INFORMATION SECURITY CHALLENGES IN CLOUD COMPUTING: CRITICAL REVIEWING STUDY

Shahad Ahmed Abdulgaffar

Information Science Department,
King Abdulaziz University, Jeddah, ***SAUDI ARABIA***

ABSTRACT

The great increase of intellectual production, the diversity of information sources and containers, and the technical revolution, which led in its turn to a large dependence on the Internet, portals and digital information sources, resulted not only in an emerging need to secure websites, computers, software and information in their various forms, but also in the growing importance of what is called the cloud computing service, which is a technical service that has changed the traditional ways of deploying services by organizations or individuals. The paper aimed at shedding light on the challenges facing cloud-computing technology, especially the information security challenge, in order to try to identify the challenges and solutions that contribute in limiting these challenges.

In fact, the lack of independent and detailed studies of these challenges that focus on practical solutions was the motive for conducting this paper. It aims at identifying and collecting the intellectual production, specifying the deficiencies, and looking out for future studies issues bearing in mind the importance of information security and its impact on the continuity and development of technology and facilitating the preservation, sharing and extraction of knowledge.

In this paper, the critical literary methodology was followed to specify the achieved studies and literature in the same issue and thus generalize the benefits and find solutions. Fifteen studies were analyzed to achieve the goal of identifying the challenges facing cloud computing. After reviewing the literature and studies, one of the most prominent results of the paper is that the most prominent challenges of cloud computing is information security. A number of studies have suggested heading to encryption as one of the solutions, and some of them have dealt with classification or the use of machine learning and fuzzy logic.

This paper recommended the necessity of conducting specialized studies in finding applicable solutions to tackle the challenges, the perfect use of machine learning techniques and fuzzy logic, the optimal use of encryption, and the adoption of systems that are "safe by default". Indeed, security is not just a technology but should be related to people and operations as well. Internet security should not be *absolute, but rather needs planning, design and building security from the birth of the idea.*

Keywords: *Information Security, Cloud Computing, Hybrid Cryptography, Risk Assessment, Cloud Computing Data Center, 3D Storage, Deffie Hellman Protocol*

INTRODUCTION

The great increase of intellectual production, the diversity of information sources and containers, and the technical revolution, which led in its turn to a large dependence on the Internet, portals and digital information sources, resulted in an emerging need to secure websites, computers, software and information in their various forms. When studying information security, which is the protection of information from any external threat, the researcher finds that it branches out into information security in ministries, institutions and banks, personal security for mobile phones and personal devices, and specialized and public systems. The importance of information security increased after the emergence of several reasons, including [1,2] where the discovery of the American company, Daewoo Securities, in 2002 mentioned that $ 21.7 million of the shares it manages had been sold illegally, as a direct result of a breach of its computer network. In 2003, an employee of a Russian company broke into the company's information network and adjusted his monthly salary and a group of his colleagues ‘salaries. He increased salaries by a certain percentage, causing very large losses to the company until the breach was discovered. The reasons for the importance of information security can be explained by technological progress, infantilism, impulsivity, and the spread of information crimes. In general, information security in the modern era is the cornerstone of the processes of information and communication technology renaissance.

Information security also requires continuous follow-up and continuous updating of everything that keeps pace with time changes to preserve information from any theft, modification, change or publication without a license. Information security challenges have increased after the emergence of the so-called cloud computing service, a technology that has changed the traditional ways in which organizations or individuals deploy services. It is a technology based on the transfer of everything stored on the computer to its storage in the cloud via a server that is accessed via the Internet. It provides various types of services to its registered users such as [3]; [4]: IAAS: Infrastructure as A Service - This service is provided by the cloud computing provider with a virtual server and an operating system. It allows companies to dispense with setting up their own information centers and using this service to install their applications on it. The company does not need a programmer to run this service, but rather it needs System Administrator, and Platform as a Service. PAAS - A model of platform service, which is a special environment service for Applications' owners to install their applications on them via the Internet. Then, it provides special services through the Internet to subscribers. This service requires those working on it to be a specialist in programming such as the Net Flex service. This company rented PAAS from Amazon and created an application that allows the subscriber via the Internet to watch the movie or TV show that he wants in exchange for a monthly subscription. SaaS: Software as a Service - The software-as-a-service model is a service that provides ready-to-work applications through the Internet or private networks. The user does not need to be a specialist in information technology to use them. They are used on a daily basis such as Gmail and Facebook in addition to special businesses services like Google Docs, Microsoft 365, and Salesforce.com.

According to the above basis, this critical paper comes to reveal the challenges of information security in cloud computing in light of the information and communication technology revolution. Hence, the study issue emerged to answer the following question: "What are the main information security challenges in cloud computing?" It aims at identifying the challenges that faced information security in cloud computing since the topic is particularly important in clarifying challenges and trying to avoid and limit them as this expected growth of data from all types of sources raises concerns about data and information protection. This confirms the importance of conducting studies on clarifying challenges and getting out with solutions and recommendations.

The topic also requires the largest amount of explanatory studies and research, especially to find appropriate solutions to ensure the protection of information and data, which is the reason for the preparation of this paper to try to search for references and seek collecting information to spread the benefits. The method applied is the critical literary review based on the use of theoretical references represented by books, references, scientific periodicals in addition to studies, research, and Arab and foreign scientific letters as well as seminars and official reports related to the subject of the study. This forms a scientific background for the study to use it as a source for collecting data and information provided that it is in the historical period between 2015-2020 AD.

After reviewing the literature, one of the most prominent results was that all references proved that information security is the most prominent challenge in cloud computing, and a number of studies have proposed encryption as one of the information security solutions in cloud computing, and the adoption of algorithms that ensure the integrity of information and data when stored. This paper also recommended the necessity of conducting specialized studies in finding applicable solutions to address the challenges and best use of artificial intelligence and machine learning techniques to deal with information security in cloud computing, with conducting applied studies about experiments that have proved successful in applying information security algorithms in cloud computing.

