پنجمین کنفرانس بین المللی مطالعات بین رشته ای در مدیریت و مهندسی
۱۴ تیر ۱۴۰۱ | محل برگزاری: دانشگاه تهران
5th International Conference on Interdisciplinary Studies in Management & Engineering (ICISME-2022)
5 July 2022 | University of Tehran
OxfordCert Universal

A Review on Cloud Computing: threats, issues and the factors influencing its acceptance in businesses

Athena Farukh
MSc of Information Technology Management, Islamic Azad University, Tehran. Iran
athena.farukh@gmail.com

Abstract:
Due to the increasing use of cloud computing in organizations as well as in everyday life, in this article we have tried to provide a comprehensive review of the research literature and update the threats and challenges. The amount of research conducted on the above topics is from the years 2017 to 2022. In this review, we aim to determine the most discussed topics along with relevant theories, as well as the factors that influence small and medium enterprises' adoption of cloud computing. This paper provides an investigation of 27 conference papers, articles, review papers, and books from popular publications like Springer, Elsevier, IEEE, EDP Sciences, and Journals. The synthesized outcome of the literature identifies benefits, responsibilities, threats, classification of cloud security issues and factors influencing the decision and adoption of cloud computing in Small and Medium Enterprises that can help researchers better understand the elements of cloud computing and in line with new research and discovery of factors take a new step. Findings in this study indicate that influential factors such as "cost" and "flexibility" can be applied to multiple benefits of cloud computing, both tangible and intangible. To facilitate the business aspect of cloud computing, researchers can address gaps in policy, risks, and service models. SME[1]s' cloud computing adoption can be guided by the insights found in this study into cloud computing services explored, and other key research issues concerning cloud computing adoption in SMEs that will guide future research.

Keywords:
Cloud computing, cloud computing threats and issues, Cloud Computing adoption, SMEs.

Introduction:

Cloud computing refers to the act of storing or accessing data and programs over the Internet rather than through our computers' hard drives. Among experts, the definition of cloud computing put forward by the National Institute of Standards and Technology (NIST) has become the most commonly accepted one (Sunyaev, 2020). According to this definition, cloud computing is a method of distributing computing resources on-demand via the Internet or a network to provide ubiquitous, convenient access whenever and wherever it is desired (Mell et al, 2011, as cited in Sunyaev, 2020, p. 198). Network access, server access, storage access, or application access is included in this definition. Our daily lives are dominated by cloud computing in one way or another without even recognizing it, such as Microsoft Office 365, Gmail, Dropbox, etc. (Kumar et al, 2018). Thus, cloud computing is currently being used by most small and large industries to handle storage, traffic, and hardware

[1] Small and Medium Enterprises

requirements (Srivastava et al, 2018),and multiple industries are now leveraging cloud services to reduce costs, expand their businesses, and even decrease their carbon footprints (Matthew et al, 2014, as cited in Stephen et al, 2019, p. 31). As a result, it is clear that cloud computing has a significant impact on society and business (Srivastava et al, 2018).

Among the most exciting innovations in recent history, cloud computing has captivated the attention of tech enthusiasts worldwide. Despite Cloud Computing's numerous advantages, including scalability, quick flexibility, measurable services, and, most importantly, cost savings for organizations, it also presents a number of security risks no enterprise can ignore (Vinoth et al, 2021) data security, lack of resources and expertise etc. (Kumar et al, 2018). Fig. 1 shows advantages of cloud computing. In the absence of solid security guidelines, companies seem reluctant to utilize an otherwise powerful cloud computing environment due to the vast array of vulnerabilities that cloud computing systems present (Scalera et al, 2014, as cited in Vinoth et al, 2021, p.2).

Figure 1. Advantages of Cloud computing

Characteristics of cloud computing technology:

According to NIST's definition of cloud computing, this cloud model consists of five basic actors (Fig. 2), three service models, and four deployment models.Figure 2 shows an overview of four cloud deployment models, three service models, and five actors as described by the NIST definition of cloud computing (Grance et al, 2011,as cited in Rashid et al, 2019, p.421).

