Journal of Computer and Communications, 2022, 10, 51-61
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Challenges of Privacy in Cloud Computing

Fatimah Khalil Aljwari

Computer Science Department, Umm Al Qura University, Makkah, Saudi Arabia
Email: 2100792@uj.edu.sa

How to cite this paper: Aljwari, F.K. (2022) Challenges of Privacy in Cloud Computing. *Journal of Computer and Communications*, **10**, 51-61.
https://doi.org/10.4236/jcc.2022.1012004

Received: October 12, 2022
Accepted: December 24, 2022
Published: December 27, 2022

Abstract

Now, cloud computing has grown from being a business concept to one of the fastest-growing segments of the information technology industry. Cloud computing is a group of resources, hardware, software, and services offered through the Internet or the network. Cloud also consists of five important characteristics, three service models and four deployment models. From the consumers' perspective, concerns about cloud computing security remain the essential inhibitors for cloud computing services, precisely related to the security and privacy issues of data in the cloud. This essay will go over .These difficulties include user data loss, data leakage, and privacy disclosure. A variety of cloud computing and service models are applied to boost an organization's investment returns, profit, and financial growth. For companies or governmental agencies to operate on the cloud, cloud computing offers a suitable environment and additional benefits or advantages. As a result, it has a number of problems with data security and privacy. The user's data are kept off-site and maintained by third parties. The consumers of cloud computing might be happy if the data are shielded from illegal access and misuse. Organizations and people who use the cloud are affected by the failure in data protection, which results in many challenges and problems, such as data theft. Concerns about privacy are also developing as "cloud computing" develops quickly and expands. For Open Systems and Internet applications, privacy has remained a touchy subject; the cloud suffers when discussing privacy. Adopting cloud computing services is only difficult because of privacy and security concerns. The challenges and solutions for cloud users and providers related to privacy and security are covered in this article. The document will provide researchers and security experts with information on privacy and security difficulties and solutions.

Keywords

Challenges, Cloud, Computing, Privacy, Saudi Arabia

1. Introduction

The name cloud computing was inspired by the cloud symbol that is usually used to illustrate the Internet in diagrams [1]. Cloud computing has been envisioned as the next-generation paradigm in computation. Several applications and computing resources such (as storage, memory, processing, servers, etc.) are delivered through the Internet as services in cloud computing to the users on-demand. Cloud Computing is suitable, the convenient environment of hardware and software computing resources that provide many services through the network or the Internet to satisfy users' or organizations' requirements on demand. [2].

Cloud Computing has now emerged as a new abstract model for hosting and delivering services over the Internet or the network. Cloud Computing uses several computing resources such as hardware and software resources provided as on-demand services through the Internet. The US National institute of standard and technology (NIST) defines cloud computing as a "model for enabling suitable, ubiquitous, on-demand network access to a shared pool of computing resources such as networks, servers, storage can be provided, edited and released quickly with minimal management effort or service provider interaction". Cloud computing presents appropriate on-demand network access to a shared pool of several computing resources. The resources refer to computing applications, processing, network resources, platforms, software services, memory, virtual servers, computing infrastructure, virtualization software, control software, and storage devices [2]. Cloud computing is recently receiving a great deal of attention among users. Another way of defining cloud computing is to examine its five essential characteristics mentioned in **Figure 1**, on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured services. On-demand self-service, the user gets services provided by Cloud as per his requirement without any human interaction. Broad network access makes cloud services available over the Internet so users can access any cloud service using the network through any client. Resource pooling characteristic makes resources available over the Cloud, and it gets access from anywhere by multiple consumers. There is no need to know where the resources are stored. Rapid elasticity tells that the Capabilities of cloud services as per consumer demand can be rapidly and elastically provisioned and available in an unlimited manner to consumers. Measured service monitor, control, and report, provide transparency for the provider and consumer of the utilized service [3]. Cloud computing presents several of services; these services put forwarded to three models as given in **Figure 1**, are software as service, platform as service, infrastructure as service. In SaaS, the applications and software already running on cloud infrastructure, consumers of cloud services can use it. These applications can be accessed from any location. An example of SaaS is salesforce.com, a CRM application. In PaaS, the cloud provider provides the platform as a service to the consumer where he can manage its application and use it without managing cloud

