in order to support a variety of activities. Generally, IaaS is defined as a service in which enterprises are provided with network equipment, devices, databases, and web servers through the provision of IaaS services. Hardware as a Service (HaaS) is another name for it and it is also referred to as HaaS. Customers who use software as a service typically pay by the hour, week, or month based on how much they use it. Customers may also be charged depending on how much space they use for virtual machines, as some providers do this. These applications can be developed, delivered to clients, and implementation tools, databases, etc., by using the underlying operating systems, security, networking, and servers.

The advantages are as follow:

i. Cost-Effective: As a result, there is no capital expense and a reduced ongoing cost, while IaaS customers pay on an hourly, weekly, or monthly basis, instead of paying capital expenses.
ii. Website hosting: In contrast to traditional web hosting, IaaS can be less expensive.
iii. Security: It is possible that IaaS Cloud Providers offer a better level of security than current software.
iv. Maintenance: No data center management is needed, nor is it necessary to introduce new releases of the underlying software or development. IaaS Cloud Providers handle all of this.

2.1.4 Anything as a Service

It is also known as Everything as a Service or EaaS for short. Cloud service providers these days offer anything as a service, which is a combination of all of the above services as well as some additional services, which is typically packaged as a single package by the cloud service providers.

The advantages are as follow:

Since this is a combined service, as a result it has all the advantages of each type of cloud service.

2.1.5 Function as a Service

There are several types of cloud computing services, but one of them is called FaaS. As part of its platform, it provides its users or customers a means of developing, computing, running and deploying the code or an entire application as functions using the code or platform. By doing this, the user will be able to develop and update the code entirely at their convenience without having to worry about the maintenance of the underlying infrastructure at any time. It is possible to execute the developed code in response to the specific event that has been developed. The model is also the same as the PaaS model. In terms of execution, FaaS is a model that is driven by events. In the serverless container, it is implemented as a serverless application. The user will now trigger an event that will execute the code in the application once it has been completed and the application is completely developed. As a result of the triggered event, the servers are activated to perform the action by responding and activating the servers. This is the type of server that is managed by the vendor and is nothing more than a Linux server or any other type of server that is managed by the vendor. Due to the fact that the customer does not have a clue about any servers, therefore they would not have to maintain any servers, which is why it is a serverless architecture.

The advantages are as follow:

i. Highly Scalable: In order to meet the demand for the service, the provider automatically scales the capacity.
ii. Cost-Effective: It is only charged based on how many events are executed.
iii. Code Simplification: As a result of FaaS, users are able to upload their entire application at once. Code can be written to write independent functions or functions like them.
iv. The code maintenance is sufficient, and the servers don't need to be maintained.
v. Any programming language can be used to write functions.
vi. System control is lessened.

2.2 Cloud Deployment Models

In a cloud deployment model, the type of cloud environment is identified based on ownership, scale, and access characteristics, as well as the cloud's nature and purpose. The location and control of the servers are both defined by a cloud deployment model. Users can specify how their cloud infrastructure should look, what changes they can make, and whether services will be provided to them or if they will have to do everything by themselves with a cloud infrastructure specification. A cloud deployment type also affects how their infrastructure interacts with their users in terms of their relationship with the infrastructure. There are five cloud deployment models as follow:

2.2.1 Public Cloud

Cloud-based public services and systems are accessible to anyone since they can be accessed by anyone. It may be less secure than a private cloud due to the fact that the public cloud is open to everyone. Several types of public clouds exist, including those in which cloud infrastructure services are made available over the Internet to the general public or the general public's groups. Cloud services are delivered by an entity, not by consumers, who own the infrastructure that provides the cloud services. This type of cloud hosting service will make it easy for the user's customers to access their systems and services. With its broad range of services, cloud hosting is an excellent example of cloud computing, which offers a wide range of services to a variety of customers. By establishing such an arrangement, backup and retrieval of storage is provided either for free, on the basis of a subscription, or on the basis of a pay-per-use basis. A good example would be Google App Engine.

The advantages are as follow:

i. Minimal Investment: The service is pay-per-use, so enterprises that need access to resources right away can use it without incurring hefty upfront fees.
ii. No setup cost: It is not necessary to set up any hardware because the cloud service providers fully subsidise the entire infrastructure.
iii. It is not necessary to manage the infrastructure when using a public cloud.
iv. Maintenance is not performed by users, but by service providers.
v. A dynamic scalability feature allows users to access resources as needed according to the needs of their business.