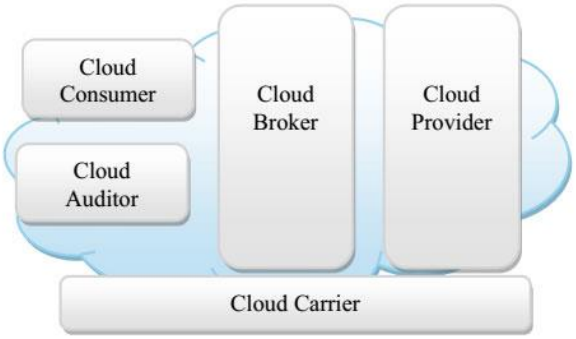

Figure 2. Cloud Computing Actors (Kumaret al, 2017)

Cloud consumer or cloud service consumer (CSC) use cloud services provided by cloud providers and pay for the service based upon usage. A **cloud provider** or cloud service provider (CSP) provides cloud services to the CSC. **Cloud auditors** conduct independent assessments of cloud services, information system operations, performance, and security of cloud implementations. **Cloud broker**

interacts between CSP and CSC to make the business happen. Who provides the connectivity and cloud services from CSP to CSC is the **Cloud carrier** (Kumaret al, 2017).

Cloud Computing Service Delivery Models:

There are three major types of cloud services (see Figure 3), each organized hierarchically according to the degree of abstraction of the capability offered and the provider's service model. The three models are:

(1) Infrastructure as a Service (IaaS),
(2) Platform as a Service (PaaS), and
(3) Software as a Service (SaaS) (Mell et al, 2011, as cited in Sunyaev, 2020, p. 203)

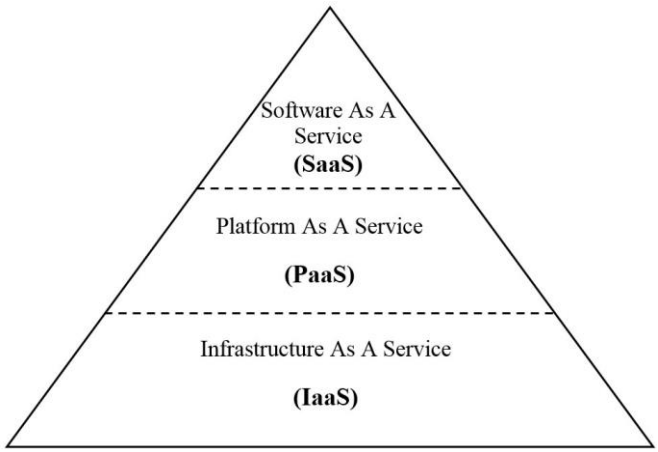

Figure 3. Cloud service models depicted as a pyramid

A) Software as a Service (SaaS)
According to this model, cloud service providers run and maintain application software, operating systems, and other resources. The SaaS model is viewed by the customer as a web-based application interface that is accessed via a web browser to deliver services over the internet. Various devices like smartphones and laptops can be used to access hosted applications such as Gmail and Google Docs. The advantage of SaaS over traditional software is that customers do not have to purchase licenses, install software, upgrade, maintain or run it on their own computers (Joint et al, 2011, as cited in Rashid et al, 2019, p. 423). Furthermore, it is multitenant efficient, configurable, and scalable (Goncalves et al, 2011, as cited in Rashid et al, 2019, p. 423).

B) Platform as a Service (PaaS)
The service provided by this cloud computing provider is more advanced. An PaaS provider offers runs and maintains both system software (i.e., the operating system) and other computing resources. Applications are designed, developed, and hosted by PaaS services. Collaboration, DB integration, security, web services integration, scaling, etc. are also available. There's no need for users to acquire their own hardware and software or to hire experts to manage their resources. In addition to providing flexibility in installing software on the system, PaaS offers scalability. Interoperability and portability are limitations of PaaS. By purchasing access to the platforms, consumers can deploy applications and software in the

cloud. Examples of PaaS solutions include Rackspace Cloud Sites, Salesforce.com's Force.com and Google App Engine, and Microsoft Azure (Rashid et al, 2019).

C) Infrastructure as a Service (IaaS)
An IaaS provider provides a set of virtualized computing resources in the cloud, such as CPU, Memory, OS, application software, etc. By incorporating virtualization technology into IaaS, customers can easily provision and release logical resources as needed. Infrastructure as a service is offered by many companies, including Rackspace Cloud Servers, Google, Amazon EC2, IBM, and Verizon (Rashid et al, 2019).