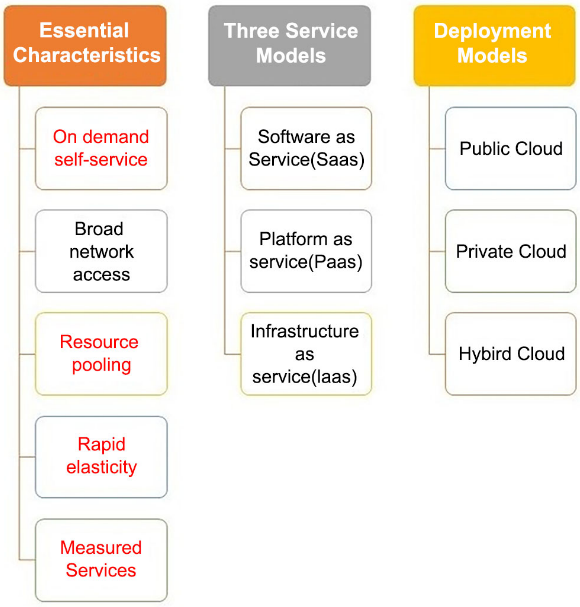


Figure 1. Introduction to cloud computing.

infrastructure. An example is Google Apps. IaaS type of service, cloud provider, provides an infrastructure where the consumer can manage its platform and application for its purpose. An example of IaaS is amazon web services (AWS). There are different types of deployment models listed by the NIST (2009) mentioned in **Figure 1**: Cloud deployment models are the public Cloud, the private cloud, and the hybrid Cloud.

The cloud infrastructure owned by a single person, single organization, or single business unit for their purpose is called Private Cloud. When cloud infrastructure is provisioned for open use by the public, owned, controlled, and operated by a business, academic, government, education organization is called public Cloud. At the same time, Hybrid Cloud is the cloud infrastructure that combines two or more distinct cloud infrastructures, private, public, or community clouds, together. Cloud Computing is continuously evolving and showing consistent growth in the field of computing. Cloud computing (so-called Cloud) represents one of the magnificent shifts in information technology which can enhance collaboration, agility, scaling, and availability, performance, functional, access and low-cost reduction through optimized and efficient computing [4] [5]. Many challenging issues face Cloud computing has attracted the attention of many researchers and service providers [6]. Cloud-based challenges have been classified into main categories: Security and Privacy. Each of these issues has affected the reliability and efficiency of Cloud-based environments [6]. The Cloud is susceptible to many Privacy and security attacks over the Internet. The biggest obstacle hindering the progress and the wide adoption the Privacy and security issues of the Cloud. Privacy is defined as "the ability of an entity to control what information it reveals about itself to the cloud/cloud SP, and the ability to control who can access that information". Cloud services have three basic models: Software as a service (SaaS), platform as a service (PaaS), and Infrastructures as a service (IaaS). Although these models have major differences, they share several security and privacy related issues [7]. Therefore, several concerns must be pointed out to deal with the privacy issues: • Who has access to personal data from cloud? • Where is it stored? • How many copies exist in a cloud? • How to be sure that it was deleted when requested? • Are laws and privacy policies respected by data actors? [8].