2.2.2 Private Cloud

As opposed to the public cloud deployment model, the private cloud deployment model is exactly the opposite. It's an environment where a single user (customer) is able to work one-on-one with the vendor. The hardware that user own does not have to be shared with anyone else. As far as the difference between a private cloud and a public cloud is concerned, it comes down to the way the hardware is handled. A “cloud within a cloud” is also known as an “internal cloud” and signifies the ability for an organization or company to access computer systems and services within its own borders. Organizations will implement cloud platforms in secure cloud environments protected by powerful firewalls under the control of their IT departments. When it comes to controlling cloud resources, the private cloud is more flexible than the public cloud.

The advantages are as follow:

i. Total Control: It is solely owned by the user. Control over IT operations, policies, and user behavior is achieved with full control of the service integration process.
ii. Data Security and Privacy: Only authorized employees have access to corporate information stored here. The access and security of resources can be improved by segmenting them within the same infrastructure.
iii. Supports Legacy Systems: Using this approach, legacy systems that cannot access the public cloud can still access the private cloud.
iv. Customization: Private clouds allow companies to customize their solutions to meet their specific requirements, unlike public clouds.

2.2.3 Hybrid Cloud

A hybrid cloud computing system combines the advantages of both public and private clouds using proprietary software. It is possible to host the application in a safe environment with a hybrid solution, while being able to take advantage of the cost savings offered by the public cloud. The need to migrate data and applications between different clouds can be met by using a combination of two or more cloud deployment methods.

The advantages are as follow:
i. Flexibility and control: Businesses can tailor their solutions to suit their unique requirements as a result of increased flexibility.
ii. Cost: Unlike private clouds, public clouds allow scalability, so user only need to pay for extra capacity if needed.
iii. Security: It is considerably less likely for attackers to steal data when it is properly separated.

2.2.4 Community Cloud

The system enables a group of organizations to have access to systems and services that are available to them. In essence, cloud computing is just a distributed system that makes use of the various services available on cloud computing to provide services tailored to specific communities, industries, or businesses. An organization that has a shared concern or task with another organization can share the infrastructure of the community between the two organizations. Management of an organization is usually carried out by three parties, typically by a third party or by several organizations working together.

The advantages are as follow:
i. Cost: Multi-organizational or community resources can be shared in the cloud, making it extremely cost-effective.
ii. Security: Better security is provided by community clouds.
iii. Shared resources: Multi-organization resource sharing is possible.
iv. Collaboration and data sharing: In addition to allowing collaboration, it also allows data sharing.

2.2.5 Multi-cloud

Like a hybrid cloud deployment, it blends public cloud resources with private cloud ones. The multi-cloud approach combines a large number of public clouds within one private cloud instead of merging private clouds. Mishaps still happen even though public cloud providers provide many tools to improve the reliability of their services. There is a fairly good chance that more than one cloud could have a problem at a given time, but it's very rare. Thus, as a result of multi-cloud deployment, users services are even more available and have a higher degree of reliability.

The advantages are as follow:
i. Different cloud providers offer different features so that user can mix and match them to meet the needs of their applications, workloads, and business by selecting a provider that meets their needs.
ii. Reduced Latency: Reduce latency and improve user experience by choosing cloud regions near user’s clients.
iii. High availability of service: The event of an incident occurring in two different clouds at the same time is quite rare. Thus, deploying multicloud improves user’s services’ availability.

2.3 Advantages of Cloud Computing

Basically, cloud computing uses remotely located servers hosting data and programs rather than the computer's hard drive or local server to store and access data and programs. Also called Internet-based computing, cloud computing refers to using the Internet to store and process data.

i. Scalability: The number and size of servers can be easily increased and decreased with Cloud hosting. Cloud resources can be increased or decreased in this way. In times of sudden growth in demand, cloud computing is an excellent solution for altering plans due to fluctuating business sizes and needs.

ii. Instant: Cloud computing makes everything instantly accessible.

iii. Save Money: The reduction in hardware costs is one of the advantages of cloud computing. Hardware needs are handled by vendors instead of in-house purchases. Hardware upgrades can be expensive, inconvenient, and large for growing companies. These issues are alleviated by cloud computing, which provides quick and easy access to resources. Vendors pay for equipment repair or replacement. Aside from reducing internal power costs and saving space, off-site hardware is also cheaper to purchase. Office space and heat are both wasted in large data centers. It is possible to maximize storage space and reduce energy costs by moving to cloud applications or storage.

iv. Reliability: Instead of being hosted on just one instance of a physical server, virtual partitions draw resources—such as disk space—from a network of underlying physical servers. The availability of a virtual server won't be affected if one server goes down since the remaining servers will continue to share resources.

v. Physical Security: Data centers still house the servers underlying the application so security measures implemented there prevent people from accessing or disrupting them.

vi. Outsource Management: Managing user’s computing infrastructure is done by someone else while user run a business. Both management and upgrading are taken care of for the user.

