Research Article

Cloud Computing Trends: A Literature Review

Nasser Taleb

Associate Professor,
Canadian University Dubai, UAE

Elfadil A. Mohamed

Assistant Professor,
Ajman University, UAE

Doi: 10.36941/ajis-2020-0008

Abstract

This study is a literature review on cloud computing cloud computing trends as one the fastest growing technologies in the computer industry and their benefits and opportunities for all types of organizations. In addition, it addresses the challenges and problems that contribute to increasing the number of customers willing to adopt and use the technology. A mixed research study approach was adopted for the study, that is, by collecting and analyzing both quantitative and qualitative information within the same literature review and summarizing the findings of previous (related) studies. Results highlights the current and future trends of cloud computing and exposes readers to the challenges and problems associated with cloud computing. The reviewed literature showed that the technology is promising and is expected to grow in the future. Researchers have proposed many techniques to address the problems and challenges of cloud computing, such as security and privacy risks, through mobile cloud computing and cloud-computing governance.

Keywords: *cloud computing trends, cloud computing challenges, cloud computing governance*

1. Background

Companies have worked to store and protect data for decades, working to protect clients' confidential data. Firms developed cloud computing, as a way to provide secure data storage and processing power for firms and private individuals. Many firms in many fields use cloud storage (Mei, Li, & Li, 2017). Cloud computing, now dubbed simply computing, uses Internet technology in dynamic applications and storage. Cloud computing has five major characteristics (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, & Zaharia, 2010): on-demand self-service; broad network access; resource pooling; rapid elasticity; and measured service. In addition, cloud computing includes three major types of services: Infrastructure as a Service, Platform as a Services and Software as a Service (Mell & Grance, 2011). Furthermore, there are four different ways to use cloud computing: public cloud, private cloud, community cloud, and hybrid cloud.

Advantages of cloud computing are availability of processing power, storage, flexibility, scalability, and reducing overhead cost on the IT infrastructure (Rajaraman, 2014). Figure 1 illustrates cloud-computing applications. Startup organizations have been able to take advantage of moving to a cloud environment by channeling capital spending into operational spending, making cloud

computing attractive when cutting IT budgets. Use of cloud computing is most commonly adopted by the smallest firms, whereas medium-sized firms have lower rates and the lowest rates are in firms with about 100 employees (Bloom & Pierri, 2018). Larger firms have enough in-house computing power. In contrast, cloud computing has some disadvantages (Ashari & Setiawan, 2011) such as requirements for Internet access, speed, and direct access to resources. Therefore, companies may find it quite risky to depend entirely on cloud-computing service providers. Any interruption in cloud services could cause organizations great damage (Grigoriou, Retana, & Rothaermel, 2012). Karkonasasi, Baharudin, Esparham, and Mousavi (2016) pointed out the main advantages: cost saving, security, privacy, and reliability. Stakeholders anticipate these issues in adopting cloud computing will be mitigated or eliminated in the future.

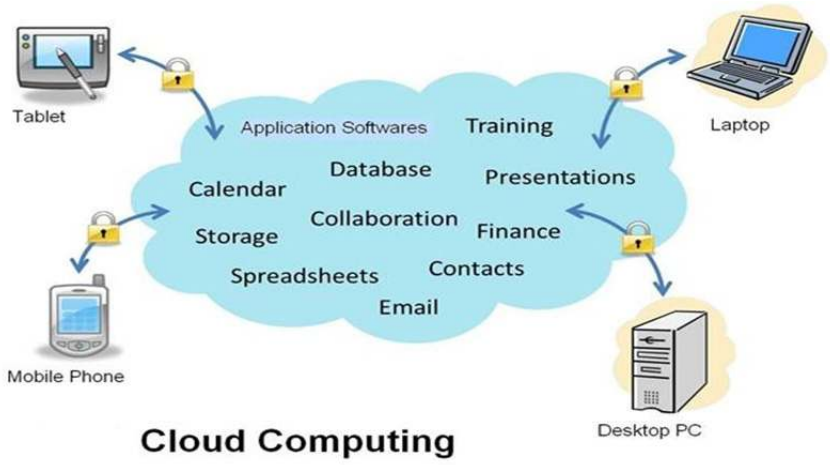

Figure 1: Cloud computing applications.
Source: From Gartner outlines 5 cloud computing trends—What they really mean, by U. Banerjee, 2019), retrieved March 10, 2019, from https://setandbma.wordpress.com/2012/04/24/gartner-5-cloud-trends/

Extant literature describes past and present trends in cloud computing and its usefulness in helping firms meet clients' needs, placing them in a position to enhance their competitive status. Researchers also discuss and expose readers to the main challenges and obstacles encountered when using cloud computing.

2. Current Trends in Cloud Computing

Cloud computing has become a major asset for firms in vying to meet their clients' need and enhance their competitive status. Their mastery of efficient and effective data storage has promoted a need for greater storage space. As a result, service providers must work to increase the capacity of online data centers. Cloud computing has become an essential part of sustaining superior performance to enhance competitive status (Baldini et al., 2017). Cisco (2018) estimated more that the cloud housed 547EB of data in 2018. As more storage space becomes available, firms are impacted positively, allowing them to store greater amounts of data. These large caches of data allow companies to house, analyze and gain helpful information on customers' information, desires, and behaviors (Duan, Fu, Zhou, Sun, Narendra, & Hu, 2015). Cloud computing also allows smaller firms to store and share data as fees for cloud computing descend.

In recent years, hackers have found ways to compromise security in cloud computing, attacking

computers through Wannacry and Ransomware (Kitchen & Reiss, 2018), and placing cloud-computing firms on guard. These continuing attacks alerted experts to increase their security and response time. Hackers have gained considerable sophistication in their efforts, forcing companies to invest time and effort in methods to detect malware (Baldini et al., 2017). Cloud computing providers help firms in these efforts, working to keep data safe and confidential. Now, companies must work harder to secure client's information, often investing immense resources to maintain security and avoid cybersecurity compromise. To do so, companies must hire experts who are able to defend data against hackers. Figure 2 shows an increase in the number of organizations that are turning to cloud computing as an alternative to run their applications.

