Critical Analysis of the Key Challenges Associated with Information Security and GDPR and its impact on the Cloud Computing Analysts

Ajith Jolly Puthiyedam

10349633

Dissertation submitted in partial fulfilment of the requirements for the degree of MBA CLOUD COMPUTING at Dublin Business School

Supervisor: GARRY PRENTICE

May 2019
Declaration

I Ajith Jolly Puthiyedam declare that this dissertation that I have submitted to Dublin Business School for the award of MBA Cloud Computing is the result of my own investigations, except where otherwise stated, where it is clearly acknowledged by references. Furthermore, this work has not been submitted for any other degree.

Signed: Ajith Jolly Puthiyedam

Student Number: 10349633

Date: 20/05/2019
Acknowledgement

I wish to thank some people at the completion of this research project those who guided me and inspired me on every step of the research project. Firstly, my sincere thanks go to my supervisor Mr. Garry Prentice who provided the required guidance and directions to me when required, and that proved helpful for me to complete the research project without any hurdle. At the next level, I wish to thank my parents who provided their valuable guidance to me during the entire journey of the research project. Their inspiration helped me to have a positive involvement in the research work and successfully accomplishing the final research project. I also want to thank my friends and relatives who provided their moral support and encouraged me on every step of the research work to keep my confidence level up and boost my morale in order to accomplish the entire research project in a successful way. I also want to thank almighty who bestowed me with great intellect and rendered me significant personality traits that proved helpful for me to accomplish this research project. My academic skills and knowledge level were a great source for me to complete this research project with the required degree of success.
Abstract

The main purpose of this research study is to analyse a critical analysis of the key challenges associated with information security and GDPR and its impact on cloud-computing analysts. In the global business environment, the issue with information security is continuously increasing such as data theft, leaking of confidential data of individuals, and using personal information of individuals of illegal purpose. The utilisation of cloud computing is increased by the different individual for the purpose of saving personal data, which also increase the illegal activities by hackers. The hackers are using advanced technologies as compared to the organisational security systems that negatively affect the confidential data of the individuals. In this context, the European Union has announced the implementation of GDPR in the year 2016 for the purpose of securing the confidential data of the users. Under the GDPR, the organisations are required to give full control to the users over their data so that they can manage their personal data. This can help the service providers to enhance the security level for cloud computing platforms. In addition, for addressing the aim of the present research study, the qualitative method is adopted because this research requires more in-depth and original information of this research. In this relation, the data is acquired by conducting an interview with 6 cloud computing analysts who are working in multinational companies in the UK. Moreover, through the thematic method, the interview data is interpreted appropriate and helped in presenting credible results. The results of the research are that the cloud computing analysts are confronting varied challenges associated with the information security and implication of GDPR such as increasing hacking activities, data theft issues, and compliance with the policies of GDPR. In this relation, varied strategic measures are presented in this research study for addressing the issue with information security and
implementing the GDPR in an organisation.
# Table of Contents

Chapter 1: Introduction .................................................................................................................. 8  
1.1 Introduction ............................................................................................................................. 8  
1.2 Research Background .............................................................................................................. 9  
1.3 Research Aim and Objectives .............................................................................................. 12  
1.4 Research Questions ............................................................................................................. 13  
1.5 Research Significance .......................................................................................................... 13  

Chapter 2: Literature Review .................................................................................................... 15  
2.1 Introduction .......................................................................................................................... 15  
2.2 Current Trends and Practices of Information Security Aspects in the Real World .......... 15  
2.4 Concepts and Significance of GDPR and Key Challenges in its Implication that are Faced by Cloud Computing Analyst .............................................................................. 21  
2.5 Key Strategic Measures for Addressing the Challenges Associated with Information Security and GDPR .................................................................................................................. 26  
2.6 Summary .............................................................................................................................. 29  