Table 1 summarizes the Benefits of Cloud Computing Services Delivery Models.

Table 1. Benefits of Cloud Computing Services Delivery Models

Cloud Computing Service Delivery Models	SaaS	PaaS	IaaS
Benefits of Solutions	Rapid Scalability	Community	Reduces cost of capital expenditures
	Accessibility from any location with Internet	No more upgrades	Users pay for the service they want
	Eliminates infrastructure concerns	Lower cost	Access to enterprise-grade IT resources and infrastructure
	Custom levels of service offerings	Simplified deployment	Users can scale up and scale down the resources based on their requirements at any time
	Bundled maintenance and Support		

A cloud computing delivery model can provide nine services, namely Application, Data, Runtime, Middleware, Operating System, Virtualization, Server, Storage and Networking which are the components in the traditional computing. CSPs (shown in boldface) and CSCs clearly distinguish the role of services each model offers as shown in Tabel 2. The CSP only provides the infrastructure like servers, storage, networks, and virtualization in IaaS. The CSC manages applications, data, runtime, middleware, and operating systems. Typically, CSC manages only the application and data, while CSP manages the rest of the services. Each of the nine SaaS services is provided by the CSP. Cloud deployment models raise security issues as well (Kumar et al, 2017).

Table 2. Services Provided by Delivery Models and the Responsibility

Services Provided by Delivery Models	**IaaS**	**PaaS**	**SaaS**
Application	CSC	CSC	**CSP**
Data	CSC	CSC	**CSP**
Runtime	CSC	**CSP**	**CSP**
Middleware	CSC	**CSP**	**CSP**
Operating System	CSC	**CSP**	**CSP**
Virtualization	**CSP**	**CSP**	**CSP**
Server	**CSP**	**CSP**	**CSP**
Storage	**CSP**	**CSP**	**CSP**
Networking	**CSP**	**CSP**	**CSP**

Cloud Computing Deployment Models:

Cloud computing consists of four main types: public cloud, private cloud, community cloud, and hybrid cloud. Cloud service providers (CSP) decide what type of cloud users can access. Figure 3 shows the deployment model of cloud computing (Namasudra, 2018).

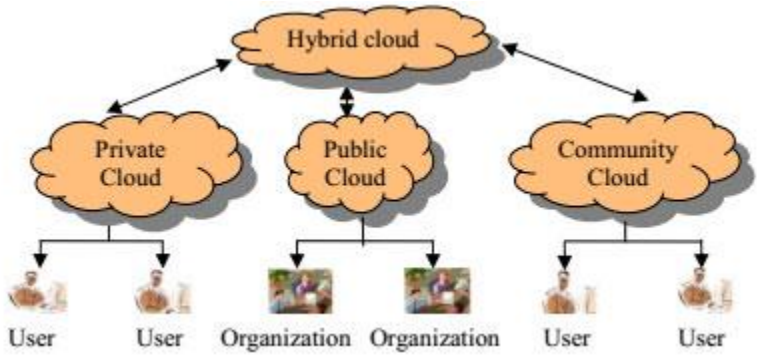

Figure 4. Deployment model of cloud computing

a. Private Cloud:

A private cloud is setup and operated exclusively for a single organization; third parties, however, can manage the cloud on behalf of the owner (Verma et al, 2011, as cited in Odun-Ayo et al, 2018). You can run a private cloud on-premises or off-premises. Private cloud has privacy, security and control.In addition, the cost and energy efficiency are excellent (Verma et al, 2011, as cited in Odun-Ayo et al, 2018). Clouds in the private sector are limited in scalability and restricted to a particular area (Odun-Ayo et al, 2018).

b. Public Cloud

The infrastructure and data centers for these services are owned and operated by a CSP. Businesses can access services on-demand and pay-as-you-go through on-premise infrastructure (Verma et al, 2011, as cited in Odun-Ayo et al, 2018). A browser connects organizations and users to a public network to access services (Khan et al, 2015 and Bhardwaj et al, 2010 as cited in Odun-Ayo et al, 2018). Despite being location independent, reliable, and highly scalable, public clouds are not secure and can't be customized (Verma et al, 2011, as cited in Odun-Ayo et al, 2018).

c. Community Cloud

Several organizations or organizations sharing a common interest host the community cloud. Universities, for example, use it for teaching and researching. Cloud management can be performed on-site or off-site, and organizations can also outsource the daily operation of the system to a third party (Verma et al, 2011, as cited in Odun-Ayo et al, 2018).

d. Hybrid Cloud

In a hybrid cloud, you can combine all or some of the deployment types, for example, private, public, and community clouds. The majority of activities are conducted in a private cloud, while less essential operations are outsourced to a public cloud. All the clouds remain independent entities, but they are interconnected by standard technology (Verma et al, 2011, as cited in Odun-Ayo et al, 2018). There are security and network issues with hybrid clouds (Odun-Ayo et al, 2018).