3. Comparative Study of Cloud Computing Implementations in Various Sectors

3.1 E-Health

It is anticipated that the future of healthcare will be characterized by information-driven models, and the healthcare industry continues to evolve continuously. In order to deal with change and complexity in the industry, cloud technology can be of great benefit to them. With the help of this promising technology, healthcare providers can be able to communicate, collaborate, and coordinate with one another more effectively. In the healthcare industry, the cloud can contribute to more value being delivered for the dollar spent. It can provide custom applications that are cost-effective, flexible, scalable, and efficient, and it can help their business grow. An electronic health record (EHR), laboratory information system, pharmacy information system, and medical image repository can all be safely stored, managed, protected, shared, and archival using the cloud if it is designed to do so in a secure environment. By keeping health records up-to-date and making it possible for different healthcare providers to interact continuously with one another, patients will receive better care in the long run. Health care providers are being held back from implementing the cloud on a large scale due to a number of obstacles, such as a lack of standards, regulations, and interoperability issues that are holding them back. Security, confidentiality, and trust issues are the other major obstacles that need to be overcome (Al-Issa, Ottom & Tamrawi, 2019).

3.1.1 E-Health Cloud Benefits

i. In the present time, the patient has been interacting continuously with different healthcare stakeholders which has resulted in an improved level of patient care. It is possible for doctors to analyze and diagnose patients' data anywhere, anytime, and at any time.
ii. Cost savings: Hardware and software do not need to be purchased in large quantities and at a high price. A major advantage is that users are able to save both direct costs associated with buying on-premises hardware and software as well as the costs associated with maintenance and support.
iii. Energy savings: It will reduce the energy bill because the data centers will not be needed on premises, so the requirement for expensive cooling systems will not be necessary. This will result in a lower energy bill.
iv. Robust disaster recovery: There is almost always a redundant system and services provided by providers of cloud services in case there is a sudden emergency.
v. Research: An epidemiological monitoring system, which can be used to monitor epidemics, help control disease outbreaks, and support research, is a key component of the cloud as a central data repository.
vi. Solving the scarcity of resources: The use of telemedicine can make it possible for doctors to provide consultations in remote areas.
vii. Rapid deployment: There is no need to wait for long periods of time before using the software or hardware systems.
viii. Data availability: A wide range of stakeholders can access this information and make informed decisions based on it, including physicians, clinics, hospitals, and insurance companies.

3.1.2 E-Health Cloud Challenges

i. Confidentiality: In order to maintain confidentiality, it is important to ensure that the health information of patients is kept from being disclosed to unauthorized parties under any circumstances. In the event that data control is delegated to the cloud, this raises the potential risk of data compromise, since an augmented number of parties are now able to access the data. In the recent years, there have been an increase in the number of parties, devices, and applications involved, which leads to increased data compromise threats. It is essential that the patient have a high level of trust in the healthcare system so that his/her data can be protected to allow the patient/doctor relationship to work effectively. Whenever the patient feels that the information they give their doctor cannot be protected, or if they are concerned that their privacy is not being maintained. Keeping the patient's health data confidential can be defined as ensuring that such data is kept entirely undisclosed to third parties who are not authorized to see such data. Data compromises are more likely to occur when data are delegated to the cloud, since more parties have access to the data. Increasingly many parties, devices, and applications are involved, resulting in increased data compromise threats. A patient's trust in the healthcare system to protect his/her privacy is necessary for an effective patient-doctor relationship. In the future, a patient can select which data he or she will share with the doctor if he or she feels the information will not be protected, or if the patient feels that their privacy will be invaded as a result of the information being provided. Medical diagnoses and treatments can be hindered by data compromise, which can negatively impact the patient-doctor relationship. Disclosing a patient's medical data may result in an employer refusing the job application. Access control and encryption techniques can be used to maintain confidentiality.

ii. Integrity: An organization that maintains the integrity of health data must ensure that the information entered its systems or supplied to a third party is accurate, reliable, and has not been altered or changed in any way. It is important to assure good reliability of cloud services when using an application as crucial as eHealth cloud. There must be no errors in any eHealth cloud service or data. Patients' health can be adversely affected by improper treatment based on inaccurate data. A covered entity must "implement policies and procedures to prevent the improper alteration or destruction of electronic personal healthcare information" as stipulated in the HIPAA Security Rule (Section 164.312(c)(1) Integrity). To be able to use data that is stored and manipulated by healthcare services, integrity and verification functions, such as a checksum or hash, should be implemented, similar to what is done by non-medical applications. Data processing is terminated without processing if the integrity check fails.