Chapter 3: Research Methodology .......................................................................................... 31  
3.1 Research Paradigm .................................................................................................................. 31  
3.2 Research Approach ................................................................................................................ 32  
3.3 Research Design ..................................................................................................................... 33  
3.4 Data Collection Tools and Techniques .................................................................................. 34  
3.5 Sample Size and Sampling Approach .................................................................................. 35  
3.6 Data Analysis Tools .............................................................................................................. 36  
3.7 Ethical Considerations .......................................................................................................... 37  

Chapter 4: Data Analysis, Findings, and Discussion .................................................................. 38  
4.1 Introduction .......................................................................................................................... 38  
4.2 Thematic Analysis ................................................................................................................ 38  
4.3 Discussion ............................................................................................................................. 51  
4.4 Summary .............................................................................................................................. 53  

Chapter 5: Conclusion and Recommendations ....................................................................... 55  

5.1 Introduction ................................................................. 55
5.2 Conclusion ................................................................. 55
5.3 Study Limitation ......................................................... 58
5.4 Recommendations .................................................... 59
5.5 Future Implications .................................................... 61
References ........................................................................ 63
Appendices ..................................................................... 71
  Appendix 1: Interview Questionnaire ............................ 71
  Appendix 2: Interview Transcripts ................................. 72
Chapter 1: Introduction

1.1 Introduction

In the present information technology world, cloud computing practices have a high prevalence to make the processes faster and efficient of managing the data and resources. Cloud computing is a network, which is widely used by large numbers of organisations in the contemporary business environment in order to enhance the productivity, data security, and organisational performance (Buyya et al., 2009; Wamuyu, 2017). The utilisation of cloud computing reduces the cost of acquiring additional hardware for storing important data. Cloud computing also minimises the time of storing the data, and it is considered safe, as the chances of losing the data are minimised. Cloud computing network allows the organisations and individuals to store their personal data and further it can access and share in an easier manner (Jangjaimon and Tzeng, 2015). Despite having significant advantages of cloud computing-based services, there are also associated issues related to information security in cloud computing-based services. In cloud-based services, the key challenges faced are related to data security and privacy. The breach of data and hacking are the major critical, critical information security issues that are faced by the cloud computing analysts in governing cloud-based services (Seo et al., 2018; Hashem et al., 2015). It is evident that in cloud computing, there is a chance of losing the confidential data and it can be accessed by other people using different hacking process and mechanisms that entail self-healing. The different reasons that lead to data breach from cloud computing mainly include inappropriate programming, open ports to the firewall, software vulnerabilities, and in-existent load-balance algorithms (Ahmed, and Hossain, 2014).
It is important for the cloud computing service providers to improve the security levels and deliver more effective services to the organisations and individuals so that the stored data can be protected from the hackers (Hashem et al., 2015). There are different types of cloud computing services are available like a public cloud, hybrid cloud, private cloud, and community cloud (Chou, 2015). The users adopt the type of cloud services as per their needs and want; however, both users and cloud service providers are not sure about the data security because the illegal activities from the hackers are increasing continuously. In order to keep a check on the information security-related issues, the introduction of General Data Protection Regulation (GDPR) is a significant measure, which is introduced for the purpose of protecting the data stored in the cloud platforms. GDPR provides a strong base and directional path for securing data and information shared on clouds. The aim of GDPR is to enable the individuals to have full control over their personal data, as they can access and share the data from anywhere and anytime (van Ooijen and Vrabec, 2018). In the implication of GDPR, varied critical challenges are faced by the computer analysts in terms of having a good understanding of the key technical measures and practices that are essential for implementing GDPR in information security processes. Inappropriate implementation of the GDPR in an organisation for data protection can lead to the heavy loss of the data (Goddard, 2017). In this context, the present research study is focused on examining the key challenges that are associated with information security and implication of GDPR and its impact on the cloud-computing analysts.