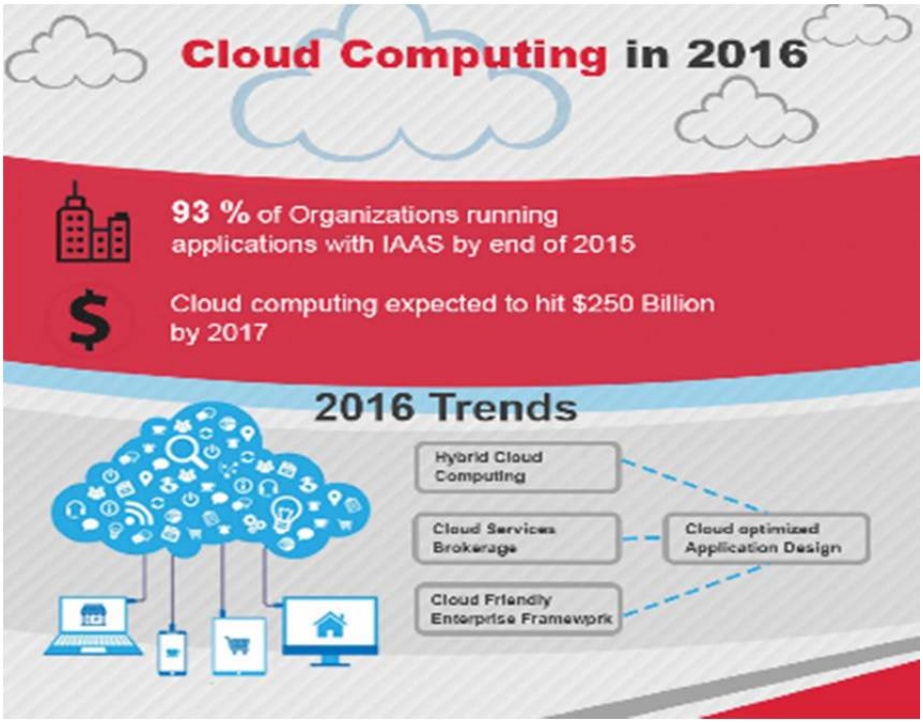

Figure 2: 2016 trends in cloud computing.
Source: From Gartner outlines 5 cloud computing trends—What they really mean, by U. Banerjee, 2019), retrieved March 10, 2019, from https://setandbma.wordpress.com/2012/04/24/gartner-5-cloud-trends/

Internet service providers work to enhance the quality of services on the Internet. Cloud-computing services require the ability to meet increasing demand for speed and storage space globally (Dempsey & Kelliher, 2017). By the inception of 2019, Internet service providers launched 5G networks with the highest speeds available to date. South Korea was first to release 5G networks in April of 2019. These increasing protocols will augment clients' ability to load and access clients' information. In turn 5G presages quality Internet from which all users will benefits, allowing people and companies to send and receive information in real-time.

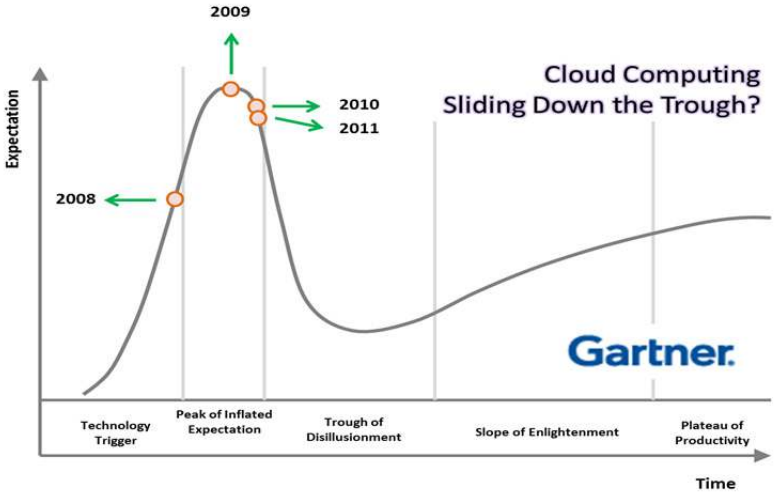

Figure 3: Gartner curve of past and future trends.
Source: From Gartner outlines 5 cloud computing trends—What they really mean, by U. Banerjee, 2019), retrieved March 10, 2019, from https://setandbma.wordpress.com/2012/04/24/gartner-5-cloud-trends/

3. Future Trends in Cloud Computing

Service providers are remunerated by organizations that use cloud-computing services. Large multinational firms are beginning to generate proprietary cloud networks that meet their specific needs. These very large firms find it lucrative to provide private cloud networks rather than using those of general service providers (Varghese & Buyya, 2018). For example, Coca-Cola has huge amounts of data and can develop a private network with high security that aligns with their particular needs. IBM, one of the largest multinational computer companies, is developing private cloud storage. Other multinational firms are likely to develop their own cloud systems, as well.

The overwhelming numbers of large companies have an IT department. As cloud service providers increasingly develop more complex offerings, they will be able to customize the cloud to answer the needs of each corporation, thereby allowing companies to outsource their IT departments (Baldini et al., 2017). Companies will no longer need to invest funds in elaborate and expensive computers and IT departments. Further, IT employees will need to learn how to manage applications on the cloud. As cloud computing becomes common and user friendly, smaller firms and private individuals will join large companies in choosing to use the cloud.

Many companies analyze data several times each year. To perform analytics, firms need powerful computers. However, over time, cloud computing will encompass that analysis so firms can access analytic information whenever they need it. Thus, organizations will not need their own expensive computers to answer that intermittent need (Baldini et al., 2017). As these services become increasingly less expensive, businesses will be able to contract for services only when needed. Thus, conducting analytics on the cloud will reduce cost and risk, thereby increasing firms' profits and reducing costs and risks (Baldini et al., 2017).

3.1 Mobile Cloud-Computing Trend

Due to the wide availability and advances in smartphones, mobile cloud computing must be addressed in supporting applications and needed computational power. Therefore, mobile cloud computing can be thought of as combining mobile computing and cloud computing. A. R. Khan, Othman, Madani, and Khan (2013) defined mobile computing as the integration of cloud computing with mobile devices to provide mobile devices with computational power, memory, and storage. In another paper, Huang (2011) dubbed mobile cloud computing *mobicloud computing.* Important issues concerning mobile cloud computing are applications, security, and unified standards (A. R. Khan et al., 2014). Mobile cloud computing may extend smartphone hardware and battery life.