The paper consists of five parts, which review a number of previous literature and studies related to the topic, clarify the issue, review the results of the surveys that have been referred to in the same regard, and finally come out with the results, conclusion and recommendations, and a proposal for future studies.

RELATED WORKS

In this section, a number of related studies will be reviewed. Such works dealt with cloud computing and its challenges, especially the information security challenge. It is noticed that there is a lack of studies that dealt with solutions to avoid lack of information security assurance in cloud computing during the historical period between 2015-2020 AD. They were reviewed in chronological order from the most recent to the oldest.

Study [5] entitled "Data Security Methods in Cloud Computing", aims at analyzing the problems of ensuring data security in cloud computing according to current technological methods using the descriptive analytical approach. It also proposes a custom method to ensure data security according to its status. Despite that Cloud computing has many advantages, the use of equipment configured and managed by a cloud service provider (third party) to process, transfer and store data may cause concerns about maintaining security. Data management must be implemented during the transfer, storage and processing to ensure the minimum of the three characteristics of information security, namely safety, availability and trust while ensuring confidentiality using encryption, access control and authorization, and integrity through the use of mechanisms that prevent data modification and availability using different methods while facilitating access at any time to the required resources. In fact, although there are many methods of data security and cybersecurity, there are incidents of frequent data loss.

Study [6] entitled "Security of Cloud Computing Environment", aims at uncovering the challenges and opportunities in cloud computing. After reviewing and discussing cloud-computing security issues it confirmed that despite the many proposed security models for improving cloud security, there is no solution currently available to deal with all security issues. Therefore, future research should focus on resolving security issues. The study pointed out that in cloud computing, service providers must adopt a security system that can prevent unauthorized people from accessing their data or from controlling it by malicious people.

This can usually be maintained by using various detection, prevention, and coding techniques. The most important security issues in cloud computing are trust, integrity, availability, authentication and authorization, confidentiality, and resources. Organizations need cloud computing to reduce cost and increase efficiency. However, cloud security issues make organizations use the cloud for less sensitive and unimportant data and use their local network to preserve sensitive and important data.

Study [7] entitled "Cloud Computing Approaches, Characteristics and Cloud Computing Status in the Arab World" is a descriptive survey that aimed at presenting all the concepts that explain cloud computing, its approaches, services, advantages and interests that surround it, and its uses. It also presented a brief history of cloud computing technology development, specifically, on cloud computing technology in the Arab countries. It also clarified Data security which is one of the most important challenges. There are many concerns that cloud-computing services are seriously affected by network speed and energy status (meaning that low energy could lead to outages and service shutdowns).

Study [8] entitled "An Exhaustive Review on Security Issues in Cloud Computing" aimed at reviewing the various security challenges in cloud computing with the available solutions and specified that encryption keys must be managed so that the data is safe to prevent unauthorized access to the data. The study provided a detailed survey of various security challenges in the cloud with the proposal of a number of measures to overcome the threats.

Study [9] entitled "Security Storage of Sensitive Information in Cloud Computing Data Center", aimed at presenting a proposed algorithm to increase the security of information through the security storage of sensitive information in the (CCDC- Cloud Computing Data Center). This algorithm uses a feature set to filter sensitive information and uses technology to encrypt the sensitive information scanned. This algorithm also uses the principle of 3D storage for the security storage of sensitive information. The experimental results show that this algorithm can effectively enhance the security of CCDC-sensitive information.

The Study [10] titled “Information Security Risk Estimation for Cloud Infrastructure” is a descriptive study aimed at suggesting a risk assessment approach to assess potential harm from an attack on confidential data and justifies the need to include private clouds with a high degree of protection. The basic concepts that will be used in the proposed approach have been identified.

Study [11] entitled "Resource Sharing Security in Cloud Computing Environment" aimed at clarifying the negative aspects and challenges in cloud computing. The focus was on the security and privacy of data on the cloud and data protection where Data is not stolen by the third party, especially for applications in which the transfer of Sensitive data is made. Therefore, the study suggested a method of encryption with a high level of security and the lowest size of encryption keys while providing three basic elements for encryption, which are integrity, confidentiality and authentication.

Study [12] entitled "An Analysis of Threats and Challenges in the Deployment of Cloud Computing", aimed at reviewing a comprehensive view of the threats and challenges of cloud computing, to contribute to facilitating the operations of using cloud computing and increasing the efficiency of their work. The study used the investigative method over a sample of IT employees in order to gain a broad understanding of cloud threats and challenges. It revealed that data security still requires a lot of research effort to address this threat as well as the challenge of implementing a compliance, compromise, organizing and auditing data policy, in addition to the spending challenge, as there is only limited literature that discussed the issue of cost estimation. It also addressed the problem of interoperability and compatibility with platforms for cloud computing which will cause concern in the future due to the increasing number of service providers, consumers and regulators.

Study [13] titled “A Proposed Framework for Security Aspects of Cloud Computing Services in Information Technology Companies.” aimed at providing a practical reference to help IT companies and decision makers in Egypt analyze the security implications of cloud computing in their businesses. The study included a list of steps, along with guidelines and strategies, to evaluate and compare the safety offerings of different cloud service providers. It also proposed standards for security protection for the adoption of cloud computing in Egypt, in addition to an extensive study covering the latest applications of cloud computing in Egypt.

Study [14] entitled "Assessment of Cloud Computing Security Risks for E-Governance Infrastructure" aimed at addressing the approach by which the government interacts and relates to citizens, companies and employees in so-called (electronic services), and the role of using cloud computing, which reduced labor costs in IT by 50% and capital utilization improved by 75%. However, the challenge is security and data protection. The risks were evaluated for employing electronic services in computing engineering. The study demonstrated the necessity of assessing risks for computing and cloud users, especially decision-makers with regard to information security and protection.

Study [15] entitled "Security Challenges and Threats in Cloud Computing Systems" provided a critical review of the various vulnerable security issues of cloud computing systems.