1.2 Research Background

Different studies are developed with respect to the challenges in the information security and implication of GDPR. Thus, it is reviewed from the study conducted by Goddard (2017) that in the current environment, the chances of losing the data from
different cloud computing platforms is increased because of illegal practices of hackers. Most of the organisations utilise cloud computing in order to save their data because it reduces the cost and time and improves the efficiency of the organisational practices. However, organisations and individuals are facing critical challenges in securing confidential data because the problem of data leakage is increased in the current scenario. Thus, it is significant for service providers to implement the most effective methods and to programme to develop the most secure platform of cloud computing (Goddard, 2017). In addition to this, Team (2017) and Politou, Alepis and Patsakis (2018) have described that in order to increase the level of information security, GDPR was announced by European Union in 2016, and it was implemented in the year 2018. General Data Protection Regulation is a regulation imposed by EU law on information security. The main purpose of GDPR is to give complete security over the data stored by the organisations or individuals within the European Union. It has been observed from the study that as per the regulation of GDPR, every individual has complete control over their data stored on the cloud services. Compliance of GDPR can increase the working process for cloud computing analyst, as in accordance with the GDPR, there would be varied limitations for the organisations to control the personal data of customers on could computing platforms (Team, 2017; Politou, Alepis and Patsakis, 2018).

However, Channon, McCormick and Noussia (2019) and Greengard (2018) have stated varied challenges that are associated with the GDPR that can affect the overall functioning of an organisation and implementation of GDRP can also have an adverse impact on the cloud computing analyst. Inappropriate implementation of GDPR can affect the business profits because the guideline of EU laws, a heavy penalty will be imposed on the organisations. In addition to this, GDPR was came in action in 2018
and most of the cloud computing analysts are not familiar with the concept of GDPR and implementation of GDPR can affect their overall performance in an organisation that can leads to the increase in the chances of data leakage (Channon, McCormick and Noussia, 2019; Greengard, 2018).

From the perspective of Chiappetta and Battaglia (2018), it is evident that there are varied challenges are associated with the implication of the GDPR in an organisation, as for the compliance with GDPR, a large number of requirements must be integrated with the information security of an organisation. It is vital for every organisation to ensure the policies related to personal data usage, access, consent, deletion, and rectification must be implemented in accordance with the GDPR regulations. Integrating policies of GDPR is a time-consuming and lengthy process that can affect the efficiency of an organisation (Chiappetta and Battaglia, 2018). In the views of Mittal and Sharma (2017), GDPR is a new regulation that includes different procedures and concepts, and people are not well aware of these procedures and concepts. The implication of GDPR can adversely affect the performance of employees because using new regulation with all new procedures and policies require effective training for the employees. Thus, implementation of GDPR in an organisation requires huge cost, as the organisations have to give training or recruiting new talent who have significant knowledge about the GDPR. In addition to this, the implications of GDPR are challenging for the organisations which are providing cloud-based services to the citizens of the EU. The organisations have to maintain transparency with the customers about their data, and they are also required to share information related to their data (Mittal and Sharma, 2017). It is also evident from the study conducted by Burton et al. (2016) that organisations also have to change their designing of security system, as they have to include data erasure algorithms, in
which they have to give access to the customers to ask for erasing their stored data in
the organisational hardware. Thus, this can have an adverse impact on the
organisational operations, and as per the guidelines of GDPR, the organisations need
to protect the data of the customers because if any breach of data happens in future,
the organisations have to pay heavy fine (Burton et al., 2016).

1.3 Research Aim and Objectives

Aim

The main purpose of the study is to analyse the challenges associated with
information security and GDPR and their impact on cloud computing analysts. In the
light of this aim, the research study is primarily focused on examining the range of
challenges related with information security aspects and other challenges that are
faced by cloud computing analysts in the implication of GDPR.

For the accomplishment of the aim of the study, key objectives are developed,
which are given below:

Objectives

- To examine the current trends and practices of information security aspects in the
  real world
- To identify the challenges associated with information security-based processes
  that are faced by cloud computing analysts
- To determine the significance of GDPR and key challenges in its implication that
  are faced by cloud computing analysts
- To determine key measures for addressing the challenges associated with
  information security and GDPR
1.4 Research Questions

The formulation of the research question is one of the critical steps for the identification of the key issues or areas that are investigated in the research. In this regard, the research question guiding the present study can be formulated as follows:

“What are the key challenges in information security and implication of GDPR within cloud computing-based processes and for cloud computing analysts?”