Issues and challenges of mobile cloud computing are performance, resources, and techniques (Akherfi, Gerndt, & Harroud, 2018). Having a standard architecture would substantially improve mobile devices' capabilities in cloud processing and storage-power resources (Akherfi et al., 2018).

Nowadays, mobile cloud computing is considered quite important for online social network services such as gaming, image handling, video processing, and general e-business. Several generic surveys pointed to the importance of mobile cloud computing. Fan, Cao, and Mao (2011) discussed two mobile-cloud application models, those of Marinelli (2009) and cloudlets by Satyanarayanan, Bahl, Caceres, and Davies (2009). Fan et al. highlighted the significance of intelligent access schemes. Klein, Mannweiler, Schneider, and Schotten (2010); Dinh, Lee, Niyato, and Wang (2013); and Guan, Ke, Song, and Song (2011) discussed generic issues of a mobile cloud. Kovachev, Cao, and Klamma (2011) compared application models.

3.2 Quantum Computing Trend

Quantum is one of hottest topics in the cloud industry that challenge the present state of cloud computing and might transform it totally. Service providers are trying to cut-throat competition and in such a scenario Quantum Computing is heading to take over the cloud computing in the near future.

3.3 Hybrid Cloud Solutions Trend

In addition to other anticipated cloud computing trends, Hybrid Cloud Solutions are expected to take its place very soon in the domain of cloud computing. Moreover, Hybrid Cloud Solutions are known for being dynamic, cost-effective, and also can adapt to the market vibrant needs. With Hybrid Cloud Solutions, it is possible to attend to these market demands due to the rise of competition by large-scale enterprises.

3.4 Automation Trend

Cloud adoption is necessary and increasing quickly, which means that organizations have to deal with more computing; this will result in more data and application resources. This would require more admin jobs and time-consuming tasks. The automation of execution will reduce repetitive jobs, reduce errors and increase productivity. Therefore, companies of all sizes should aim to automate different processes. Automation will help simplify cloud administrators' jobs by saving cost and time.

4. Cloud-Computing Challenges

Adopting cloud computing has many challenges and problems. This section discusses the main challenges and problems that might hinder the adoption of cloud computing that must be addressed to convince organizations to embrace this emerging technique.

4.1 Cloud-Computing Governance

Past and the current decade have witnessed a wide adoption and use of cloud computing. Due to the importance of cloud computing for improving organization performance, its governance plays an important role for decision-makers. Cloud-computing governance can be considered part of the general umbrella of IT governance. Researchers have offered several definitions for the term IT governance. Brandis, Dzombeta, Colomo-Palacios, and Stantchev (2019) defined IT governance as "IT governance is about the configuration of organizational resources to ensure effective management" (p. 1). An important aspect of IT governance is the alignment of IT objectives with corporate strategy. A compelling need exists for cloud-computing governance and how it can be implemented. In a recent work, Bounagui, Mezrioui, and Hafiddi (2019) presented a new cloud-computing–governance framework based on endorsed IT models: ITIL, Control Objectives for Information and Related Technologies (COBIT), and ISO/IEC 27001/2. The proposed framework aims to develop evaluation and integration approaches with IT models.

One issue that might hinder the adoption and use of cloud computing is compliance with general regulations and laws for customers and cloud providers. Kundu, Sura, and Sharma (2018) proposed a framework aimed at helping organizations cope with compliance aspects in their cloud-oriented environments. The proposed framework has been implemented in two organizations. The results are encouraging and may lead adopter organizations to fewer reported compliance violations, higher contribution of cloud computing to overall quality of service, and organizational-compliance management.

Another important issue related to cloud-computing governance is the lack of expertise in handling cloud-computing-based IT control. S. N. Khan, Nicho, Takruri, Maamar, and Kamoun (2019) tried to link cloud computing and IT governance to humane arrangements, validating and ranking role assigning and taking components through in-depth interviews with 12 IT decision-makers and 44 Information Systems Audit and Control Association members, engaged as panelists in a Delphi-technique implementation. The S. N. Khan et al. study indicates that skills and competencies are prioritized determinants of IT controls, whereas IT security, risk, and compliance emerge as capabilities crucial in evaluating and managing cloud-computing service providers. Such results should be subjected to further investigation to consider different regions.

Hardware systems have become quite complex and the complexity is exacerbated by the adoption of cloud computing. To alleviate such complexity Kundu et al. (2018) presented a vision on how hardware-system development and governance should be carried out. They suggested applying a fresh approach to the problem of hardware development and verification, going from a black-box-driven model to a white-box model to improve trust, reliability and efficiency in a dynamic, collaborative, and accountable manner.

Despite the huge benefits that cloud computing can deliver for organizations, many corporations remain skeptical of adopting the technology. The main reason might be attributed to poorly understood factors that inhibit adopting and using the technology. To address this problem, Borgman, Bahli, Heier, and Schewski (2013) proposed a framework based on a technology–organization–environment model with a goal of discerning the factors that influence companies' decisions to use cloud computing. Borgman et al. study showed that the technology and organization companies engage affects their ability to implement their goals.

The authors divide the challenges related to the cloud computing governance into management problems and hardware compliance problems. While the issue of hardware compliance has received greater attention and viable solutions were introduced, however, the management problem still needs further investigations and solutions. The authors suggest drafting international IT compliance regulations that can be adopted by cloud computing service providers all over the world. These compliance regulations should be applicable for both customers and the service providers in case of any dispute that might surface in the future between the two parties. This approach is expected to expel the customers' fear from adopting the cloud computing technology.

4.2 Cloud-Computing Security

Computer security remains a critical and vital subject for scientists and practitioners. The problem is aggravated by the introduction of cloud computing because customers lack full control of the resources provided by cloud-computing service providers. Security in cloud computing is more challenging for customers and cloud-computing providers. IT governance offers visibility and IT control; therefore, efforts toward corporate governance can reduce operation risks, can establish compliance, and can protect the invested value (Suicimeczov & Georgescue, 2014). To address cloud-computing security, mechanisms are needed to enhance and protect users from intrusion and attack. Researchers have long recognized the importance of protecting computer data from unauthorized access. Researchers discussed a three-way authentication approach that helps in data security (Dangi & Pawar, 2019). The approach proposed would help in effective three-factor security with low computational parameters that are effective while looking at security aspects compared to previously defined authentication techniques in cloud security.