It concluded that threat risks are the biggest problem facing users today, and also shed light on the different types of cloud computing applications and the potential threats associated with them. The analysis showed that cyber-attacks increase accompanies the increase in application usage.

Study [16] titled "Personal Data in Cloud. Russia Experience", clarified what is related to the security of data when it is stored in cloud computing. It answered the following question: Is it possible to ensure that the technology allowing us to access cloud computing is reliable and secure. What if the public information and IT systems were hosted abroad? The study concluded that in the Russian Federation there are not many examples of using cloud-based public service models. It explained that its results will be used in further scientific research aiming at defining approaches to organizing and securing the digital economy in Russia.

Study [17] entitled “The Gap between Cloud Computing Technology and the Audit and Information Security “analyzed the gap between rapid technological development and supportive standards and legislation in terms of information security. The study revealed that risks and controls are also subject to continuous change. Therefore, follow-up processes should always be adapted to the specificities of each organization. It explained that there is a gap between the rapid development of technology and the supporting standards and regulations trying to keep pace with it. For example, a company operating in Romania that uses cloud-based applications for management may find its software and data physically located in a different country, or even a different continent. Thus, a growing problem is how to ensure full compliance with regulations.

Study [18] entitled "Security in Cloud Computing: Opportunities and Challenges" is an exploratory study intending to find out details of the security problems that arise due to the nature of cloud computing. In addition to modern solutions, it stressed communications security among the challenges. Among the solutions mentioned was the use of two Deffie Hellman lines for key management, which is a cryptographic protocol that allows two groups of people who do not have prior knowledge of each other to create a shared secret key on an unsecured conversation channel. This key can be used later to encrypt subsequent conversations using a symmetric key encryption algorithm. It also uses the Merkle tree allowing verification and security in large data structures for more security and Data encryption with 128-bit Secure Sockets Layer-SSL (Secure Socket Layer) protocol.

Study [19] titled “What About Trust in the Cloud? Archivists' Views on Trust”, is an exploratory descriptive study that focused on understanding Trust-in-cloud solutions from a file archivist's perspective, exploring whether cloud computing has changed the role of archivist, and how archivists are responding to problems and challenges related to the cloud through interviewing twelve archivists in Sweden. It was revealed that their role has changed from being reactive to becoming proactive, i.e. ensuring that requirements, contracts and agreements between the organization and the Cloud service provider are valid and precise. Based on the conducted interviews, it revealed that their role changed due to the impacts of cloud computing and the introduction of cloud services in the field of archiving.

RESEARCH PROBLEM STATEMENT

In light of the huge increase of intellectual production, and heavy reliance on the World Wide Web, portals and digital information sources, the need for security and the need to secure websites, computers, software and information in various forms has increased. Information security also requires continuous follow-up and continuous updating of everything that keeps pace with the time changes in order to preserve information from any theft, modification, change or publication without a license.

The challenges of information security increased after the emergence of the so-called cloud computing service, a technology that changed the traditional ways in which services are deployed by institutions or individuals [3]; [4] It is a technology based on transferring everything stored on the computer to storing it in a cloud via a server and accessed via the internet. It is imperative to identify the challenges that faced this service, especially information and data security, and conduct studies to try to address those challenges and find solutions.

On this basis, this paper comes to reveal the challenges of information security in cloud computing. Thus, the study issue is answering the following question: "What the main challenges of information security are in cloud computing?" and the following sub-questions are derived:

▪ What is the main challenge that the studies have agreed upon?

▪ What are the main solutions?

▪ What are the deficiencies that were left after the survey study according to the searcher's point of view?

THE APPLIED RESEARCH METHODOLOGY

The method of critical review was used, where the analysis will be done through the use of theoretical references represented by Arab and foreign books, references and scientific periodicals in addition to Arab and foreign studies, research and theses, as well as seminars and related official reports. This work will cover the historical period between 2015-2020 AD. As a result, it is noticed that the studies agreed, regardless of their different references, that the biggest challenge and the most important threat to cloud computing is the protection of information and data. It also noticed that:

Study [5] proposes a customized method for ensuring data security so that it is combined with mechanisms that use machine-learning algorithms, through a dynamic learning process, and adapted to the type and real needs of data security. Thus, it guarantees the security of data in cloud computing if used and implemented correctly on the basis of control of data that is downloaded from the cloud, data protection and data management in the cloud through methods of concealment, access control, structure configuration and security event monitoring, information management throughout the Data life cycle, ensuring the auditing process, managing the physical location of the data centers and implementing strategies to ensure the availability and recovery of data in case of disasters, and the need to take into account the state of the data at a certain time (in use, transfer or sleep) in order to use different safety methods, as follows:

- Saved data (stored in certain memory locations). They are stored in the cloud on various physical media devices (hard disks and tapes) or virtual, in an organized or unorganized manner: databases, file servers, network storage units (NAS- Network Attached Storage) connected to the SAN- Storage Area Network, e-mail servers.

Depending on the contracted service in the cloud, it can also provide media storage that is sufficient for the amount of data for the needs of enterprises, with the possibility of expansion. There are also many methods of masking to process data in a silent state, such as encryption and coding.

- Data in transit (in the process of being transmitted over the communication channel). There are two cases when data is in transit either over the communication channel connecting the customer to the data center or crossing within the data center. To secure the communication channel, the most commonly used mechanisms are:

VPN-Virtual Private Network services and use of hardware encryption

- *Data Loss Prevention (DLP- Data Loss Prevention, URL-Uniform Resource Locator)*

- *Internet Protocol Security, SFTP-* Secure File Transfer Protocol

Transport Layer Security-TLS, SSH-Secure Shell.

- Data in use (data is in volatile memory, RAM, CPU, records or cache). The data used can be protected with full hard disk encryption. This study is one of the strongest recent studies that do not have gaps from the researcher's point of view as it covered the topic of information security from all sides in terms of presenting a poll and presenting a detailed proposal for information security in cloud computing, and the title of the study is fully compatible with its content.