iii. Availability. In order for the healthcare cloud system to function effectively, it is imperative that the information is accessible at all times. It is important to note that the availability of data in critical situations is a critical component of the eHealth system, and that it includes the ability to continue operations despite misbehaviour from some authorities and even if a security breach occurs. System upgrades, power outages, and hardware failures should not disrupt high-availability systems. After HIPAA security and privacy rules are enforced, healthcare records should also remain usable.

iv. Ownership and Privacy of Healthcare Information: Owners of information are generally those who created it. The protection of patient medical information requires information ownership to prevent unauthorized access. Healthcare information can be protected through the combination of encryption and watermarking techniques, so that it cannot be transmitted, accessed, or released without the mutual consent of all parties involved. Other healthcare practitioners can share patients' information with them if the patient allows it or denies it. Patients can assign permissions to users to share specific healthcare data within a healthcare system based on their roles or attributes.

v. Nonrepudiation: Authenticating a signature after accessing health information is a repudiation threat. Patients and doctors cannot deny the authenticity of their signatures after misappropriating their health data in the healthcare industry, for instance. The use of digital signatures and encryption in healthcare cloud applications can confirm its authenticity and nonrepudiation just like in electronic commerce.

vi. Data Remanence and Freshness: Remaining data represents data that has been de-identified or removed in some way. Unintentional breaches of data confidentiality may result from the presence of residual data. If data freshness is not taken into consideration, data integrity and confidentiality will not be sufficient in the healthcare system. Health records for patients must be recent and accurate in order to be considered fresh. In critical situations, data inconsistency is caused by storage delays and outdated notifications.

3.2 E-Commerce

It has been widely discussed that cloud computing and e-commerce are adopting widely in developing countries. A number of studies indicate that by deploying these innovations, the developing countries were able to transform into a digital economy, which led them to expand their markets globally and achieve national economic growth. Cloud computing has the potential to transform E-commerce in a positive way. However, smart companies will have to make a trade-off between the benefits and costs before moving towards this technology. The cloud computing platform is a great way for a company to carry out business without having to invest in the development and maintenance of IT infrastructure. In addition to allowing businesses to sell products online without having to rent an office, e-commerce also provides businesses with the flexibility to build their brand and sell products online, but there are still expenses that must be incurred in terms of hardware and software. As a result of the development of cloud computing, many more E-commerce companies are able to benefit from the advantages of this technology (Almarabeh, & Majdalawi, 2019).

3.2.1 E-Commerce Cloud Benefits

i. Cost saving: This method reduces the time and cost associated with IT implementation, installation, and maintenance.
ii. Scalability: As the business demands change constantly, it is necessary to adapt to those changes. In order to adapt to these rapid changes, cloud computing allows IT systems to be adapted quickly.
iii. Efficiency: In order to get benefits from their research and development efforts, IT organizations are able to dedicate their time and resources to their business.
iv. Availability and Mobility: With the advent of smartphones, consumers can access products and services whenever and wherever they want.

v. Easy management: A number of processes have been simplified, such as the maintenance of hardware, software, and even infrastructure.

3.2.2 E-Commerce Cloud Challenges

i. Security: As a matter of fact, it is one of the biggest challenges, since data is vulnerable to being accessed, modified, or even destroyed during processing or transmission. As of right now, there are no solutions that are effective when it comes to protecting programs and data and it has been difficult to do so.
ii. Data Privacy: In spite of the fact that information about the clients has always been a concern, there is no technical solution for protecting it as of yet.
iii. Data Storage: Cloud clients worry that they will not be able to control the location in which their data is stored while using cloud services.
iv. Trust: There are several ways to define trust, but as a simple definition one could use "the degree to which something that is being done is considered secure, such as software, a device, a server, or any information they deliver." It was difficult in the past for consumers to tell the difference between good and bad E-commerce websites. As a result of this situation, enterprises and clients are not encouraged to move to the cloud in the near future.
v. Connectivity: For the cloud application to work, the user must have an Internet connection in order to be able to access shared information or resources.
vi. Service standards issues: It can be very difficult for enterprises to obtain information regarding the mode of operation, the technology employed, and the staff situation of a cloud environment, which gives them reasons to worry about implementing cloud technologies without knowing these details.

3.3 Banking

In the latest era of rapidly changing technology, changing consumer behaviors, new regulations, and intensified competition, the banking industry has undergone a series of changes which have turned it into a highly turbulent and dynamic business environment. A large number of users are utilizing mobile devices as a result of the explosive growth of information systems, which has resulted in a gradual shift from legacy in-house systems toward web-based ones, with many using them to gain access to data. This trend is also accelerating due to the diffusion of cloud computing, specifically cloud CRM. In spite of the substantial influence of CRM, cloud CRM is becoming one of the most widely used applications today. In order to demonstrate this, Salesforce.com, one of the most influential companies in the world, launched its CRM software on its website with a market value of 50 billion dollars and a resource value of 500 million US dollars, and there are other providers (i.e., IBM Congnos, NetSuite, Microsoft Dynamics CRM, etc.). A cloud-based CRM solution allows organizations of all sizes to test and implement it much more quickly than traditional CRM modules. A larger advantage of cloud-based CRM is that it allows financial institutions to manage their data more effectively, allowing them to provide better, faster, and more efficient customer service. A bank's cloud strategy and infrastructure should also be based on security and trust (Nguyen & Ali, 2021).