The protection of data from being tampered with by the cloud provider is a formidable task, especially if hackers are colluding with the cloud provider. To address such problems, Cao, Zhang, Liu, Zhang, and Neri (2019) proposed a technique based on blockchain technology. In using this technique, data will be stored in the public blockchain as transactions and will be modified only by authorized people. Security analysis and performance evaluation of the proposed technique demonstrates it can provide strong security guarantees with a high efficiency. To prevent leaking sensitive data to the cloud service provider, cryptographic methods can be used to ensure verifiability and privacy (Zhao, Hu, Song, & Zhao, 2019).

One method used to address the security and privacy issues of cloud computing is by introducing data encryption. However, the encryption of data increases the computational overhead and hence has a negative impact on the speed of data searches and retrieval. To alleviate such problems and gain the best results in obtaining encrypted data from outside sources and reducing the computational overhead of cloud servers, Q. Zhang, Wang, and Liu (2019) suggested a scheme for cloud environments. Their idea was to use matrix encryption to ensure user privacy (Q. Zhang, Wang, & Liu, 2019). The researchers suggested a cooperative method of preserving personalized searches that would maintain the privacy of the user. Another interesting method used to address the problem of cloud-computing security is a lightweight-secure-conjunctive-keyword-search scheme in hybrid cloud environments (LCKS) based on a ciphertext-policy ABE algorithm, which supports file-owner authorized conjunctive keyword searches for multiple parties (He, Zhang, Li, Jin, & Zhang, 2019). The LCKS security analysis and performance evaluation indicate it is secure, highly efficient, and well suited for the hybrid cloud.

Researchers who address the complexity of encrypted data are increasing in number. Recently Manoharan and Ruba Soundar (2019) proposed an effective securable fuzzy-logic-based ranking mechanism for document searching on outsourced cloud data. Their approach employs elliptic-curve-cryptograph (ECC)-based encryption and a fuzzy-logic based ranking scheme over the encrypted data to retrieve documents from the cloud. The experimental analysis of the approach indicated it is highly secure and efficient and exhibits better recall and precision in the information-retrieval system to address the document-retrieval process.

Cloud computing users must be aware of the vulnerabilities and the type of attack that might occur in cloud computing. Asvija, Eswari, and Bijoy (2019) conducted an excellent survey that attempted to highlight the significant vulnerabilities and expose readers to the various existing attacks related to hardware-assisted virtualization, as it has become the most widely used form of virtualization in building modern-day massive data centers and cloud infrastructures. Security remains one of the greatest challenges that keep many organizations from adopting the technology. Although numerous researchers have introduced many privacy-preserving models and security mechanisms in recent years, many customers were not convinced by these mechanisms. Recently Prabhu Kavin and Ganapathy (2019) proposed a new Chinese-remainder-theorem (CRT)-based data-

storage mechanism for storing user data securely in a cloud database. The proposed model adopts two encryption schemes that use new formulas to perform the first and second encryption and also uses a new formula to decrypt the cloud data. Prabhu Kavin and Ganapathy's data-storage security model outperformed existing models.

Cloud computing security is challenging and the problem becomes more complicated if we move to mobile cloud security. Many researchers have proposed solutions to alleviate such problems. For example, Dey, Ye, and Sampalli (2019) proposed a machine-learning-based intrusion-detection scheme for mobile clouds involving heterogeneous client networks. Their proposed scheme is highly effective in intrusion detection, does not require rule updates, and its complexity can be customized to suit the requirements of the client networks.

The methods used for protecting computer data from unauthorized access and modifications can be classified into two main categories. The first type use encryption and decryption. While methods using such approach are very reliable in protecting the computer data from unauthorized access, however, the methods are not efficient especially for data that need stringent requirements for storage and retrieval, because the encryption and decryption take considerable amount of time. The authors in this paper suggest that customers willing to adopt cloud computing have to conduct thorough investigations about their needs and whether efficiency is of paramount importance for them before choosing this methods or the cloud computing service providers adopting such approach.

The second type of methods that can be used for securing the data from unauthorized access and modifications, specially the internal threat, are based on Blockchains, a new technology that can be used to protect the customer from internal threat that might be committed by personnel of the cloud computing service providers.

4.3 Data Privacy

One of the greatest challenges of cloud computing is the privacy issue. Several studies have worked to address such challenges and problems. In the area of Internet of Things (IoT), devices are configured to access content or resources from multiple resources of variously integrated devices at the edge, which raises the issue of data privacy. To address such problems, Duan, Lu, Zhou, Sun, and Wu (2019) proposed to model the privacy content of multiple sources by mapping them as resources of types of data, information, and knowledge in the well-known DIKW architecture. Their proposed model provided a protection solution according to explicit and implicit divisions for privacy targets for typed data.

The healthcare sector has witnessed substantial increases in the use of cloud computing for the storage of patient medical information. Protecting patient medical data stored in the server from unauthorized personnel is very important for patients. The problem is exacerbated when the data are stored in the cloud-computing environment. Preserving privacy becomes a major concern for patients. Patients are concerned about the privacy of their data being stored on a cloud server. For this reason, healthcare providers must find solutions that guarantee the protection of patient data.

Researchers have proposed myriad solutions to address issues of the medical-data privacy. To address this problem, X. Zhang, Zhao, Mu, Tang, and Xu (2019) suggested using elliptic curve cryptography for medical cyberphysical systems that would be identity-based and proxy-oriented way to outsource public auditing. Interestingly, the proposed system preserves data privacy while simultaneously allowing any third-party auditor to audit the medical data efficiently, without retrieving the entire medical data.

W. Li et al. (2018) proposed a novel attribute-based encryption scheme for fine-grained and flexible access control to personal health records (PHRs) data in cloud computing. Their proposed scheme generates shared information through a common-access subpolicy based on different patients' access policies. Then, the scheme combines the encryption of PHRs from different patients. The proposed scheme is quite efficient in time and adheres to a ciphertext-policy attribute-based

encryption scheme.