1.5 Research Significance

The main focus of the present research study is to critically analyse the key challenges that are associated with the information security and implication of GDPR and its impact on the cloud computing analyst. The present research study will explore the critical challenges that are associated with the information security and implication of GDPR with the specific context to cloud computing. Cloud computing is a network that allows the organisations to store the data and different individuals can also store their personal data in different cloud application (Buyya et al., 2009). In the current business environment, organisations are providing the services of cloud computing to the individual for securing the data from potential threats. However, the chances of losing the data from cloud computing are increasing due to a breach of data and hacking (Hashem et al., 2015). In this relation, GDPR is a framework that mainly focused on securing the data of every individual and giving significant rights of the individuals to have more control over the data they have stored in the cloud.

With this respect, it has been observed that there are limited researches has been conducted on the challenges in information security and implication of GDPR and its impact on the cloud computing analyst. Thus, the aim of this research work is to present in-depth, updated information related to the topic that bridge the gap of existing research work and it help the readers and future researchers to have
significant knowledge about the issues associated with the cloud computing and implication of GDPR. In addition to this, this research will also have a significant contribution for the cloud computing service providers to understand the key challenges associated with the information security and implication of GDPR and measures that can help in overcoming with the challenges. This research has used a qualitative research method for collecting the data in which the interview method is applied. With the help of interview method, the data will be collected appropriately in order to address the aim of the research study. The use of interview method help in collecting the detailed and updated information about the current challenges that are associated with the information security and implication of GDPR and their impact on the cloud computing analysts.
Chapter 2: Literature Review

2.1 Introduction

The importance of cloud computing is increasing, as large numbers of organisations are utilising the services of cloud computing for the purpose of saving the confidential information. However, there are varied risks associated with the utilisation of cloud computing such as losing of data and increasing activities of hackers. Development of cloud computing nowadays is happening at a fast pace and as a reason that a high number of cloud service providers are joining the cloud market. Cloud computing is a model that provides convenience, on-demand access to the network having pooled resources that can be easily accessed without any intervention of service provider (Liu, Esseghir and Boulahia, 2016; Chou, 2013). In this context, the following literature review is based on critically analysing the secondary resources pertaining to the key challenges that are related to information security and GDPR and their effect on cloud computing analysts. In this regard certain themes are have been evolved in the light of research objectives in order to centralise the literature that is assembled on the research topic.

In order to analyse the challenges of information security and GDPR, the literature review includes the analysis of current trends and issues in information security, and benefits and challenges of GDPR in cloud computing. Moreover, the chapter also includes identification of the measures for addressing the associated challenges of information security and GDPR.

2.2 Current Trends and Practices of Information Security Aspects in the Real World

The present business world is experiencing a great transformation in the field of technology. The advent of new technologies in the era of information technology has
opened several new avenues for computer specialists and IT experts. The information
technology-based processes have made the real-world business practices faster and
efficient however at the other side the issue of information security has evolved at the
same time. The study conducted by Cavusoglu, Cavusoglu and Raghunathan (2004)
has revealed that information technology has increased the interconnectivity of the
computers as a result of internet related advancements; however, it has also increased
the crimes related to information security. With the emergence and growth of
information technology means, the probability of cybercrimes and information
security-related issues have increased. As a result of this, several new trends and
practices are adopted by IT-based companies and experts. This has been evident that
in the real world, the information security related crimes have jumped up in recent
years. Due to the issues of the security breaches, the business organisations have been
facing increased cost burden of security breaches. The changing trends of information
security have posed a burden on the organisations for facing the loss of credibility and
increased corporate liability (Cavusoglu, Cavusoglu and Raghunathan, 2004).