3.3.1 Banking Cloud Benefits

i. Immediate “Savings” Benefits: Many institutions may be able to substantially lower their upfront costs with the use of a cloud CRM solution, based on a combination of lower hardware and software infrastructure, networking, and more complex operating systems as well as maintenance and support services. There is also a tendency for employees to be trained quickly, and it might also be possible to implement and share projects online by using the Internet. Consequently, both their management and IT costs, which constitute a considerable portion of their total costs, are maximized.

ii. User-Driven Customization: In light of the lack of infrastructure, it is not necessary to determine the level of customization per user. The cloud-based CRM vendors provide limited customization options that are built into the CRM platform, allowing this initiative to be flexible and customizable for the end user, who can personalize messages and logos and acclimate the user experience in a manner that suits their needs.

iii. Accessibility: On the basis of the cloud CRM system, sales and marketing departments tend to have direct access and simultaneous access to data when and where they need it regardless of their location. Also, it gives businesses a real edge by providing the possibility for a global team or an independent workforce to access the platform easily, which helps companies to reach new heights of success.

iv. Structured Data and Automated Salesforce: It is believed that cloud CRM applications are capable of structuring customer data in a way that facilitates business's team to demonstrate a target segment and customize targeted marketing campaigns to suit customer's needs. These capabilities will make it possible for businesses to share better insights with customers and to act fast and efficiently.

v. Actionable Customer Information: All departments, particularly marketing and sales, have the ability to easily access their CRM systems via the cloud so that they can obtain greater insight into where their customers are in the buying cycle and be able to respond more quickly and effectively.

vi. Increased Productivity: SME's should take advantage of a cloud based CRM service in order to increase their efficiency. There are many instances in which employees work away from an office desk, servers or desktops and are not tethered to one office desk or server. By doing this, they will not have to wait until they get home to find out information about those who are in need of their services. In order for a company to be more productive and efficient, such employees may be able to deliver more frequent and actionable insights to clients.

3.3.2 Banking Cloud Challenges

i. Security: The information that companies have today is one of their most valuable assets. Those who are using cloud CRM are particularly concerned about this issue, as the data and applications are located in the cloud. In order to meet the security requirements of the cloud, a cloud service provider needs to be involved. Especially for a banking industry, where customer information is at the heart of transactions, this industry has a great deal of sensitivity attached to it.

ii. Downtime Issue: An outage of the cloud CRM application may not only have a direct financial impact on the enterprise, but it may also lead to customers questioning the service as to its reliability in the long run. This can result in the customer discontinuing to use the service and choosing another service provider, due to the fact that their current service provider is not reliable, which can result in them stopping to use the service.

iii. System Integration: As a result of cloud CRM, customers are identified and retained using the integration approach. In order to accomplish this, it is imperative that departments and geographies work together smoothly. When departments or geographies are not integrated properly, it can lead to a significant increase in manual processes, data inaccuracies, and can translate into a difficult time obtaining reports.

iv. Privacy Concern: Data privacy laws differ from one country to another in terms of their implementation when it comes to the protection of personal information. In order to protect the interests of national security, the US government agencies have substantial power over the acquisition of confidential data, while in Europe, the government agencies are more restrained and are partial to the protection of privacy rights. Due to the nature of cloud technology, the storage infrastructure is divided across a variety of geographical locations around the world, posing a potential security concern for users who may reside in those areas.

3.4 Construction Industry

In the construction industry, there is an immense amount of data generated continually as the project moves forward, as heterogeneous data is continuously collected. There are usually several different silos of data stored for different stages of a project, such as the server or desktop of the team, the computer of the individual, the laptop, the smartphone, etc. In order to coordinate the overall project, it is essential to integrate the data since the absence of a holistic view of the data often results in mistakes that could prevent the project from moving forward as well as damage the project's performance and profitability. Information and Communication Technologies (ICT) are traditionally used for a company's solutions in storing, processing, and analyzing the data it receives from its subcontractors by acquiring a high-end computing system. Pay as you go computing is a new technology that allows cloud computing facilities to be offered at an affordable and scalable cost. As a result, cloud computing functionality is suitable for SME's because it offers a wide variety of features. Construction is one of the industries that are experiencing significant challenges with the use of ICT due in part to the application of cloud computing, which eliminates most of the cost of acquiring, installing, and maintaining computing facilities, which has resulted in the slow adoption of ICT within this industry (Bello, Oyedele, Akinade, Bilal, Delgado, Akanbi & Owolabi, 2021).