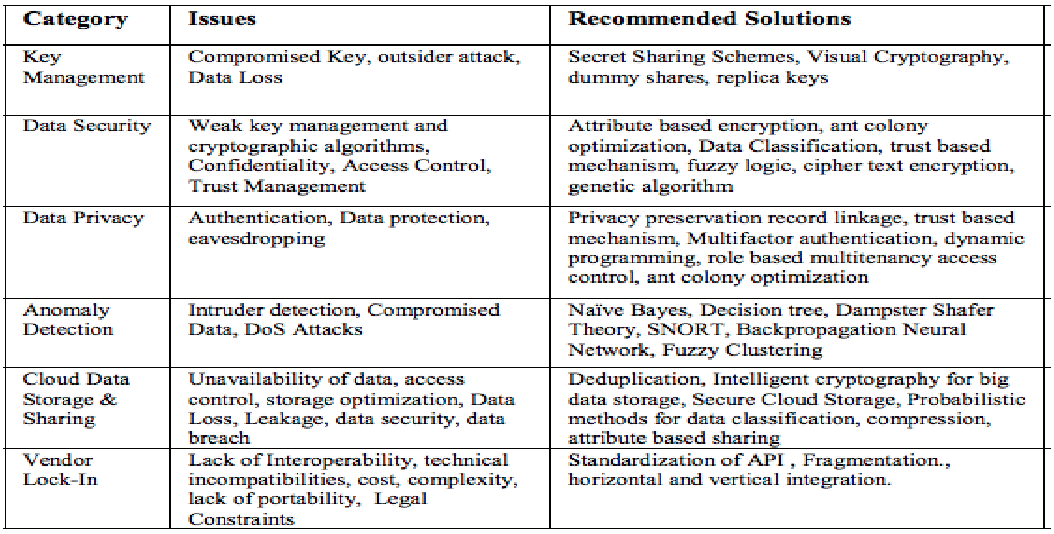
As for study [6], it agreed with all the studies that were referred to in terms of the most prominent challenges of cloud computing, which is the security of information. The study is very valuable from a descriptive point of view of cloud computing, but it did not provide solutions to ensure data security in cloud computing. And since the title of the study is general it is possible to develop it by adding application models and solutions to ensure the security of information in cloud computing after conducting a poll on the most prominent challenges of cloud computing.

Study [7] is considered important because it is one of the few recent studies that has dealt with Arab countries, and presented the documented facts related to the position of Arab countries in the field of information technology industry. It clarified the concerns in terms of information security and in terms of its loss, as cloud computing services are seriously affected quickly by the network and the state of energy (that is, the decrease in energy can lead to interruption and the suspension of service). The study also stressed what the Vision 2030 goals emphasized regarding the need to develop a strong cloud services industry in the Kingdom of Saudi Arabia to create an advanced digital infrastructure, which is necessary for the current progress Industrial activities. Arab countries are also receiving a lot of attention from leading companies in the field of cloud computing.

DELL also announced the introduction of cloud services to companies in the East and the Kingdom of Saudi Arabia. According to the researcher this study is one of the strongest recent studies as it covered all the aspects of the topic of information security in terms of presenting a survey and a detailed proposal for information security in cloud computing which makes its title fully compatible with its content. However, it lacks presenting proposals or experiments and solutions that have been implemented to ensure information security. It focuses on the most prominent challenges, which is information security and the extent to which data is affected by network speed and power status.

Study [8] agreed with studies [6] and [5] and with all the studies that have been referenced on the most prominent challenges in cloud computing, which is data security, but it reviewed a number of solutions through the use of the "Anomaly Detection" feature to discover unusual activities in the cloud in order to include security measures for the data on the cloud. It also clarified the "Vendor Lock-In" feature, which is a period specified by the cloud service provider for the user using the services. If the user is not satisfied with the services of the cloud service provider, he cannot transfer his data to another service provider until the lockout period expires. Therefore, the transfer of computing services and data from one service provider to another is very complex. The study was distinct by providing a detailed survey of the various security challenges in the cloud, as indicated by the title with the proposal of a number of measures to overcome the threats, including coding, classification and fuzzy logic. It was also distinct by presenting solutions in a table:

Table 1. *Challenges of cloud computing with suggested solutions [8]*



Category	Issues	Recommended Solutions
Key Management	Compromised Key, outsider attack, Data Loss	Secret Sharing Schemes, Visual Cryptography, dummy shares, replica keys
Data Security	Weak key management and cryptographic algorithms, Confidentiality, Access Control, Trust Management	Attribute based encryption, ant colony optimization, Data Classification, trust based mechanism, fuzzy logic, cipher text encryption, genetic algorithm
Data Privacy	Authentication, Data protection, eavesdropping	Privacy preservation record linkage, trust based mechanism, Multifactor authentication, dynamic programming, role based multitenancy access control, ant colony optimization
Anomaly Detection	Intruder detection, Compromised Data, DoS Attacks	Naïve Bayes, Decision tree, Dampster Shafer Theory, SNORT, Backpropagation Neural Network, Fuzzy Clustering
Cloud Data Storage & Sharing	Unavailability of data, access control, storage optimization, Data Loss, Leakage, data security, data breach	Deduplication, Intelligent cryptography for big data storage, Secure Cloud Storage, Probabilistic methods for data classification, compression, attribute based sharing
Vendor Lock-In	Lack of Interoperability, technical incompatibilities, cost, complexity, lack of portability, Legal Constraints	Standardization of API , Fragmentation., horizontal and vertical integration.