Many organizations, Small and medium, started using Cloud computing rapidly because of fast access to applications and reduced cost of infrastructure. But due to the constant increase in the popularity of cloud computing, there is an ever-growing risk of security and Privacy becoming main and top issues. Cloud computing raises several essential issues related to the privacy of consumers. Risk of comprises to confidential information through third-party access to sensitive information. This can pose a significant threat to ensuring the protection of intellectual property (IP) and personal information. Many laws have been published yet to protect the Privacy of individuals' data or business secret information. Since privacy problems still become more hazardous. The definition of privacy is the protection of the use of personal information of cloud users from authorized access [8]. Privacy is also defined as a fundamental human right related to collecting, using, disclosing, storing, and destroying personal data. Many issues for cloud users may create by Privacy breaches and Unauthorized access to the data in clouds. Cloud users expect high-level protection always for their sensitive data and application in the cloud. Violation of security leads to users' dissatisfaction. For example, maintaining sensitive data by organizations in the Cloud; however, data may be stolen by a third party. This paper mainly focuses on privacy Challenges in cloud computing. Privacy is the right and obligation of individuals and organizations concerning collecting, using, retaining, and disclosing personal information .definition by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Charted Accountants (CICA). The paper has been arranged as follows. The Challenges to Security and Privacy are described in section 2. Existing Solutions to Privacy are described in section 3. The conclusion is given in section 4.

2. Literature Review

Today, there are numerous innovative technologies. In light of this, cloud computing is a novel and innovative technology for the upcoming wave of Internet applications. As a new and quickly evolving computer paradigm, cloud computing has introduced numerous difficulties. As the following some Literature review.

In (Alferidah & Jhanjhi, 2020) [9], they proposed the about crucial to create techniques and policies that will safeguard IoT systems because of this which in turn safeguard critical information about persons. IoT system security and privacy have grown in importance and become a difficulty. The degree to which security and privacy issues are dangerous varies. There are attacks that are riskier than others. Attacks also vary in terms of where they come from; some are internal and others are external. Attacks can differ, but they always have the same negative effects and range in risk level. A review of the literature on IoT security and privacy was offered in this survey article. Additionally, the layer-by-layer discussion of IoT system security and privacy concerns.

In [10], they presented the study about the cloud computing environment is a new and quickly evolving computer scenario that poses a variety of difficulties. In this study, we have classified various existing solutions, discussed their strengths and weaknesses, and examined some important security and privacy issues in cloud computing. We anticipate three future research trajectories to safeguard the cloud environment based on the discussions.

In (Singh Bharati, 2020) [11], they discussed the study about Business tycoons purchase and study this vast data to assess public trends and moods. This information is essential for forming corporate policies. Big data is becoming popular and necessary to raise people's awareness of and sensitivity to society. Big data is analyzed by professionals in biotechnology and bioinformatics to forecast biological problems like cancer, HIV, hepatitis, allergies, etc. Data is obtained from a variety of sources and used for analysis and prediction. Big data has many problems, including storage, administration, security, and privacy. This essay concentrates on and thoroughly examines the problems, paying particular focus to security and privacy.

3. Challenges to Security and Privacy

It is the protection of transmitted data from passive attacks. The objective is to ensure that the customer's sensitive data is not being accessed or disclosed by any unauthorized person (**Figure 2**, The Privacy Issues of Cloud computing).

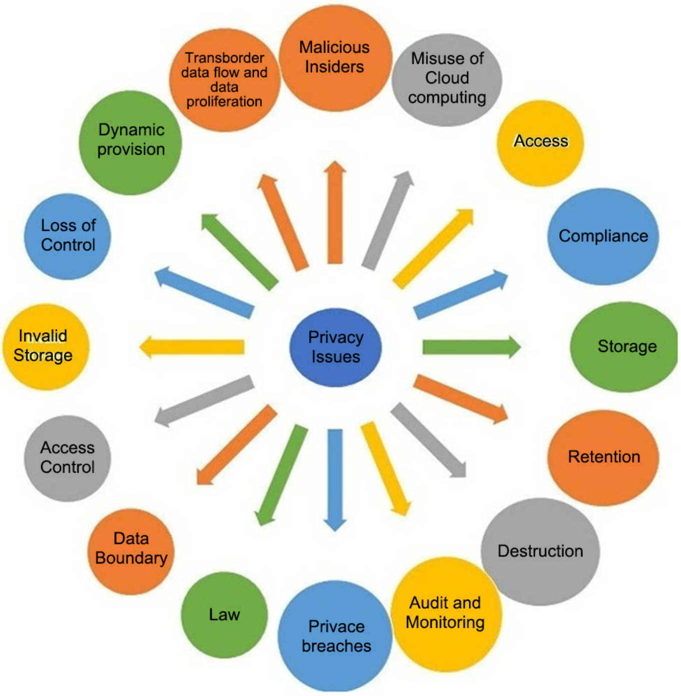


Figure 2. The Privacy issues of cloud computing.