Further improvements in preserving medical-data privacy are needed. Recently Kumar, Ahmad, and Kumari (2019) discovered several security flaws in a cloud-assisted authentication and privacy-preservation scheme for a telecare medical information system (TMIS). Examples of the discovered security flaws include message-authentication failures in health care center uploads and impersonation attacks in the patient data-upload phase. Kumar et al. proposed a protocol that addresses the problems of a cloud-assisted authentication and privacy-preservation scheme. Working solutions to address data privacy in cloud computing apply encryption and decryption algorithms such as a homomorphic encryption algorithm, which has the serious limitation of supporting only limited data types. To handle this problem, Min, Yang, Sangaiah, Bai, and Liu (2019) proposed a parallel fully homomorphic encryption algorithm that supports floating-point numbers. The proposed algorithm uses the characteristics of multi-nodes in the cloud environment to conduct parallel encryption through simultaneous group-wise ciphertext computation.

To encourage healthcare providers to use the cloud server to store their patients' medical data, many studies have been proposed to quell fear about the privacy of the data. Essa, Hemdan, El-Mahalawy, Attiya, and El-Sayed (2019) suggested an intelligent security system, dubbed Intelligent Framework for Healthcare Data Security that would allow medical staff to gain and process large amounts of data. The proposed system would have less impact and thus less staff time, in data processing.

Liu, Liu, Jiang, Zhao, and Wang (2018) proposed a new solution to protect patient private data. In this solution, they proposed the use of a blockchain-based scheme to secure the sharing and trading of x-ray medical-image data based on blockchain. The procedure used to secure the x-ray data followed three steps: first the assigned x-ray data are transmitted to the cloud using the message queuing telemetry-transport protocol. Second, the patient image data are encrypted using a hashing algorithm. Third is applying a watermark to the image data and finding generating blocks through the agreement mechanism of the block. Although the solution seems fine, further investigation about its viability is required.

Additional solutions have been proposed to protect the privacy of medical data stored in the cloud based on data encryption. However, the encryption of data limits the ability of the cloud center to process the data. To address this problem, researchers proposed schemes based on fully homomorphism concepts for privacy protection and data processing of medical data (X. Wang, Bai, Yang, Wang, & Jiang, 2019).

Another prominent protocol for protecting the privacy of patient medical data that is widely used is the three-factor authentication protocol. Although the protocol is verified at the user side, a high chance exists that the data might be compromised. D. Xu, Chen, Zhang, and Liu (2018) proposed a novel, efficient, truly three-factor authentication protocol for TMIS. In this proposed protocol, the three factors (password, smart card, and biometric) are verified at the server side. As claimed by its inventor, the performance of the protocol is quite efficient and suitable for TMIS.

The research that aims to address the data-privacy problem in cloud computing continues to increase. Researchers have proposed several new algorithms and techniques. Cryptosystem-based methods are an example of methods that employ high computing power of cloud servers that preserve data privacy. The main characteristic of these methods is to allow sharing and provide multi-user independent services. The encryption of data on the server side results in delays in the allocation and release of resource sharing by the cloud-computing server. To address this problem, J. Li, Wang, Huang, Wang, and Xiang (2019) proposed a decentralized cryptographic protocol for multi-user consensus systems. Based on this protocol, the researchers designed a decentralized multi-role e-voting protocol using the CRT, where each role's election aligns with a sub-access structure.

Another problem that faces cloud-computing clients is the choice of the cloud-computing service provider, determining which cloud-computing service provider would better protect the confidentiality of data. Cloud-computing service providers and clients' practices should align, spelled out in security-level agreements. Silva, Silva, Rocha, and Queiroz (2019) proposed a model to

calculate service-provider reliability. Their model measures solutions and mitigation of breaches in security. The Silva et al. model anticipates the ability to categorize services and develop abstract methods of defining emphases in the structure of the data storage to maintain privacy and enhance trust.

Among research areas that received considerable attention is mobile cloud computing. The proliferation of smart phones has encouraged the need to outsource data storage to the cloud server. Such requirements raise the issue of data privacy. Among the solutions used to protect data privacy is the use of encryption before sending the data to the cloud server. At the same time, users need to retrieve the data quite quickly and ensure the integrity of the queried data. To reduce the overhead of searching the data, Z. Xu, Lin, Sandor, Huang, and Liu (2019) presented a study that allowed searches for data belonging to specific ranges. Their proposed work achieved data privacy and query-result completeness verification using an encrypted data index and the vector-neighbor chain. Their work also addressed the limitation of stringent mobile devices by designing a lightweight protocol based on linear algebra operations for 1-dimensional and multidimensional data.

Encrypting and decrypting the data at the cloud server has proven its viability as an acceptable technique to preserve the privacy of data. Y. Wang, Ding, Wu, Wei, Qin, and Wang, (2018) proposed a technique that guarantees the privacy of road-condition data stored in the cloud server in ciphertext format, which requires that the cloud server can distinguish the reported data from different vehicles in ciphertext format for the same place without compromising their confidentiality.

To ensure the security and integrity of data stored in the cloud server, provides can use various cryptographic tools such as cryptography based on identify and cryptography lacking certificates. This method would mitigate the escrow problem that seems intrinsic to identity-based cryptography (Wu, Mu, Susilo, Guo, and Zhang, 2019).

In mobile computing, many users share information through the mobile cloud. To address the problem of data privacy stored in the cloud server, data owners usually encrypt their data before outsourcing them to the cloud server (Cui, Zhou, Xu, & Zhong, 2019). Data encryption is a viable solution for preserving data privacy, but does not come without cost. The major problem of data encryption is the lack of efficiency. The encryption and decryption of the data takes considerable time and resources. The problem becomes more serious in the case of IoT devices, which have resource constraints. Zhou et al. (2019) presented a new fog-assisted privacy-preserving IoT data-search framework such that the data from each IoT device is collected by a fog node, stored in a predetermined document and outsourced to the cloud server. The users search the data through the fog nodes, and the fine-grained search management is maintained at the document level.