Study [9] also agreed with all the referred studies that information security is one of the main challenges of cloud computing and presented a proposed algorithm for increased security. This algorithm uses a set of features to filter sensitive information and uses technology to encrypt sensitive information that has been scanned. This algorithm also uses the principle of 3D storage for the security storage of sensitive information. The experimental results show that this algorithm can effectively enhance the security of CCDC-sensitive information. A proposed algorithm and its experiment characterized the study, and it was proved that the use of the proposed algorithm effectively enhanced the security of sensitive information from CCDC.

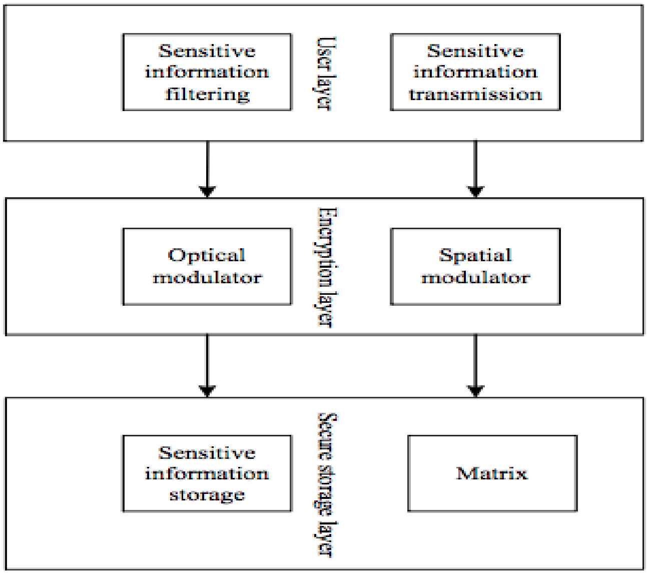

Sensitive information filtering
User layer
Sensitive information transmission
Optical modulator
Encryption layer
Spatial modulator
Sensitive information storage
Secure storage layer
Matrix

Figure 1. *Suggested algorithm [9]*

Study [10] was similar to studies [14] and [16] where the topic of risk assessment in cloud computing was addressed, but it was distinguished by the presentation of a risk assessment approach in this descriptive study to assess the potential harm of attacking confidential data and justify the need to include special clouds with a degree of High protection. This study is unique in following a proposed approach to assessing the risks of information security, as the studies dealt with the necessity of assessing risks without clarifying an approach for evaluation, and the title of the study is fully compatible with its content, but it lacks to present experiments that have been applied, and the results of those experiments.

Study [11] agreed with all the referred studies. The focus was on the security and privacy of data on the cloud, protecting data from theft, and not stealing data by third parties, especially for applications where sensitive data is transferred. The study proposed a method of encryption with a high level of security and the lowest size of encryption keys while providing three basic elements for encryption, which are integrity, confidentiality and authentication. Its goal was to develop a hybrid of symmetric and asymmetric encryption to achieve the three basic elements, as symmetric encryption uses one key for encryption and decryption. The encryption, therefore, is fast to implement. As for asymmetric encryption, it uses a different key for encryption and another key for decryption and thus is slow to implement. The study presented a proposal for new hybrid encryption protocols to achieve security in mobile cloud computing. The proposed protocol divides the plain text into two parties that are encrypted using two different encoding systems. These two systems are done simultaneously so that the time required to make coding for all regular texts is short as they are executed in parallel thus obtaining a lot of security with less time and achieving security services such as authentication, confidentiality, integrity, non-repudiation and availability.

The proposed hybrid encryption algorithm has been developed to secure data and information that is sent over the cloud. The goal of the hybrid cipher algorithm is to efficiently encrypt and secure the transmitted data. The study was characterized by presenting a protocol and a proposal to solve the problem of information security in cloud computing. Extensive experiments were also conducted to study the efficiency of the implemented hybrid encryption algorithm in encrypting and decrypting data in the least possible time. The hybrid-encoding algorithm was tested on different file sizes. This gave the study strength as most of the referenced studies that deal with challenges and threats, and a survey of opinions without describing a proposed solution. Its title is characterized by a brief explanation of the content.

Study [12] is similar to study [13] in terms of addressing the cost challenge in cloud computing in addition to the information security challenge. It aimed at presenting a comprehensive view of the threats and challenges of cloud computing, to contribute to facilitating the operations of using cloud computing and increasing the efficiency of its work as it relinquished part of the control over information security. The study used the investigative method as it targeted information technology personnel in order to gain a broad understanding of cloud threats and challenges, and revealed that data security still requires a lot of research effort to address this security threat as well as the challenge of implementing a policy. Data compliance, compromising, regulation and audit. Also, the spending challenge as there is only limited literature discussing the issue of cost estimation, and the issue of interoperability and compatibility with other cloud computing platforms is one of the problems that cause great concern in the future due to the increasing number of cloud service providers, consumers and regulators.

Despite the strength of the study and its analysis of the challenges facing cloud computing and the focus on information security as it represents the first issue of the threats and challenges of using cloud computing, it did not mention a solution that can be applied to avoid the information security challenge. As well, it did not address what is the specific problem such as data theft or modification. In addition, the analysis was only from the point of view of a sample of IT personnel. The study agreed with most of the literature that information security is the most prominent threat to cloud computing. The title of the study also has the advantage of briefly explaining the content without lengthening the title. However, the study sample category should be added to the title.

Study [13] demonstrated that failure to ensure adequate security protection when using cloud services can ultimately lead to the highest potential costs and losses to businesses. Among the results of the survey in the study were: It is imperative to achieve all aspects of security, to attract more customers, and the need to support technical companies and technicians to protect the client's application. There must be many service providers and all security agreements must be unified. It also explained security threats such as: seizure, loss of governance or control, the possibility of data loss or leakage, and the case when data is transferred to cloud services where it is possible to change the ownership of the data file. It stressed that this newly emerging technology can be successful and widespread in the future only if service providers with the help of governments put in place the necessary security agreements, so that all parties' rights are preserved. The study is strong, targeted and important. It included a survey and presented a proposal, in addition to a study of the current situation, but it is specific to the environment in Egypt, and it was better to clarify the study area (Egypt) in the title. The study also recommends trying to find a secure application development with Google APPS, or other engines, which would be economically feasible in the future of IT. It is also possible to expand the study in different areas to generalize the results.