A comparison of public clouds, private clouds, and hybrid clouds is also provided in Table 2 (Tabrizchi et al, 2020).

Table 3. The pros and cons of public, private, and hybrid clouds

Cloud development models	Advantages	Disadvantages
Public cloud	Scalability and reliability with on-demand resources	Can be unreliable
	Easy to use	Less secure
Private cloud	Organization-specifc	More costly
	Customizable	Requires IT expertise
Hybrid cloud	Flexible infrastructure	Lack of visibility
	Cost controls	Potential challenges in application and data integration
	Faster speeds	

Figure 6 shows an overview of cloud computing configuration based on the NIST definition (Csrc.nist.gov, 2018, as cited in Tabrizchi et al, 2020).

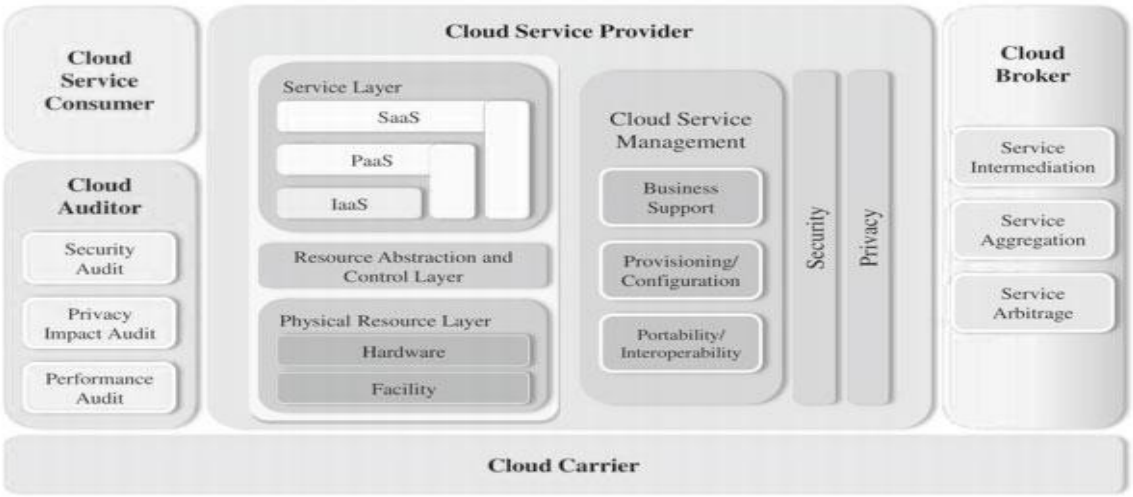

Figure 5. NIST cloud computing confguration

Essential Characteristics Of Cloud Computing:

Several interesting characteristics make cloud computing systems a promising option for future IT applications and services. We describe below the five essential characteristics of cloud computing systems as defined the National Institute of Standards and Technology (NIST) (Rashid et al, 2019).

On-demand self-service:

On-demand self-service allows cloud customers to provision resources like server time and network storage automatically and almost immediately (Mell and Grance 2011 as cited in Sunyaev, 2020, p. 198). It is noteworthy that cloud providers are able to handle this automatically without any human intervention. Customer licensing can thus be adjusted according to their current requirements, such as increasing or decreasing computing, storage, or application licenses (Sunyaev, 2020).

Broad Network Access (mobility) :

Standard mechanisms allow clients (including tablets, laptops, workstations, and mobiles) to access the cloud (Odun-Ayo et al, 2018).

Rapid Elasticity:

Resource provisioning and release can be done rapidly and elastically based on the demand of the consumer (Rashid et al, 2019). It is crucial that the cloud architecture is flexible enough to scale up and down seamlessly, ensuring that the consumer sees the capabilities as unlimited (Odun-Ayo et al, 2018).