Based on this framework, Zhou et al. (2019) proposed two searchable encryption schemes: credible fog-node assisted searchable encryption and semi-trusted fog-node assisted searchable encryption. The performance of the proposed schemes is feasible and highly efficient. Although many solutions have been proposed to address the computation overhead of the encryption and decryption of data stored in the client and cloud server, the problem of IoT devices continues to need improvement. Chen et al. (2019) deviated from conventional software-based solutions and proposed a secure and efficient remote-monitoring framework called SRM. The framework uses the latest hardware-based trustworthy computing technology such as Intel SQX. The proposed framework shows that SRM can protect user data privacy against unauthorized parties with minimum performance cost compared to existing software-based solutions.

Protecting the privacy of personal multimedia data generated in large volume also has received interest from researchers. Magdy, Abouelseoud, and Mikhail (2019) investigated several features for use in building a privacy-preserving content-based image-retrieval system. The results they obtained are insightful, offering interesting trade-offs between security, computational efficiency, and accuracy.

The large increase in the generation and storage of sensitive personal data in the cloud server raises immense concerns about the privacy of such data. Domingo-Ferrer, Farràs, Ribes-González, and Sánchez (2019) conducted a survey that covers technologies that allow privacy-aware outsourcing

of storage and processing of sensitive data to public clouds. The researchers reviewed masking methods for outsourced data based on data splitting and anonymization, in addition to cryptographic methods covered in other surveys.

Analytics functions work to extract knowledge and support decision-making. The quality of decision-making depends on preserving data privacy and data quality. Alabdulatif, Khalil, Kumarage, Zomaya, and Yi (2019) introduced a scalable, cloud-based model to provide a privacy-preserving anomaly-detection service for quality-assured decision-making in smart cities. They employed homomorphic encryption to preserve data privacy during the analysis and a MapReduce-based distribution of tasks and parallelization to overcome computational overhead associated with homomorphic encryption.

Among the prominent methods in use to protect data privacy in the cloud and provide structured access control is ciphertext (W. Li et al. 2018; Min et al. 2019; Y. Wang et al., 2018). Yu et al. (2019) proposed a scheme with a direct-attribute revocation mechanism. Their idea was to use multiple authorities with encryption of attributes of a ciphertext policy. Based on their proposed revocation mechanism, remaining users need not update their secret keys when revocation happens. As claimed by their inventors, the scheme is more efficient than similar work in the encryption, decryption, and revocation stages.

The issue of data privacy remains one of the hottest challenges in cloud computing due to the proliferation of IoT devices that have resources constraint and at the same time there is a compelling need to improve the security to protect the customer private data. The authors in this paper suggest the development of efficient algorithms and protocols that run under resource constrains and without giving up the high level of security required to protect he private data.

5. Conclusion

In summary, cloud-computing trends are poised to answer companies' current and future needs. Because technology is essential to firms, cloud computing allows companies to store and access their data at any time. This feature has caused cloud computing to become increasingly popular very quickly. Over time, services providers are working to increase the number of services they provide, which are likely to include enhanced analytics services. Various benefits arise from the use of cloud-computing and cloud-storage services. Foremost is security of data. Over time, more and more businesses will store their data in the cloud and will contract with service providers to perform data analytics using the cloud. Even more notable is that, in the future, companies will have no other option than to store their data in the cloud. Business competition will rest largely on data safety and the ability to share and access data. Organizations are likely to become increasingly interdependent. Companies require a reliable cloud-computing environment that meets their needs and desires. Optimally, global enterprises will develop a plan to improve their use of cloud computing. To align with those plans, Internet service providers will enhance Internet speeds and reduce times when computers are offline, enabling users to rely on the cloud to access data instantly. Companies that do not join in this effort are likely to be less competitive.

References

Akherfi, K., Gerndt, M., & Harroud, H. (2018). Mobile cloud computing for computation offloading: Issues and challenges. *Applied Computing and Informatics, 14,* 1–16. doi:10.1016/j.aci.2016.11.002

Alabdulatif, A., Khalil, I., Kumarage, H., Zomaya, A. Y., & Yi, X. (2019). Privacy-preserving anomaly detection in the cloud for quality assured decision-making in smart cities. *Journal of Parallel and Distributed Computing, 127,* 209–223. doi:10.1016/j.jpdc.2017.12.011

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50–58. doi:10.1145/1721654.1721672

Ashari, A., & Setiawan, H. (2011). Cloud computing: Solusi ICT? *Jurnal Sistem Informasi [Journal of Information Systems], 3*(2), 336–345. Retrieved from https://ejournal.unsri.ac.id

Asvija, B., Eswari, R., & Bijoy, M. B. (2019). Security in hardware assisted virtualization for cloud computing—State of the art issues and challenges. *Computer Networks, 151,* 68–92. doi:10.1016/j.comnet.2019.01.013

Baldini, I., Castro, P., Chang, K., Cheng, P., Fink, S., Ishakian, V., Suter, P. (2017). Serverless computing: Current trends and open problems. In S. Chaudhary, G. Somani, & R. Buyya (Eds.), *Research advances in cloud computing* (pp. 1–20). Singapore: Springer.

Banerjee, U. (2019). *Gartner outlines 5 cloud computing trends—What they really mean.* Retrieved from https://setandbma.wordpress.com/2012/04/24/gartner-5-cloud-trends/

Bloom, N., & Pierri, N. (2018, August 31). Research: Cloud computing is helping smaller, newer firms compete. *Harvard Business Review.* Retrieved from https://hbr.org/2018/08/research-cloud-computing-is-helping-smaller-newer-firms-compete

Borgman, H. P., Bahli, B., Heier, H., & Schewski, F. (2013, January). Cloudrise: Exploring cloud computing adoption and governance with the TOE framework. In *2013 46th Hawaii International Conference on System Sciences* (pp. 4425–4435). Washington, DC: IEEE. doi:10.1109/HICSS.2013.132

Bounagui, Y., Mezrioui, A., & Hafiddi, H. (2019). Toward a unified framework for Cloud Computing governance: An approach for evaluating and integrating IT management and governance models. *Computer Standards & Interfaces, 62,* 98–118. doi:10.1016/j.csi.2018.09.001

Brandis, K., Dzombeta, S., Colomo-Palacios, R., & Stantchev, V. (2019). Governance, risk, and compliance in cloud scenarios. *Applied Sciences, 9,* Article 320. doi:10.3390/app9020320

Cao, S., Zhang, G., Liu, P., Zhang, X., & Neri, F. (2019). Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. *Information Sciences, 485,* 427–440. doi:10.1016/j.ins.2019.02.038

Chen, Y., Sun, W., Zhang, N., Zheng, Q., Lou, W., & Hou, Y. T. (2019). Towards efficient fine-grained access control and trustworthy data processing for remote monitoring services in IoT. *IEEE Transactions on Information Forensics and Security, 14,* 1830–1842. doi:10.1109/TIFS.2018.2885287

Cisco. (2018) *Cisco global cloud index: Forecast and methodology, 2016–2021.* San Jose, CA, Author.