Study [14], was similar to studies [10] and [16] in terms of addressing the necessity of risk assessment. It aimed at addressing the approach by which the government interacts and relates to citizens, companies and employees in the so-called electronic services. The infrastructure of the e-government is also mentioned. The latter was divided into 3 parts: the first part is the threat of virtualization, the second part evaluates the connection threats, and the third part assesses the data threats. The study demonstrated the necessity of assessing risks for computing and cloud users, especially decision-makers in terms of security and information protection, but it did not clarify any security measures, as it was mentioned that a number of security measures would be reviewed in future research.

Study [15] clarified the different types of cloud computing applications and the potential threats associated with them. The analysis showed that cyber-attacks also increase with the increase in the use of applications. The main issues were divided into the following categories: Internet threats, application-based threats, physical threats, and network-based security threats. The study also confirmed and agreed with all the reviewed literature that the problem of information security is one of the most important issues in cloud computing. And although cloud computing systems are capable enough to exchange information and services using the Internet without the need for any physical infrastructure, they are more vulnerable. In view of the security threats that must be solved, the study lacks presenting solutions, but it reviewed the concepts and issues of security in cloud computing in detail according to what the title of the study indicates.

As for the study [16], which is similar to [10] and [14], it identified the risks according to the following: The user does not have or cannot access the cloud, the safety of user data depends heavily on ISP-Internet Service Provider of the company. There are no generally accepted standards in the direction of cloud computing security, there is no specific answer about the responsibility of the party providing the service to the user, and the Internet service provider for personal data must guarantee the conditions for using electronic signatures. it also stated that its results will be used in further scientific research aimed at defining approaches to organizing and securing the digital economy in Russia.

The study clarified in its title the area in which it was conducted, specifically with regard to the security of personal data. This is considered a strong point in the title as it is clarified and defined from the researcher's point of view, and despite the descriptive coverage in the study, it needs to be re-applied in the future after the use of significant cloud computing. This allows ensuring interaction between the state and citizens, accelerating information interaction, achieving state services, and reducing costs.

Study [17] was distinguished by analyzing the gap between the rapid technological development and the supporting standards and legislation in terms of information security. The study revealed that with the rapid technological development, the risks and controls it addresses are also subject to continuous change. That is why the authors believe that audits and follow-up should always be adapted to each company's specifics, technology, and environmental risks. The study focused on information security legislation, as it was characterized by clarifying the legislations, but it did not work on practical experience, as it was based on a previous study to clarify the gap.

Study [18] illustrated the security of communications. Among the solutions mentioned was the use of two Deffie Hellman lines for key management. A cryptographic protocol that allows two groups of people who do not have prior knowledge of each other to create a shared secret key on an unsecured chat channel. This key can be used later to encrypt subsequent conversations using a symmetric key encryption algorithm. It also used the Merkle tree, which allows verification and security in large data structures for more security. It also suggested data encryption with a 128-bit Secure Sockets Layer-SSL encryption. The study is strong as it deals with the challenges of cloud computing with clarifying solutions for each challenge, which is clear from the title of the study, but it lacks practical examples.

Study [19] is distinct in terms of its aim, purpose and category. However, as was explained in the study, interviews were only conducted with Swedish archivists. So that the results of the study can be only generalized in similar circumstances. In addition, it is preferable to specify the study area in the title and to focus on solutions and determine the nature of the work of archivists in light of the transition to cloud services, and mechanisms to ensure information security.

RESULTS

In this section, we try to answer the main problem question and the sub-questions, and followed the survey approach resulted in the following points:

▪ (15) studies were referred to according to the historical period between 2015-2020, according to the following drawing: -

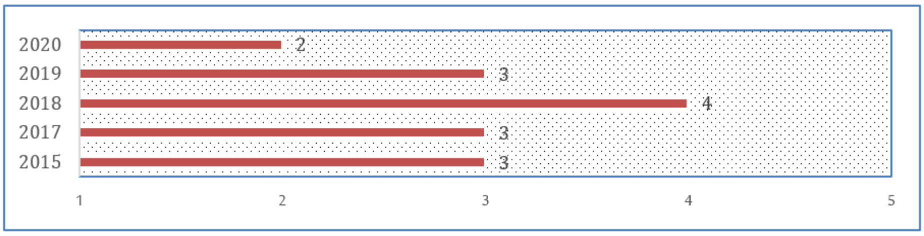


Figure 2. *The referenced studies against years*

▪ With regard to the question of the study issue about the most prominent challenges, it was clear that the studies agreed on the following challenges classified according to their frequency in the studies

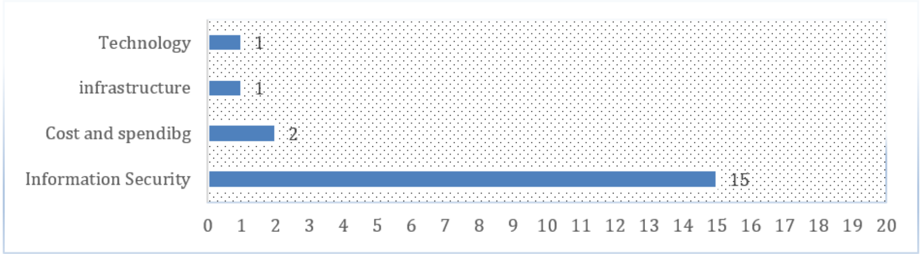


Figure 3. *Main Challenges Facing Security of Cloud*

It is noticed from Figure 3 that:

▪ Most studies agreed that information security is the most important and biggest challenge.

▪ The technical challenges are not mentioned in a large scale, and this may be due to the technical revolution in this era.