Measured Services:

The CSPs monitor, control, and optimize cloud resources and services based on a pay-per-use model (Rashid et al, 2019) in order to ensure optimal resource utilization and proactive forecasting. An embedded metering capability achieves this (Odun-Ayo et al, 2018).

Resource pooling:

Multitenant models pool resources to provide services to multiple clients. To satisfying every peculiarity provision of customers, services should be able to customized (Odun-Ayo et al, 2018). According to that customers has not any control or knowledge about their location, these resources are independent of location (Rashid et al, 2019). Multitenancy, Scalability, Reliability, Economies of scale, Customization, Efficient resource utilization and Virtualization are other cloud computing characteristics (Rashid et al, 2019).

Data Security Issues or Challenges

As cloud service providers (CSPs) maintain data centers in various geographically distributed locations, the users have no idea where their sensitive data is located, posing several security challenges and threats (Subramanian et al, 2018). In addition to traditional security checks, cloud computing data must be protected with additional security methods. Due to the rapid spread of threats via virtualized environments, traditional security techniques like firewalls, host-based antivirus software, and intrusion detection systems cannot offer adequate security in virtualized systems (Subramanian et al, 2018). Secure cloud architecture is required for the location of the ultra reports. Also, the demand nodule, an access part of an enormous relevant information location has to be safe as well (Kollolu, R., 2020). As a cloud service provider, one of the most important tasks is to ensure that the services available for data readiness are easily accessible and can be relied upon by users for the continuity of their business (Wang, 2017,as cited in Abdurachman et al, 2019).

Cloud computing threats and risks:

According to Table 4, these articles are pertaining to the types of threats or obstacles that can arise in the cloud computing environment. Types of threats are collected based on the reference article and from the year 2018 to 2022.

Table 4. Type of threats on cloud computing

No.	Type of threat on cloud computing	Cloud service resources	Reference
1	Loss of Governance, Lock-In, Isolation Failure, Malicious Insider, Insecure or Incomplete Data Deletion, Security, Management Interface Compromise, Costing Model, Charging Model	Data/ Application Data Data Infrastructure Data - - - -	Pallathadka et al, 2022

2	Multitenancy, Loss of Control, Location Intransparency, Lack of Availability, Compromised Ease of Use, Vendor Lock-In, Limited Service Continuity, Communication Issues, Data Breaches, Data Loss, Data Scavenging, Insufficient Identity, Credentials, and Access Management, Insecure Interfaces and APIs, System Vulnerabilities, Shared Technology Vulnerabilities	Infrastructure - - - - Data - Application Data Data Data Data Application Application Infrastructure	Sunyaev, 2020
3	Data Privacy Issues, Internet Quality Issues, Applications Issues, Personal Devices Issues, CCE (Cloud Computing Environment)	Data Infrastructure Application - Infrastructure	Alashhab et al, 2020
4	Data breaches, Hacked interface and application program interfaces, Account hijacking, Malicious insiders, Distributed denial-of-service attacks	Data Application Application Data -	Tabrizchi et al, 2020
5	Privacy data security, Access control and identity authentication, Virtualization security, Multi-tenant and cross-domain sharing, Advanced Persistent Threat (APT), System security vulnerability, Insider threat, Wrong application of cloud service, Service availability	Data - Infrastructure Infrastructure - Application Data Application Service in general	Sun, 2020
6	Absence of visibility and control over assets, Some cloud service providers may not fulfll security measures according to the industry protocols, Issues of data privacy, Event log management and notification, User access control management, Security risk due to vendor lock-in	- - Data - - Data	Verma et al, 2020
7	Data Protection, Data Recovery and Availability, Management Capabilities, Regulatory and Compliance Restrictions	Data Data - -	Rashid et al, 2019
8	Reliability, Privacy, Bandwidth, Availability, Integrity, Denial of Service (DoS), Distributed Denial of Service (DDoS), Authentication, Access control	Application Data Infrastructure - Data - - Application -	Amalarethinam et al, 2019