Cui, J., Zhou, H., Xu, Y., & Zhong, H. (2019). OOABKS: Online/offline attribute-based encryption for keyword search in mobile cloud. *Information Sciences, 489,* 63–77. doi:10.1016/j.ins.2019.03.043

Dangi, R., & Pawar, S. (2019). An improved authentication and data security approach over cloud environment. In N. Yadav, A. Yadav, J. C. Bansal, K. Deep, & J. H. Kim (Eds.), *Harmony Search and Nature Inspired Optimization Algorithms* (pp. 1069–1076). Singapore: Springer.

Dempsey, D., & Kelliher, F. (2017). *Industry trends in cloud computing: Alternative business-to-business revenue models.* Berlin, Germany: Springer.

Dey, S., Ye, Q., & Sampalli, S. (2019). A machine learning based intrusion detection scheme for data fusion in mobile clouds involving heterogeneous client networks. *Information Fusion, 49,* 205–215. doi:10.1016/j.inffus.2019.01.002

Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless Communications and Mobile Computing, 13,* 1587–1611. doi:10.1002/wcm.1203

Domingo-Ferrer, J., Farràs, O., Ribes-González, J., & Sánchez, D. (2019). Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. *Computer Communications, 140–141,* 38–60. doi:10.1016/j.comcom.2019.04.011

Duan, Y., Fu, G., Zhou, N., Sun, X., Narendra, N. C., & Hu, B. (2015). Everything as a service (XaaS) on the cloud: Origins, current and future trends. In C. Pu & A. Mohindra (Eds.), *2015 IEEE 8th International Conference on Cloud Computing* (pp. 621–628). Washington, DC: IEEE.

Duan, Y., Lu, Z., Zhou, Z., Sun, X., & Wu, J. (2019). Data privacy protection for edge computing of smart city in a DIKW architecture. *Engineering Applications of Artificial Intelligence, 81,* 323–335. doi:10.1016/j.engappai.2019.03.002

Essa, Y. M., Hemdan, E. E. D., El-Mahalawy, A., Attiya, G., & El-Sayed, A. (2019). IFHDS: Intelligent framework for securing healthcare BigData. *Journal of Medical Systems, 43,* 124. doi:10.1007/s10916-019-1250-4

Fan, X., Cao, J., & Mao, H. (2011). A survey of mobile cloud computing. *ZTE Communications, 9*(1), 4–8. Retrieved from https://www.zte.com.cn

Grigoriou, K., Retana, G., & Rothaermel, F. (2012, January 06). IBM (in 2010) and the emerging cloud-computing industry. *Harvard Business Review.* Retrieved from https://hbr.org/product/ibm-in-2010-and-the-emerging-cloud-computing-industry/MH0008-PDF-ENG

Guan, L., Ke, X., Song, M., & Song, J. (2011, May). A survey of research on mobile cloud computing. In S. Xu, W. Du, & R. Lee (Eds.), *2011 10th IEEE/ACIS International Conference on Computer and Information Science* (pp. 387–392). Washington, DC: IEEE.

He, H., Zhang, J., Li, P., Jin, Y., & Zhang, T. (2019). A lightweight secure conjunctive keyword search scheme in hybrid cloud. *Future Generation Computer Systems, 93,* 727–736. doi:10.1016/j.future.2018.09.026

Huang, D. (2011). Mobile cloud computing. *IEEE ComSoc Multimedia Communications Technical Committee (MMTC) E-Letter, 6*(10), 27–31.

Karkonasasi, K., Baharudin, A. S., Esparham, B., & Mousavi, S. A. (2016). Adoption of cloud computing among enterprises in Malaysia. *Indian Journal of Science and Technology, 9,* Article 88128. doi:10.17485/ijst/2016/v9i48/88128

Khan, A. R., Othman, M., Madani, S. A., & Khan, S. U. (2013). A survey of mobile cloud computing application models. *IEEE Communications Surveys & Tutorials, 16,* 393–413. doi:10.1109/SURV.2013.062613.00160

Khan, S. N., Nicho, M., Takruri, H., Maamar, Z., & Kamoun, F. (2019). Role assigning and taking in cloud computing. *Human Systems Management, 38,* 1–27. doi:10.3233/HSM-180336

Kitchen, K., & Reiss, M. (2018, May 8). *Ransomware is coming. It'll make you Wannacry.* Heritage Foundation. Retrieved from https://www.heritage.org/technology/commentary/ransomware-coming-itll-make-you-wannacry

Klein, A., Mannweiler, C., Schneider, J., & Schotten, H. D. (2010, May). Access schemes for mobile cloud computing. In *2010 Eleventh International Conference on Mobile Data Management* (pp. 387–392). Washington, DC: IEEE. doi:10.1109/MDM.2010.79

Kovachev, D., Cao, Y., & Klamma, R. (2011). Mobile cloud computing: A comparison of application models. arXiv preprint. Retrieved from https://arxiv.org/abs/1107.4940

Kumar, V., Ahmad, M., & Kumari, A. (2019). A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS. *Telematics and Informatics, 38,* 100–117. doi:10.1016/j.tele.2018.09.001

Kundu, A., Sura, Z., & Sharma, U. (2018, October). Collaborative and accountable hardware governance using blockchain. In *2018 IEEE 4th International Conference on Collaboration and Internet Computing* (pp. 114–121). Washington, DC: IEEE. doi:10.1109/CIC.2018.00026