3.4.1 Construction Cloud Benefits

i. Economic benefits: Since the low profit margin of construction companies makes it difficult for them to adopt IT solutions, the cost of adopting IT solutions is a significant hurdle. In order to lower infrastructure and operational costs, construction companies are seeking new methods. Consequently, there are some concerns that the industry doesn't have the buoyancy to keep up with the huge IT infrastructure, which requires specialized human resources and training to be maintained. As a result of the use of cloud computing technologies, construction businesses, especially small to medium size industries, are now able to access high end computing infrastructure and applications for a fraction of the price of traditional methods. Thus, by reducing the overall cost of project delivery, construction companies will be able to gain a competitive advantage and gain an operational advantage. Construction companies can operate more efficiently as a result of the simple nature of cloud computing technology and the fact that ownership and operational costs are eliminated.

ii. On-demand scalability of computing resources: In cloud computing, IT resources can be purchased by construction companies based on their particular requirements at that particular time. There is no longer any economic reason to tie up capital in computing facilities for short-term needs for higher capacity infrastructure in order to meet short-term needs for higher performance infrastructure. It is possible that due to the unexpected demand for infrastructure, it may even be impossible to purchase and install it. Now, construction professionals will be able to take advantage of cloud computing services that offer quality hardware and powerful CPUs and GPUs for an affordable price. Without a big initial investment, SMEs will compete with large companies.

iii. Secured platform: Security measures in the cloud have matured in recent years, and among the most popular security measures include; encryption, the use of up-to-date security software, cyber insurance coverage, security audits, and so on. The construction industry is highly fragmented and there are literally no SMEs that can afford to have the same level of data security found in the cloud in their internal infrastructure as they do in the cloud. The security threats affecting on-premise construction data, such as Crypto Locker and the associated ransom demand, have further compelled the use of cloud storage for safekeeping construction data, thus necessitating using cloud storage to keep construction data safe. Construction companies are also experiencing a very high cost for implementing systems that are highly available and that match the 99.99% service level agreements and uptime that cloud providers offer.

iv. Massive storage: As the owner's building idea is transformed into a functional design by the professionals, there is a huge amount of data generated throughout the construction process. IoT, augmented reality, 5D BIM, and other emerging technologies generate a huge amount of data continuously. In order to store aerial imagery of a site on a typical computer, it will take hundreds of gigabytes of space. Because of the volume and the equipment infrastructure required to store construction data on-site, it has been difficult to store this data on-site. The data can also be stored and retrieved remotely with cloud storage, which does not restrict space or time like on-site storage. The construction industry has great benefits from cloud storage.

v. Facilitating collaborative practice: Several project teams execute construction projects, each with its own business reporting model stored in a different silo. It is difficult for the stakeholders in the industry to make timely and critical decisions based on scattered data. Due to this, projects have been delayed, costs have risen, and ROI has been decreased. An end-to-end solution based on cloud technology helps the construction industry become more productive and organized. Using up-to-date project data and the ability to keep the project team organized and well-integrated, it is possible to have a greater level of participation by the construction workers.

3.4.2 Construction Cloud Challenges

i. Latency: There may be some time-sensitive construction applications that cannot be addressed by cloud adoption due to the limited transfer rate and response time. Possibly there is a problem with the software or with the network. By using distributed cloud architecture, software designers can make sure that latency to a specific application is low through appropriate software design techniques. Since cloud applications scale well in cloud infrastructure, they have recently been designed as cloud-native applications. The construction companies can also be connected to the service provider with dedicated links if they wish to avoid the delays that may result from using the Internet as a transport medium. By selecting service providers with closer data centers, companies in the construction industry may also be able to avoid delays because the network performance will be improved due to fewer hops between the service provider and the customer. Application Performance Monitoring (APM) tools are used to identify the cause of latency problems and to implement solutions in order to be able to resolve them faster. Identifying the source of latency problems early in the process is crucial to implementing solutions on time.

ii. Trust, data privacy and security: A fluid security perimeter is increasing the vulnerability associated with the adoption of cloud technology. Usually, business partners do not readily share private information with third parties, such as project costs. In the construction industry, it is understandable that companies are concerned about the cost and security of storing their financial and design information on shared resources. It is more likely that the anxiety is the result of the perception that certain unknown people may have access to the data, in most cases. Data chain integrity is most important to the client. Client devices are most often used by employees for work, so most data leaks from the cloud occur there. There is a possibility of infecting or hacking these own devices. A data protection strategy should be implemented by construction companies in order to prevent data leaks. In rare cases of data bridges from service providers, however, cloud service providers may have to adhere to privacy and security laws in order to ensure compliance.