9	Data breaches, Compromised credentials and broken authentication, Hacked interface and Application Program Interfaces, Exploited system vulnerabilities, Account hijacking, Malicious insiders, The Advanced Persistent Threat(APT) parasite, Permanent data loss, Inadequate diligence, Cloud service abuses, Denial-of-Service(DoS) attacks, Shared technology, shared dangers	Data Application Application Application Application Data - Data - - Service in general Infrastructure	Subramanian et al, 2018
10	Availability, Confidentiality, Access control, Data related issues, Storage related issues, Policy issues, Security issues, Trust issues, Legal aspects, Attacks on the cloud environment	- Application Infrastructure Data Infrastructure Infrastructure - Application Data -	Namasudra, 2018
11	CIA Related Security Issues, AAC Related Security Issues, Broken Authentication Session & Access Other Data Related Security Issues	Data Data Data Data	Kumar et al, 2017

A threat is anything that is capable of damaging a computer system in a serious way. With a large number of hardware and software components, cloud computing suffers from a wide range of security concerns. Computer systems, networks, and other communication infrastructures can be attacked due to threats. Viruses, trojans, back doors, and outright hacking attacks can all pose threats. Because each kind of cloud, whether public, private, or hybrid, provides a flexible management model and cost efficiency, privacy of data and security of software have become increasingly important concerns (Tabrizchi et al, 2020).

According to Table 4, the threats related to cloud services within the cloud computing environment to better understand the relationships between them are shown. Most papers contain more than one type of threat, even the same one appears in several papers. The grouping relies on the definition and understanding of the threat. Due to the nature of cloud computing, there are four major types of service resources that are potentially vulnerable: (i) Threats to applications; (ii) Threats to data; (iii) Threats to infrastructure; and (iv) Threats to cloud services in general Abdurachman et al, 2019).

The security situation of cloud environments is include five categories. The subsections of this section are assigned to a common security property as illustrated in Fig. 7. They can be categorized into the following categories: security policies, user-oriented security, data storage security, application security, and network security (Singh et al, 2016, Khalil IM, 2014, as cited in Tabrizchi et al, 2020).

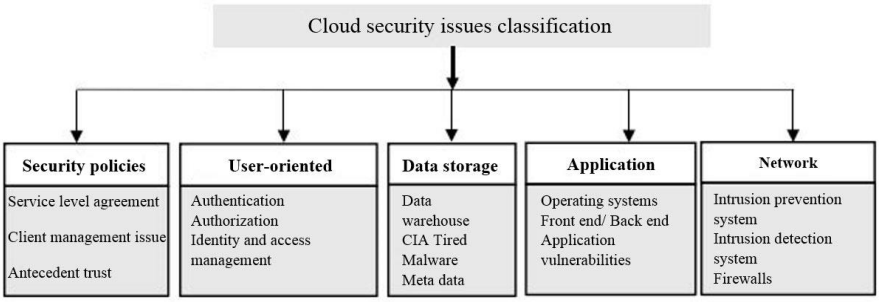

Figure 6. Diferent categories of cloud security issues

Big data management, SMEs, and cloud computing:

Big data management and cloud computing are becoming new business trends due to globalization and rising demand for quality products (Lu et al, 2019). According to research (Fernandez at al, 2011, as cited in Gupta et al, 2021). Smart entrepreneurs can capitalize on new financial trends, launch new products in a shorter time frame, and organize accountants' work with cloud computing services. Big data is helping companies gain competitive advantage over their competitors and drive investors towards a peak globalization as a result of artificial intelligence, robots, and big data adoption (Ionescu, 2021). As a metaphor for the internet, clouds are a source of anxiety for businesses and individuals becaeuse cloud computing simply lingers in cyberspace, making it vulnerable to unauthorized access but security and privacy are ensured by cloud computing providers (Mollah et al, 2012, as cited in Alouffi et al, 2021). Cloud computing's infrastructure is insecure if compromises the confidentiality and availability of information. It is enforced to configure firewalls, patch servers, and put an intrusion-detection system in place. Data confidentiality and availability can be ensured through encryption and authentication processes (Alouffi et al, 2021).

In terms of managed services cloud-based offerings like cloud sourcing, SMEs make up a key market (Shetty et al, 2019) that they were getting more benefits through cloud computing. Benefits are Flexibility, Increased collaboration, Security, Work from anywhere, Environmentally friendly, Disaster recovery, and Competitiveness, for example, cloud technologies grant SMEs access to enterprise-class technology by providing various solutions (Sunil et al, 2020) such as customer relationship management (CRM), enterprise resource planning (ERP), project management (PM), and other sales, marketing, and accounting applications on the premises (Attaran et al, 2018). SMEs decision to use Cloud Computing is heavily influenced by top management support and relative advantage (Nguyen et al, 2022).