Li, J., Wang, X., Huang, Z., Wang, L., & Xiang, Y. (2019). Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing. *Journal of Parallel and Distributed Computing, 130,* 91–97. doi:10.1016/j.jpdc.2019.04.003

Li, W., Liu, B. M., Liu, D., Liu, R. P., Wang, P., Luo, S., & Ni, W. (2018). Unified fine-grained access control for personal health records in cloud computing. *IEEE Journal of Biomedical and Health Informatics, 23,* 1278–1289. doi:10.1109/JBHI.2018.2850304

Liu, B., Liu, M., Jiang, X., Zhao, F., & Wang, R. (2018, December). A blockchain-based scheme for secure sharing of X-ray medical images. In C.-N. Yang, S.-L. Peng, & L. C. Jain (Eds.), *International Conference on Security with Intelligent Computing and Big-Data Services* (pp. 29–42). Cham, Switzerland: Springer. doi:10.1007/978-3-030-16946-6_3

Magdy, S., Abouelseoud, Y., & Mikhail, M. (2019). Effect of chosen features on performance of privacy preserving image retrieval systems. *Computers & Electrical Engineering, 76,* 411–424. doi:10.1016/j.compeleceng.2019.04.020

Manoharan, S. N., & Ruba Soundar, K. (2019). A novel securable fuzzy logic based ranking scheme for document searching on outsourced cloud data. *Wireless Personal Communications, 105,* 175–218. doi:10.1007/s11277-018-6108-4

Marinelli, E. E. (2009). *Hyrax: Cloud computing on mobile devices using MapReduce* (Unpublished master's thesis, No. CMU-CS-09-164). Carnegie-Mellon University, School of Computer Science, Pittsburgh PA.

Mei, J., Li, K., & Li, K. (2017). Customer-satisfaction-aware optimal multiserver configuration for profit maximization in cloud computing. *IEEE Transactions on Sustainable Computing, 2,* 17–29. doi:10.1109/TSUSC.2017.2667706

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing.* Boston, MA: Harvard Business School.

Min, Z., Yang, G., Sangaiah, A. K., Bai, S., & Liu, G. (2019). A privacy protection-oriented parallel fully homomorphic encryption algorithm in cyber physical systems. *EURASIP Journal on Wireless Communications and Networking, 2019,* Article 15. doi:10.1186/s13638-018-1317-9

Prabhu Kavin, B., & Ganapathy, S. (2019). A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications. *Computer Networks, 151,* 181–190. doi:10.1016/j.comnet.2019.01.032

Rajaraman, V. (2014). Cloud computing. *Resonance, 19,* 242–258. doi:10.1007/s12045-014-0030-1

Satyanarayanan, M., Bahl, P., Caceres, R., & Davies, N. (2009). The case for VM-based cloudlets in mobile computing. *IEEE Pervasive Computing, 8*(4), 14–23. doi:10.1109/MPRV.2009.82

Silva, A., Silva, K., Rocha, A., & Queiroz, F. (2019). Calculating the trust of providers through the construction weighted Sec-SLA. *Future Generation Computer Systems, 97,* 873–886. doi:10.1016/j.future.2019.02.034

Suicimeczov, N., & Georgescue, M. R. (2014). IT governance in cloud. *Procedia Economics and Finance, 15,* 830–835. doi:10.1016/S2212-5671(14)00531-0

Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. *Future Generation Computer Systems, 79,* 849–861. doi:10.1016/j.future.2017.09.020

Wang, X., Bai, L., Yang, Q., Wang, L., & Jiang, F. (2019). A dual privacy-preservation scheme for cloud-based eHealth systems. *Journal of Information Security and Applications, 47,* 132–138. doi:10.1016/j.jisa.2019.04.010

Wang, Y., Ding, Y., Wu, Q., Wei, Y., Qin, B., & Wang, H. (2018). Privacy-preserving cloud-based road condition monitoring with source authentication in VANETs. *IEEE Transactions on Information Forensics and Security, 14,* 1779–1790. doi:10.1109/TIFS.2018.2885277

Wu, G., Mu, Y., Susilo, W., Guo, F., & Zhang, F. (2019). Privacy-preserving certificateless cloud auditing with multiple users. *Wireless Personal Communications, 160,* 1161–1182. doi:10.1007/s11277-019-06208-1

Xu, D., Chen, J., Zhang, S., & Liu, Q. (2018). Privacy-preserving and efficient truly three-factor authentication scheme for telecare medical information systems. *Journal of Medical Systems, 42*(11), 219. doi:10.1007/s10916-018-1047-x

Xu, Z., Lin, Y., Sandor, V. K. A., Huang, Z., & Liu, X. (2019). A lightweight privacy and integrity preserving range query scheme for mobile cloud computing. *Computers & Security, 84,* 318–333. doi:10.1016/j.cose.2019.04.003

Yu, P., Wen, Q., Ni, W., Li, W., Sun, C., Zhang, H., & Jin, Z. (2019). Decentralized, revocable and verifiable attribute-based encryption in hybrid cloud system. *Wireless Personal Communications,* 1–20. doi:10.1007/s11277-019-06187-3

Zhang, Q., Wang, G., & Liu, Q. (2019). Enabling cooperative privacy-preserving personalized search in cloud environments. *Information Sciences, 480,* 1–13. doi:10.1016/j.ins.2018.12.016

Zhang, X., Zhao, J., Mu, L., Tang, Y., & Xu, C. (2019). Identity-based proxy-oriented outsourcing with public auditing in cloud-based medical cyber-physical systems. *Pervasive and Mobile Computing, 56,* 18–28. doi:10.1016/j.pmcj.2019.03.004

Zhao, M., Hu, C., Song, X., & Zhao, C. (2019). Towards dependable and trustworthy outsourced computing: A comprehensive survey and tutorial. *Journal of Network and Computer Applications, 131,* 55–65. doi:10.1016/j.jnca.2019.01.021

Zhou, R., Zhang, X., Wang, X., Yang, G., Wang, H., & Wu, Y. (2019). Privacy-preserving data search with fine-grained dynamic search right management in fog-assisted Internet of Things. *Information Sciences, 491,* 251–264. doi:10.1016/j.ins.2019.04.003