The Internet of Things (IoT) is a wireless, interconnected system in which smart nodes (IoT devices) communicate with one another to exchange data across a communication channel. IoT technology is now crucial for anyone who wants to create intelligent systems that rely on technology. IoT created opportunities for improved human communication. However, the attackers allowed attacks on IoT systems to take advantage of users' private data [9].

Big data can be used to describe extraordinarily large amounts of information regarding things like jeans, cancer, pharmaceuticals, HIV, social networking sites, etc. Humans are attempting to decipher biological data to solve puzzles involving biological systems. People from other fields are drawn to big data. Big Data has more uses and applications than before, and it is gaining popularity in the biological streams of data scientists. The volume of big data is immense, and it is produced quickly from numerous sources. Thousands of posts are created on social media every second [11].

Although cloud computing is becoming more and more popular, a variety of security and privacy concerns are arising that slow the quick uptake of this new computing paradigm. Additionally, the advancement of defensive measures is being held back. To guarantee a secure and reliable cloud environment, it is crucial to recognize the shortcomings of current solutions and foresee potential lines of inquiry.

A service model known as "cloud computing" allows for convenient, on-demand network access to a sizable shared pool of reconfigurable computing resources (such as networks, servers, storage, applications, and services) that can be swiftly provisioned and released with little management work or service provider involvement [10].

4. Privacy Issues

4.1. Misuse of Cloud Computing

The provider gives unlimited access to network and storage at a limited cost, or sometimes they provide the free trial, so the type of things causes further harm to the cloud computing paradigm. Although the owner of the data has no control over or management over many businesses that deal with data proliferation, it is exceedingly challenging to guarantee that data backups or duplicates are not kept or processed by a specific authority; nonetheless, if such a request is made, all of these copies of data are deleted. Vendors don't need to worry about copied data being used in numerous data centers. The laws, rules, practices, standards, and contractual obligations for cloud users' data governance. The USA Patriot Act (UPA), the electronic communication privacy act (ECPA), and other laws are among the many procedures that are available to secure data in the cloud. The data of cloud users may occasionally be required by the government to uphold the rule of law in the nation. The aforementioned steps fell short of protecting privacy. The removal of user data from the cloud is a step in the destruction of this kind of problem. Without the user's consent, cloud providers are not permitted to erase a user's data. The cloud user must be able to recognize any violations and dangerous actions with the data they have access to. Real-time attacks on user data in the Google Service Provider occurred in the privacy violations. In January 2010, Chinese hackers attacked Google's information technologies. After that, they made the decision to shut down their sizable internet market in China because of the coordinated and deadly attacks on the clouds. Data may be stored on a secondary memory or inappropriate space of the cloud provider if the provider uses actual storage to store customers' data since the provider must pay for the consumption of storage. Therefore, this raises serious concerns about data privacy.

4.2. Malicious Insiders

Generally, providers may not reveal their employee's access to assets or resources; this helps the attacker to gain access to support or data [6]. The consumer saves their confidential or private data in the Cloud, yet no one can be held accountable for the security of that data. Therefore, there is a requirement for the Cloud to dynamically provision data. The physical location of the user's data in cloud computing is indicated by the definition of the storage. In cloud computing, there are numerous physical locations all over the world that are available for storage. Organizations typically do not feel comfortable storing their data outside of their data centers because doing so could result in unwanted access to the data and use for unauthorized purposes. Therefore, the cloud service providers cannot guarantee data transparency for customers and enterprises. Data storage period is indicated by retention. After the predetermined amount of time, the cloud-stored data must be erased automatically. Additionally, if the data is not deleted, cloud privacy concerns will arise. The problems with technology will change whenever it does. Therefore, technology is advancing daily. The regulations governing the issue, however, are not frequently revised. The cloud provider's stated policies, rules, practices, and standards must all be open and transparent. The cloud users will not be able to understand the rules and regulations if it is not transparent.