iii. Data availability: Technology cannot be perpetual, so downtime is not uncommon with cloud-based technologies. Their resources may have been unexpectedly shutdown by a cloud provider. As a result, how will the building data be used once the building data is unavailable? Further, is there a project for the construction of the building? A construction project is made more difficult when this happens. There is a 99.99% availability guarantee as part of the service level agreement between cloud providers and their clients. Moreover, cloud technology development is resulting in open-source tools that allow for the exchange of data between cloud providers, and the creation of standards for the representation of data as well. Data can be exchanged between cloud providers if one provider is unavoidably unavailable, so that lock-in issues will not occur in the event of an unavoidable outage.

iv. Data governance: In construction projects, there are many professionals involved, so the contractual relationship between them must be clearly defined. Considering this, it may be considered that the data belongs to all since it is being contributed. Since all parties have access to the data and are responsible for updating it continuously, the question of who owns the data may arise. Additionally, information exchange requirements among the members of the construction team must be considered, as well as the relationship between them. Do the building owner and the engineer have access to data? Data management and production stakeholders may need different access levels. In order to harness the power of cloud computing, applications should implement appropriate access control features rather than leaving this responsibility to cloud service providers.

v. Cost implication of long-term use: According to the type of deployment, the accumulated cost of cloud infrastructure could be substantial. Since cloud researchers have focused on incorporating market value and creating personalized pricing methods, cloud SaaS pricing has become more complex than it was at the inception of the industry due to efforts made by cloud researchers.The current cost of cloud services is expected to reduce with further improvements in ICT technologies, even though assured patronage in the form of reservations provides a good deal. In addition, even within the same construction company, the cost implication depends on the type of cloud deployment. Performing machine learning and analytics on projects could be expensive if high-end resources like GPUs are rented. The installation of a cloud deployment model might need to be analyzed individually by each construction company before it is chosen.

vi. High chances for scoring dark data: Data can be stored in the cloud easily and inexpensively. As a result, dark data is being stored more frequently. Using dark data means acquiring data without processing it or analyzing it for any meaningful purpose. Usually, sensor generation capacity outweighs the analytical capacity, which causes a large proportion of data that is generated by sensors to never be utilized because the generation capacity of sensors surpasses the analytics capability. Regulatory policies are usually what drive the collection of most data. Storage of this data was sometimes based on the idea that it could be used in analytics in the future even though it is not currently usable. Usually, data values are time-based, since data that is eventually useless, redundant, or obsolete due to its inability to be processed fast enough. It is becoming more and more common for money to be spent on storing irrelevant data, as a result of which there is an increasing amount of energy being consumed in the storage of dark data.

4. Security Challenges in Cloud Computing

It is undeniable that Cloud Computing has several advantages, but it also poses some security challenges. The following are some of the security challenges associated with cloud computing.

i. Data Loss: Cloud Computing is prone to data loss. The term Data Leakage can also refer to this phenomenon. The sensitive data users hold is in the hands of Someone else, and their database is not entirely under their control. As a result, hackers may be able to access user’s sensitive data or personal files if they manage to break the security of cloud services.

ii. Interference of Hackers and Insecure API’s: Cloud computing and its services are all part of the Internet, as everyone know. Furthermore, APIs are the easiest way to communicate with Clouds. Consequently, external users should be protected from access to interfaces and APIs. The public domain is also limited in cloud computing. In Cloud Computing, there is a vulnerability in that these services may be accessed by third parties. As a result, hackers may be able to access the data easily through these services.

iii. User Account Hijacking: Cloud computing security is most vulnerable to account hijacking. A hacker steals an account or an organization if they somehow gain access to it. In that case, the hacker can perform Unauthorized Activities with full authority.

iv. Changing Service Provider: Cloud computing also faces the issue of vendor lock-in. Shifting from one vendor to another can lead to a variety of problems for many organizations. It may happen that an organization wishes to switch from AWS Cloud to Google Cloud Service and faces various problems regarding shifting all data, as well as differing techniques and functions between the two clouds. Additionally, there is a possibility that AWS's charges differ from Google Cloud's.

v. Lack of Skill: IT companies that do not have skilled employees face problems such as shifting to another service provider, needing extra features, and learning how to use features. To work with cloud computing, users need a skilled individual.

vi. Denial of Service (DoS) attack: Too much traffic can cause this type of attack. Banks, governments, and other large organizations are the most commonly targeted by DoS attacks. DoS attacks result in the loss of data. Data recovery requires both time and money, so it requires a great deal of money.