In the same alignment Appari and Johnson (2010) have affirmed that in order to
ensure a good degree of information security, the organisations are adopting several
new practices such as digital recording and tracking systems, adoption of new
information security regulations and increased information exchange in a secured
manner. All these practices have become essential for better information security in
organisations (Appari and Johnson, 2010). Information security has become a new
discipline in the era of information technology in order to keep a check on the
information security risks. In the management information system, new advancements
have been made such as tracking of the unauthorised access of computer data (Appari
and Johnson, 2010).
According to Narain, Gupta and Ojha (2014), several software, which are related to information security, are there in the market. They are made by the well-reputed large companies which are known for computer hardware, and reputation is gained by the small firms also because of the repair done by them after the information security breach. Some of these applications even protect the information from Advanced Persistent Threats (APTs). Whereas, some other applications says that they will protect the data from malicious communication and unauthorised access. The adoption of such applications by the organisation can play an essential role in information security. There is a framework which is in current trend that helps in security of the information. Some key points of that framework are organisation should maintain awareness of all the configuration changes that are happening in the infrastructure. Access control policies should be implemented so that monitoring, detection, and prevention of malicious activities across every point even including desktops, laptops, and server could be done. Monitor and block known bad and unknown applications which reasons information breach are. Organisations should detect, prevent, and remove the software which is malicious from online and offline networks. It there is an information breek organisation should determine which software and data are affected so that serious actions could be taken on an urgent basis. Lastly, monitoring all the software which are coming through the online gateway which may contain viruses, if the organisation correctly implements this framework then there will not be any information breach in the future (Narain, Gupta and Ojha, 2014).

Chen, D. and Zhao (2012) have affirmed that there are several new trends in the present world that are changing the old measures which were used by the organisations, these trends discussed below. Oraganisations are nowadays using a
safer browser for any transaction and especially for those transactions which are confidential because there is the threat of stealing the data on the web applications persists, and web servers are the best platform to breach the information. These days, large, medium and small-scale organisations are shifting to cloud computing services because these cloud computing services are providing security to the data stored in them by any individual or organisations. APT (Advanced Persistent Threats) is a very high level of cyber crimeware because attackers are growing bolder organisations following a trend by improving their security. Encrypting the data is one of the best trends that are currently present in the real world because, in this, the data or information is encrypted using an encryption algorithm which is difficult for hackers to decode. Most of the organisations are currently following these trends for better information security (Chen and Zhao, 2012). Appari and Johnson (2010) have asserted that the adoption of GDPR and other federal regulations to impose them on the organisations is also a significant measure in the field of information security in recent years (Appari and Johnson, 2010).

2.3 Challenges Associated with Information Security based processes that are faced by Cloud Computing Analyst

In the views of Romansky (2012), cloud computing refers to the delivery of computing services such as databases, storage, software, and intelligence over the internet with the intent to offer flexible resources and faster innovations. Cloud computing renders the facility of sharing resources including infrastructures, and software with the help of virtualisation. Moreover, cloud computing is utilised for facilitating on-demand network access to configurable computing devices that are available on a shared pool (Romansky, 2012). Liu, Esseghir and Boulahia (2016) have also reviewed that the facility of cloud computing has allowed the organisations to
store their data with easy accessibility and sharing facility. If the data is easily accessible, it will reduce the idle time and during that time, other productive work can be accomplished. In the current business environment, the utilisation of cloud computing has been increased among organisations for different purposes such as storing documents and sharing information. One of the major services provided by the cloud computing organisations is security of the stored data, which attracts every individual and organisations to adopt cloud computing (Liu, Esseghir and Boulahia, 2016).