4.3. Malicious Insiders

Generally, providers may not reveal their employee's access to assets or resources; this helps the attacker to gain access to support or data [3]. Cloud service providers have easy access to each person's data. When a request is made to delete data from the Cloud, the user must receive the Confirmation after deletion. Data storage period is indicated by retention. After the predetermined amount of time, the cloud-stored data must be erased automatically. Additionally, if the data is not deleted, cloud privacy concerns will arise. The manner that cloud consumers watch cloud providers is a form of privacy concern. Because cloud services are not properly regulated, user data is misused and used for inappropriate purposes. The cloud provider will be the owner of the user's data while they are using cloud computing. If a user is eager to switch service providers, there is a chance that his data, which is already present in the data center of his current provider, could be threatened by misuse or manipulation. When a user doesn't use cloud-based data for a prolonged length of time, this happens. Inadequate access control permissions will allow unauthorized access to use the data in an illegal manner. To make several copies of the same data and make it available to consumers wherever they are, the cloud computing provider has performed. Multiple copies of the same data could result in data loss or leakage. It is necessary to eliminate any data that the data center has stored but hasn't used in a while.

5. Security Issues

Security: It is the protection of sensitive data from vulnerable attacks (**Figure 3**, The Security Issues of Cloud computing). There is various risk factors are involved with cloud computing which is explained as bellows:

5.1. Multitenancy

Multitenancy is nothing but one program that can run on multiple machines at the same time, but this causes vulnerabilities in the case of cloud infrastructure.

5.2. Access

The sensitive information in the cloud has many threats. An attacker may hack the data which is present in the cloud and which can be accessed and used later.

5.3. Availability

In the cloud, whatever the data user store so it should be available to that user at anytime and anywhere, but in the case of the cloud, there is the problem of backup recovery in case of failure. This resulted in a loss of confidence among the consumers.

5.4. Trust

In the case of the cloud, there are still lots of issues related to the cloud. There is

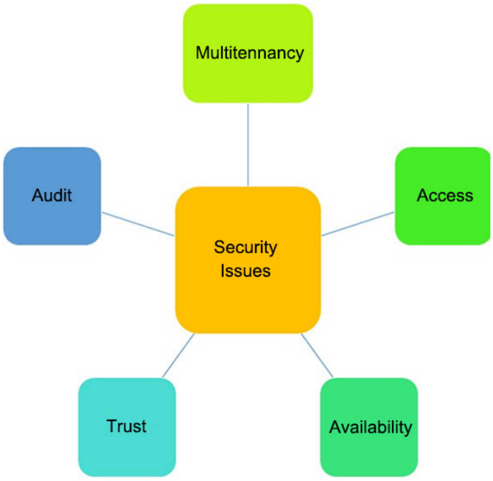


Figure 3. The Security issues of cloud computing.

still no trust relationship between the cloud provider and the consumer of the cloud one who uses the cloud. The consumer cannot trust entirely the provider about their private data to be stored on the cloud.