5. Conclusions

By utilizing cloud computing, traditional computing approaches have been completely revolutionized and have now been replaced with a new type of computing model that is more innovative, optimized, and cost-effective. In the world of information technology, it is a game changer and it will lead the IT sector to a greater level of modernization than ever before. The world of IT has become a much more exciting place with the advent of the Internet and the Cloud. While there are many advantages to the cloud, there are also some challenges that need to be addressed in regard to secure information sharing. A lot of recent research is being done in relation to the security of Cloud computing, with a host of mechanisms being developed. It is the purpose of this paper to discuss the implementation of cloud computing in various sectors as well as focusing on the security issues that are associated with cloud computing. In spite of that, there is still a need to enhance current security measures in order to make cloud computing more secure. The conclusion I have drawn from all this is that despite the fact that cloud computing has many advantages, it suggests that you only adopt cloud computing services after you have assessed all the main security issues involved in cloud computing.

Acknowledgments

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Systems & Network Security Project. This work was supported by University Utara Malaysia.

References

Tadapaneni, N. R. (2020). Cloud computing security challenges. International journal of Innovations in Engineering research and Technology, 6(7).

Sureshkumar, V., & Baranidharan, B. (2021, July). A study of the cloud security attacks and threats. In Journal of Physics: Conference Series (Vol. 1964, No. 4, p. 042061). IOP Publishing.

Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: a survey. Journal of healthcare engineering, 2019.

AlMendah, O. M., & Alzahrani, S. M. (2021). Cloud and edge computing security challenges, demands, known threats, and vulnerabilities. Academic Journal of Research and Scientific Publishing, 2(21), 156-175.

Vistro, D. M., Rehman, A. U., Mehmood, S., Idrees, M., & Munawar, A. (2020). A Literature Review on Security Issues in Cloud Computing: Opportunities and Challenges. J. Crit. Rev, 7, 1446-1455.

Talha, M., Sohail, M., & Hajji, H. (2020). Analysis of research on amazon AWS cloud computing seller data security. International Journal of Research in Engineering Innovation, 4(3), 131-136.

Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. Materials Today: Proceedings, 51, 2172-2175.

Chinedu, P. U., Nwankwo, W., Aliu, D., Shaba, S. M., & Momoh, M. O. (2020). Cloud Security Concerns: Assessing the Fears of Service Adoption. Archive of Science & Technology, 1(2), 164-174.

George Amalarethinam, D. I., & Rajakumari, S. (2019). A survey on security challenges in cloud computing.

Jabbar, J., Mehmood, H., & Malik, H. (2020). Security of cloud computing: belongings for the generations. International Journal of Engineering & Technology, 9(2), 454-457.

Altobishi, T., Podruzsik, S., & Gabor, S. Z. (2018, October). A review of the security challenges in the cloud computing. In Proceedings of the 7th International Conference on Research in Science and Technology, Munich (pp. 19-21).

Suthar, F., Khanna, S., & Patel, J. (2019). A Survey on Cloud Security Issues. International Journal of Computer Sciences and Engineering (IJCSE), 7(3), 120-123.

Mandal, S., & Khan, D. A. (2020). A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic.

Yan, L., Hao, X., Cheng, Z., & Zhou, R. (2018, April). Cloud computing security and privacy. In Proceedings of the 2018 international conference on big data and computing (pp. 119-123).

Kumar, Y. K., & Shafi, R. M. (2020). An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem. International Journal of Electrical and Computer Engineering, 10(1), 530.

Khandelwal, M., & Saini, H. (2019, October). Review on Security Challenges of Cloud Computing. In International Conference on Advancements in Computing & Management (ICACM-2019).

Kumar, M. (2020). STUDY ON SECURITY CHALLENGES IN CLOUD COMPUTING. distributed computing, 29(02), 4789-4797.

Kaur, A., & Singh, G. (2020). Cloud Computing Security Issues and Challenges.

Ahmed, A. A., & Hussan, M. T. (2018). Cloud computing: study of security issues and research challenges. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 7(4), 13-23.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

Almarabeh, T., & Majdalawi, Y. K. (2019). Cloud Computing of E-commerce. Modern Applied Science, 13(1), 27-35.

Nguyen, N. D. K., & Ali, I. (2021). Implementation of Cloud Customer Relationship Management in Banking Sector: Strategies, Benefits and Challenges. International Journal of Electronics and Communication Engineering, 15(6), 242-247.

El-Attar, N. E., & Awad, W. A. (2019). Integrated Learning Approaches Based on Cloud Computing for Personalizing e-Learning Environment. International Journal of Web-Based Learning and Teaching Technologies, 14(2).

Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., ... & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. Automation in Construction, 122, 103441.