Factors affecting Cloud Computing acceptance in SMEs are: security and privacy, cost savings, comparative advantage, compatibility, superior management support, competitive pressure, regulatory support, and awareness (Jayeola et al, 2022), Technology readiness[2], Organization readiness[3], Knowledge and training, Vendor support[4], Size of organization, Complexity, Ease of use and convenience/simplicity, Reliability, Trialability, Trust, Sharing and collaboration, Organizational risk, Partner pressure, Competitive advantage, Elasticity, Ecological sustainability, Risk analysis, Integrity, Data sensitivity, Strategy, Geo-restriction (Nguyen et al, 2022); the most significant factors derived from studying are TOE[5] and DOI[6].

[2] Including technology readiness, IT resources, computer self-efficacy, facilitating conditions, availability of good internet connection, adequate telecom services

[3] Including organization readiness, competency of the enterprise, previous technological experience, business concern, prior experience, the organization support

[4] Vender support, supplier efforts, service providers' support, efficient service delivery

[5] Technology, Organization, and Environment

[6] Diffusion of Innovation

Conclusion:

Cloud computing is an almost emerging technology whose wide range of benefits can be a good solution to many problems and limitations of small and large businesses. Although cloud computing is somewhat well known, many questions remain unanswered, especially for large businesses, large companies, and big data. The tendency of great companies in the IT industry to present cloud computing services is unavoidable and this is good news (Taghipour et al. 2020). In this article, we first gave a brief overview of cloud computing, types, components, main characters, as well as its benefits, and then briefly describe its threats and challenges. Due to the increasing use of cloud services in the field, we finally examined the impact of cloud computing on businesses and expressed the factors influencing the decision and acceptance of cloud computing in businesses. It is clear that this technology has a significant impact on society and business.

Although most of the articles mention three cloud services including IaaS, PaaS, and SaaS, in the article of Kumar et al., 2017, new services are introduced based on the developments like Container-as-a-Service (CaaS), Software-defined networking (a concept to design and manage networks that abstracts applications away from the underlying networks), Software-defined-storage (abstracts the logical storage services and capabilities away from the underlying hardware) and Cloud-of-Things (CoT), (a concept combining cloud computing and Internet-of-Things (IoT) for smart city applications), And in Rashid et al, 2019 article, another case is mentioned as Recovery as a Service (RaaS). Companies can recover entire data centers, servers (OS, applications, configuration, and data), and database files by using RaaS providers. The use of these services and the accurate identification of threats can make a significant improvement in the information security and data protection of large organizations.

Based on Sunil et al, 2020, research, Public clouds are used by 83% of organizations to store sensitive data, and the public cloud is trusted by 69% of organizations as a more secure way to protect sensitive data.Globally, 61% of personal customer data will be stored in public clouds. Cloud computing offers many advantages to businesses, such as flexibility, increased collaboration, automated software updates, environmental friendliness, disaster recovery and security. Despite this, cloud computing also has several concerns, as does every other technology. One of the biggest problems in the cloud is data breaches. Only when the concerns are addressed will more organizations be willing to accept cloud computing. A better understanding of decision factors and acceptance of cloud computing is effective in small and medium enterprises. Therefore, managers, suppliers, and policymakers will benefit from the findings of this study, and with these factors, precise strategies can be developed to assist them in adopting CC.

In addition, in this article, according to the definition and scope of types of threats, they are classified based on service resources in the cloud, which can be effective in providing privacy and security, and shows that all people involved in cloud computing, including users and service providers are responsible for this.

This study also has some limitations. First, the number of related articles reviewed in this study is limited. In addition to the research problem, there is likely to be a lot of unresearched material. Cloud computing is used in different ways in different types of enterprises, so the factors that affect its application differ. The future needs to include studies that provide the aspects affecting the application of CC within each specialized industry.

References:

Abdurachman, E., Gaol, F. L., & Soewito, B. (2019). **Survey on threats and risks in the cloud computing environment**. Procedia Computer Science, 161, 1325-1332.