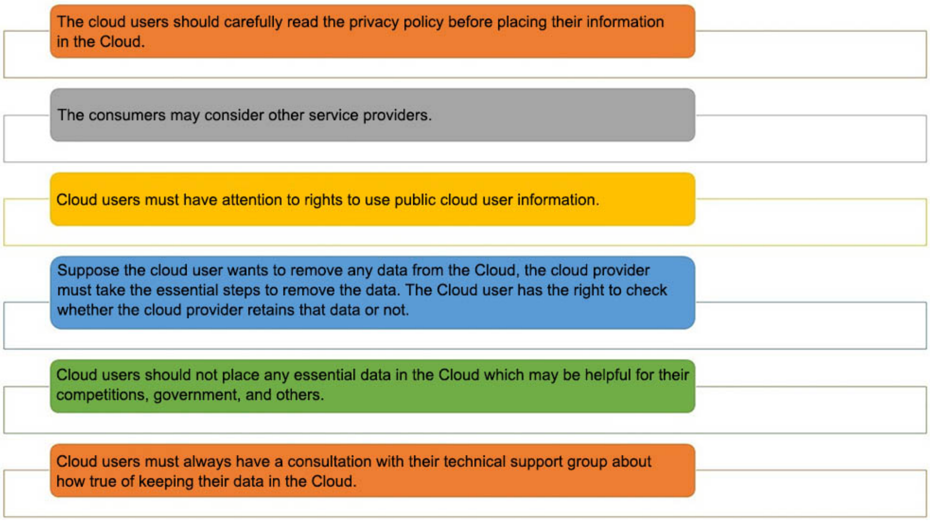
5.5. Audit

To implement internal monitoring control CSP, there is a need for an external audit mechanism, but still, the cloud fails to provide auditing of the transaction without affecting integrity.

6. Suggestions and Solutions to Privacy Issues

6.1. Solutions for Cloud Users

These solutions are given to the cloud users when consumers place their data in the Cloud (Figure 4):



The cloud users should carefully read the privacy policy before placing their information in the Cloud.

The consumers may consider other service providers.

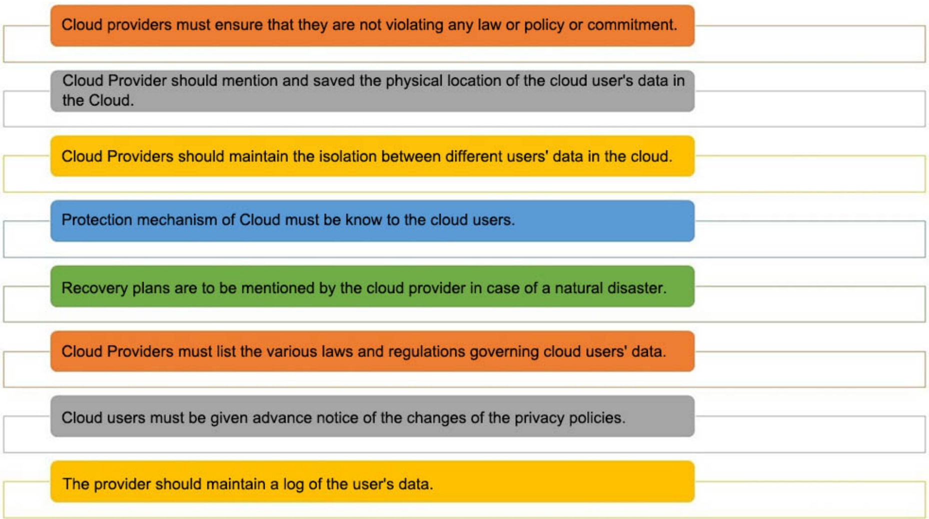
Cloud users must have attention to rights to use public cloud user information.

Suppose the cloud user wants to remove any data from the Cloud, the cloud provider must take the essential steps to remove the data. The Cloud user has the right to check whether the cloud provider retains that data or not.

Cloud users should not place any essential data in the Cloud which may be helpful for their competitions, government, and others.

Cloud users must always have a consultation with their technical support group about how true of keeping their data in the Cloud.

Figure 4. Solutions for cloud users.



Cloud providers must ensure that they are not violating any law or policy or commitment.

Cloud Provider should mention and saved the physical location of the cloud user's data in the Cloud.

Cloud Providers should maintain the isolation between different users' data in the cloud.

Protection mechanism of Cloud must be know to the cloud users.

Recovery plans are to be mentioned by the cloud provider in case of a natural disaster.

Cloud Providers must list the various laws and regulations governing cloud users' data.