▪ With regard to the question of the study issue about deficiencies, and as far as the researcher knows, there is a lack of studies that dealt with applied experiments to ensure information security in cloud computing and a lack of studies that came up with an actual application system. Most of them provided recommendations and proposals to implement mechanisms that contribute to solving challenges and threats in cloud computing namely information security.

▪ With regard to the question of the study problem about the most prominent solutions, there were studies that came up with solutions according to the following figure:

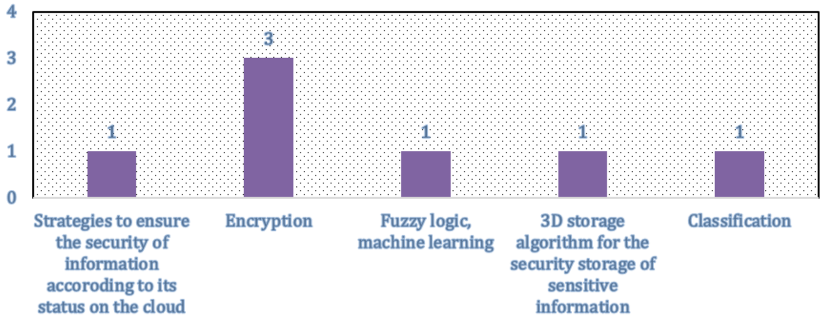


Figure 4. *Various suggested Solutions of Inf. Security*

According to Figure 4: -

▪ A number of studies agreed that encryption is one of the solutions that may prove to be effective for ensuring information security in cloud computing.

▪ Among the possible solutions that can be found [20]:

Encryption: where the plain text message sent from the sender is encrypted into a special format called "encrypted text" by applying some encryption algorithm and then transmitting it over the network. Then a text message is decrypted into the original plain text again by applying some decryption algorithm. Thus, only the sender and recipient of the communication can read the encrypted message and not anyone else.

This uses encryption to address network security problems. The following items must be known to whoever uses encryption:

▪ Data integrity: as the information has value only if it is accurate and correct, and this shows the need to maintain the accuracy and consistency of the data.

▪ Authentication: Deciding whom to talk to before revealing sensitive information or entering into a business transaction.

▪ Encryption cannot be refused: as it may deal with signatures and ensure that the party, contract or any person cannot deny the validity of his signature and send a message that it is created.

▪ Confidentiality: Keeping information from the hands of unauthorized users related to loss of privacy and identity theft.

Administrative controls which include guidelines and standards and provide a framework for procedures.

Technical controls which include access control, authentication, firewalls, and encryption.

Operational controls: The processes and procedures applied by individuals. It is based on management controls

Technological controls: disaster recovery, configuration management, incident response, and physical security.

Business owners and strategic decision-makers should assess the potential impact of cloud computing on their competitiveness, and assess critical security issues related to implementing cloud technologies.

A comprehensive set of guidelines must be formulated and the adaptation of the integration of data protection, trust and privacy policies. These guidelines may include developing a general policy for business cloud computing that highlights the organization's position on information protection, the governance of installing and connecting cloud computing when IT decisions are made, and financial auditing in terms of current IT and tax processes with embedding security and cloud audit practices.

Cloud computing security requires transparency, and one of the most important protocols in ensuring transparency within cloud computing is the availability of a legal agreement between the service provider and the customer including tracking and reporting, problem management, legal compliance, resolving disputes with the customer, security responsibility, and preserving confidential information. With the necessity that the service provider be responsible for maintaining the service quality guarantee.

Organizations must decide whether there are appropriate security measures in place to secure their data and applications or that they decide from the outset to share the responsibility jointly with service providers in the cloud computing environment, and typically web browsers usually store all the user's saved passwords, browsing history, and other sensitive information in one place. It is therefore possible for malicious sites to exploit these vulnerabilities in order to steal information associated with others, such as logging into an email account or online banking session. For this reason, some security experts recommend that consumers use one web browser for general browsing, and another for more sensitive tasks like online banking.

The customer must always make sure of the speed of his Internet connection and that the privacy of his information is not known to anyone but him, and the service provider must try to provide the best applications to protect the customer's data. Data protection is a participatory element between the customer and the service provider, and the system must include what reveals and verifies identity.

A breach testing system can be used to ensure that there are no vulnerabilities in the system. Some electronic clouds provide data processing tools and software tools that allow the customer to develop any code, which should be of high efficiency and not allow any unimportant data to be saved. The availability of the necessary policies and procedures that preserve the rights of the customer and the service provider.

Security must be increased whenever the sensitivity and confidentiality of the data increases, and this could be achieved by using different types of cloud, for example, highly confidential data should be used only at the level of the organization. As for the least confidential, it can use the integration between the organization and the service provider.

CONCLUDED COMMENTS & RECOMMENDATIONS

The paper aimed at limiting the challenges of information security in cloud computing, and thus contribute to finding appropriate solutions by programmers and specialists, and to take advantage of the characteristics and advantages of cloud computing to preserve intellectual production and facilitate access to it.

The following conclusions were made:

- The great similarity between researchers in the reviewed studies on the main challenges.

▪ Information security is the main challenge in cloud computing.

▪ Cloud computing may be an ideal solution for institutions, organizations and individuals, but there are many concerns related to technology services and it may contain defects or security flaws within the complex computing system and software. Therefore, it is imperative to apply security methods to preserve information on a large scale that depends on techniques to detect defects, understand their consequences, isolate their effects, and find appropriate solutions.

However, there are some observations that are worth noting in the following points:

▪ The studies lack the practical part that can be introduced and implemented.

The paper recommends the following:

▪ The necessity of completing specialized studies in addressing the challenges of cloud computing, especially information security, according to actual regulations that can be applied.

▪ Utilizing technology such as artificial intelligence and fuzzy inference in solving cloud-computing problems.

▪ Adopting "safe by default" systems, bearing in mind that security is not just a technology but must be linked to people and processes as well. Internet security should not be absolute, but rather needs planning, design and building as soon as the idea is born.