Alashhab, Z. R., Anbar, M., Singh, M. M., Leau, Y. B., Al-Sai, Z. A., & Alhayja'a, S. A. (2021). **Impact of coronavirus pandemic crisis on technologies and cloud computing applications**. Journal of Electronic Science and Technology, 19(1), 100059.

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). **A systematic literature review on cloud computing security: Threats and mitigation strategies**. IEEE Access, 9, 57792-57807.

Attaran, M., & Woods, J. (2019). **Cloud computing technology: improving small business performance using the Internet**. Journal of Small Business & Entrepreneurship, 31(6), 495-519.

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

Gupta, A., Mazumdar, B. D., Mishra, M., Shinde, P. P., Srivastava, S., & Deepak, A. (2021). **Role of cloud computing in management and education**. Materials Today: Proceedings.

Ionescu, L., & Andronie, M. (2021). **Big data management and cloud computing: Financial implications in the digital world**. In SHS Web of Conferences (Vol. 92, p. 05010). EDP Sciences.

Jayeola, O., Sidek, S., Abd Rahman, A., Mahomed, A. S. B., & Hu, J. (2022). **Cloud computing adoption in small and medium enterprises (SMEs): A systematic literature review and directions for future research**. International Journal of Business and Society, 23(1), 226-243.

Kollolu, R. (2020). **Infrastructural constraints of Cloud computing**. International Journal of Management, Technology and Engineering, 10, 255-260.

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). **Exploring data security issues and solutions in cloud computing**. Procedia Computer Science, 125, 691-697.

Lu, Y., & Xu, X. (2019). **Cloud-based manufacturing equipment and big data analytics to enable on-demand manufacturing services**. Robotics and Computer-Integrated Manufacturing, 57, 92-102.

Namasudra, S. (2018). **Cloud computing: A new era**. Journal of Fundamental and Applied Sciences, 10(2).

Nguyen, G. T., & Liaw, S. Y. (2022). **Understanding the Factors Affecting the Small and Medium Enterprises Adoption of Cloud computing: A Literature Review**. International Journal of Business, Management and Economics, 3(2), 149-162.

Odun-Ayo, I., Ananya, M., Agono, F., & Goddy-Worlu, R. (2018, July). **Cloud computing architecture: A critical analysis**. In 2018 18th international conference on computational science and applications (ICCSA) (pp. 1-7). IEEE.

Pallathadka, H., Sajja, G. S., Phasinam, K., Ritonga, M., Naved, M., Bansal, R., & Quiñonez-Choquecota, J. (2022). **An investigation of various applications and related challenges in cloud computing**. Materials Today: Proceedings, 51, 2245-2248.

Rashid, A., & Chaturvedi, A. (2019). **Cloud computing characteristics and services: a brief review**. International Journal of Computer Sciences and Engineering, 7(2), 421-426.

Shetty, J. P., & Panda, R. (2021). **An overview of cloud computing in SMEs**. Journal of Global Entrepreneurship Research, 1-14.

Srivastava, P., & Khan, R. (2018). **A review paper on cloud computing**. International Journal of Advanced Research in Computer Science and Software Engineering, 8(6), 17-20.

Stephen, A., Anitha, A. A., & Arockiam, L. **Cloud Computing: Opportunities and Challenges**. TIRUCHIRAPPALLI-620 002, TAMIL NADU, INDIA.

Subramanian, N., & Jeyaraj, A. (2018). **Recent security challenges in cloud computing**. Computers & Electrical Engineering, 71, 28-42.

Sun, P. (2020). **Security and privacy protection in cloud computing: Discussions and challenges**. Journal of Network and Computer Applications, 160, 102642.

Sunil, S.T., Khadri, S., & Sachin, K. T. (2020). **Cloud Computing for Business Development**. International Journal of Research in Engineering, Science and Management , 3(2), 225-227.

Sunyaev, A. (2020). **Internet computing: Principles of Distributed systems and emerging internet-based technologies**. Springer Nature.

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). **A survey on security challenges in cloud computing: issues, threats, and solutions**. The journal of supercomputing, 76(12), 9493-9532.

Taghipour, M., Soofi, M. E., Mahboobi, M., & Abdi, J. (2020). **Application of cloud computing in system management in order to control the process**. Management, 3(3), 34-55.

Verma, G., & Adhikari, S. (2020). **Cloud computing security issues: a stakeholder's perspective**. SN Computer Science, 1(6), 1-8.

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.