Cloud users must be given advance notice of the changes of the privacy policies.

The provider should maintain a log of the user's data.

Figure 5. Solutions for cloud providers.

6.2. Solutions for Cloud Providers

To protect the user's data in the Cloud, the following suggestions for the cloud providers to maintain the user's data in cloud computing (**Figure 5**).

7. Conclusion

The rapid expansion of cloud computing, security, and privacy issues are being hampered by privacy violations, illegal access, and other issues. Researchers have put out a wide range of data privacy options. Between companies, users, and cloud service providers, trust is crucial. No organizations, governments, or businesses will, however, move their data, software, or information to the cloud unless customers and cloud service providers have established trust. The idea of trust is crucial for moving data to the cloud. Cloud service providers should nevertheless close many of the remaining gaps in cloud computing. Cloud service providers must put forth a lot of effort to get businesses to adopt cloud computing, distribute it extensively, and do so responsibly. This study looked into several privacy and security options for cloud computing to help users develop trust in cloud service providers. In this study, we discussed privacy-related problems, challenges, and solutions. Cloud computing technology is advancing quickly, notably in terms of processing capacity and response time. Whether through public service or privately for the enterprise, the public can now have considerably more experience with and chance to use cloud computing than they could a few years ago. In conclusion, educating the public about data privacy should be a priority for the development of cloud computing, as doing so can increase people's responsibility for how they handle their personal information, help them understand the value of internet security, and help them recognize the negative consequences of accidentally leaking sensitive information.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Lashkaripour, Z. (2021) Security and Privacy in Cloud Computing, *Journal of Management Information Systems*, **2**, 17-20.

[2] Sun, Y., Zhang, J., Xiong, Y. and Zhu, G. (2014) Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks*, **10**, 190903. https://doi.org/10.1155/2014/190903

[3] Kumar, S.N. (2015) Cryptography during Data Sharing and Accessing over Cloud. *International Transaction of Electrical and Computer Engineers System*, **3**, 12-18.

[4] Moghaddam, F.F., Ahmadi, M., Sarvari, S., Eslami, M. and Golkar, A. (2015) Cloud Computing Challenges and Opportunities: A Survey. In 2015 1*st International Conference on Telematics and Future Generation Networks* (*TAFGEN*), Kuala Lumpur, 26-28 May 2015, 34-38,

[5] Tari, Z., Yi, X., Premarathne, U.S., Bertok, P. and Khalil, I. (2015) Security and Pri-

vacy in Cloud Computing: Vision, Trends, and Challenges. *IEEE Cloud Computing*, **2**, 30-38. https://doi.org/10.1109/MCC.2015.45

[6] Sahmim, S. and Gharsellaoui, H. (2017) Privacy and Security in Internet-Based Computing: Cloud Computing, Internet of Things, Cloud of Things: A Review. *Procedia Computer Science*, **112**, 1516-1522. https://doi.org/10.1016/j.procs.2017.08.050

[7] Sravani, K. and Nivedita, K.L.A. (2019) Effective Service Security Schemes in Cloud Computing. *International Journal of Computational Engineering Research IJCER*, **3**, 30-35.

[8] Shankarwar, M.U. and Pawar, A.V. (2015) Security and Privacy in Cloud Computing: A Survey. In *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications* (*FICTA*) 2014, **328**, 1-11. https://doi.org/10.1007/978-3-319-12012-6_1

[9] Alferidah, K. and Jhanjhi, N. (2020) A Review on Security and Privacy Issues and Challenges in Internet of Things. *IJCSNS International Journal of Computer Science and Network Security*, **20**, 263-285.

[10] Liu, Y., Sun, Y., Ryoo, J. and Rizvi, S. (2015) A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions. *Journal of Computing Science and Engineering*, **9**, 119-133. https://doi.org/10.5626/JCSE.2015.9.3.119

[11] Singh Bharati, T. (2020) Challenges, Issues, Security and Privacy of Big Data. *International Journal of Scientific & Technology Research*, **9**, 1482-1486.