REFERENCES

1) Hassanein, Rajab (2012). Electronic information network security: risks and solutions. Cybrarians Journal. P (30). Available on https://bit.ly/39EaZKR. Retrieved October 16, 2020.

2) Al-Ghatbar, Khaled; Al-Hesheh, Soliman (2009). Electronic chasing methods and procedures available. Center of Excellence for Information Security. King Saud University. Riyadh. Available at https://bit.ly/37FBUn0. Retrieved October 16, 2020.

3) Gawali, Mahendra; Shinde, Subhash (2018). Task scheduling and resource allocation in cloud computing using a heuristic approach. Journal of Cloud Computing. Available at https://bit.ly/3lM4Grl, Received at 16/10/2020.

4) Al-Shutb, Radi (2015). “Communication and information technology systems. Cloud Computing Personal Blog 2. Available at https://bit.ly/3qsOoa2. Retrieved October 18, 2020.

5) BRUMĂ, Livia Maria (2020). “Data Security Methods in Cloud Computing”, Informatica Economical, Vol. 24 Issue 1, p48-60. 13p. Available at https://bit.ly/2JIzZFY, Received at 17/10/2020.

6) Karajeh, Huda; Maqableh, Mahmoud; Masadeh, Raed (2020). “Security of Cloud Computing Environment’, The 23rd IBIMA Conference Vision 2020: Sustainable Growth, Economic Development, and Global Competitiveness, Volume: pp. 2202-2215, Spain, Available at https://www.researchgate.net/publication/262378869_Security_of_Cloud_Computing_Environment, Received at 16/10/2020.

7) Aldossary, Shalhood; Saad, Aminah (2019). “Cloud Computing Approaches, Characteristics and Cloud Computing Status in the Arab World”, Multi-Knowledge Electronic Comprehensive Journal for Education & Science Publications (MECSJ). 2019, Issue 25, p1-18. 18p

8) Shahin, Fatima; Shish, Ahmad (2019). “An Exhaustive Review on Security Issues in Cloud Computing. *KSII Transactions on Internet and Information Systems*, 13, 6, (2019), 3219-3237.
DOI: 10.3837/tiis.2019.06.025.

9) Wang, Jia; Zhong, Li (2019). “Security Storage of Sensitive Information in Cloud Computing Data Center”, International Journal of Performability Engineering 15(3):1023-1032.
DOI: 10.23940/ijpe.19.03.p32.10231032

10) Tsaregorodtsev, A.V.; Kravets, O.Ja; Choporov, O.N.; Zelenina, A.N. (2018). “INFORMATION SECURITY RISK ESTIMATION FOR CLOUD INFRASTRUCTURE”, International Journal on Information Technologies & Security, № 4 (vol. 10), 2018, Available at https://bit.ly/39LjIuX, Received at 16/10/2020.

11) AbdElminaam, Diaa Salama; Hosny, Khalid M (2018). “Resource Sharing Security in Cloud Computing Environment”, International Arab Journal of e-Technology. Jun2018, Vol. 5 Issue 2, p47-57. 11p., Available at https://bit.ly/3qpnY9c, Received at 17/10/2020.

12) Yang Chong, Ngo; Humayun, Bakht (2018). “An Analysis of Threats and Challenges in the Deployment of Cloud Computing”, International Journal of Computing Network Technology. May 2018, Vol. 6 Issue 2, p63-69. 7p, Available at https://bit.ly/36DmRuR, Received at 11/10/2020.

13) Tahon, Amira Ahmed H.; Frahat, Farahat Farag (2018). “A Proposed Framework for Security Aspects of Cloud Computing Services in Information Technology Companies”, Scientific Conference of Information Systems & Computer Technology. 2018, Issue 26, p5-11. 7p., Available at https://bit.ly/3omjA9f, Received at 10/10/2020.

14) Srivastav, Riktesh (2017). “Assessment of Cloud Computing Security Risks for E-Governance Infrastructure”, International Journal on Information Technologies & Security, Journal of Network and Information Security, Volume 5 Issue 2 2017, Available at https://bit.ly/2JNpVLN, Received at 10/10/2020.

15) Khan, Hiba; Vasim Ahamad, Mohd; Samad, Abdus (2017). “Security Challenges and Threats in Cloud Computing Systems”, Volume 8, No. 2, March 2017 (Special Issue) International Journal of Advanced Research in Computer Science, Available at https://bit.ly/3oowR0S, Received at 11/10/2020.

16) Zharova, Anna; Elin, Vladimir; Panfilov, Petr (2017). “PERSONAL DATA IN CLOUD. RUSSIA EXPERIENCE”, Annals of DAAAM & Proceedings. 2017, Vol. 28, p1136-1142. 7p, Available at https://bit.ly/3qmVXzc, Received at 11/10/2020.

17) BENDOVSCHI, Andreea; IONESCU, Bogdan (2015).” The Gap between Cloud Computing Technology and the Audit and Information Security”, Audit Financiar. 2015, Vol. 13 Issue 125, p115-121. 7p, Available at https://bit.ly/39Mn00O, Received at 11/10/2020.

18) Ali, Mazhar; Khan, Samee U.; Vasilakos, Athanasios V. (2015). “Security in cloud computing: opportunities and challenges”, Information Sciences. An International Journal (Inform. Sci.) (20150101), 305, 357-383. ISSN: 0020-0255 (print). eISSN: 1872-6291, Available at https://bit.ly/39EXJFZ, Received at 11/10/2020.

19) Borglund, Erik A.M. (2015). “What About Trust in the Cloud? Archivists' Views on Trust”, Canadian Journal of Information & Library Sciences. Jun2015, Vol. 39 Issue 2, p114-127. 14p., Available at https://bit.ly/3g7ExSu, Received at 11/10/2020.

20) Mody, Rushabh (2017). Cloud Computing-Information Technology. Available at https://bit.ly/2I8qrnn. Received at 17/10/2020.