However, Chou (2013); Avram (2014) there are several critical challenges associated with information security faced by cloud computing analysts such as privacy and security, connectivity and open access, reliability, changes in IT organisations and political challenges. Security and confidentiality of the data is a significant challenge that a cloud computing analyst faces because cloud computing is more or less a new computing model that is why it difficult for cloud computing analysts to achieve security at all the levels. Cloud computing provides open access and connectivity to each, and everyone and that is why it is challenging for cloud computing analysts to monitor each and every malicious activity at every point. Reliability issue related to cloud computing is not a new thing, and this is because of the recent increase in the volume of cyber-attacks that is why it is challenging for cloud computing analysts to make people believe that cloud computing is reliable. In IT organisations trend changes at a very high pace as soon as the trend changes could computing analysts have to improve services related to cloud according to the trend. In the world of cloud computing, there is the variability of places where physical data resides, where all the processing is done and where the data is going to be accessed. These are the reason why several rules and regulations that applies to cloud
computing and it is challenging for the cloud computing analysts check compliance with all the laws and regulations while forming a cloud. The enhancement in the facility of cloud computing has also increased the issues of data security for cloud computing analysts. In the global business environment, securing the information in the cloud platforms become difficult for every individual and the organisations to protect their data in the cloud platforms because the issues of data leakage are increasing. In cloud computing, maintaining privacy is the biggest issue for every individual, as the users lose control over their confidential data because the data is stored on the computer of service providers. Thus, the chances of losing the data are high from cloud platforms (Chou, 2013; Avram, 2014).

From the perspective of Svantesson and Clarke (2010), it is evident that the activities of hacking are continuously increasing and due to this, the cloud service providers are facing challenges in securing the personal data of the users. The service providers mainly focused on overcoming the issues they face related to a data breach by adopting more enhanced security systems and hiring professions who have the expertise to deal with the data breach issues. Hacking is considered as a major issue in protecting the confidential data of users, as the cases of hacking is increasing nowadays. In the current environment, data security is the major concern for every individual, organisation, and service provider. However, the illegal activities of the hackers are affecting the capabilities of cloud service providers that make the users and providers of cloud service vulnerable. The issue of cybercrimes is significantly increasing, which is affecting the daily operations of organisations, and it is also creating a complex situation for the cloud computing analysts to secure the data of their users (Svantesson and Clarke, 2010). In a similar context, Chen, D. and Zhao (2012) and Jathanna and Jagli (2017) have reviewed that the amount of data stored is
increased at different cloud platforms due to this the service providers become the attractive targets for the hackers. The cloud computing analysts are confronting varied issues such as data breach through hacking and illegal access that create challenges for cloud computing analyst to protect the data of the users because hackers majorly utilise multiple systems in order to conduct cyber-attacks on the computers of the users (Chen and Zhao, 2012; Jathanna and Jagli, 2017).

2.4 Concepts and Significance of GDPR and Key Challenges in its Implication that are Faced by Cloud Computing Analyst

From the study of Wachter, Mittelstadt and Russell (2018), it has been identified that the European Union introduced the General Data Protection Regulation (GDPR) in the year 2018. This regulation has been developed in replacement of the Data Protection Directive that was established in 1995. The main aim behind the establishment of GDPR is to enhance the level of protection of that personal data of any individual or organisation that is present in Europe or even outside the Europe. This regulation ensures that only the individuals are in charge of their personal information, as no organisational personnel holds the authority to control the personal data of the individuals. Protection of information of any individual or organisation is very important and with the implementation of GDPR, information can be protected from the hackers up to a significant level. With the help of GDPR regulation, the EU citizens can easily understand the manner in which their data is being used, and if the individuals found any issue with their data, they can also file a complaint to the authorities in order to ensure the security of their data. Thus, rules and regulations that are provided by GDPR if implemented properly, it will be really helpful in increasing the security related to personal data of any individual or organisation. The study has also explored that GDPR is a significant regulation because it includes amendments
that focus on the protection of the user’s personal information that goes through various modern technologies. GDPR is the only law, which protects the personal information of any individual or organisation from hackers or any other kind of data theft process, who focuses on information breach. Some of the specific points that show GDPR is significant in the present world are data security and protection of personal data. The previous laws which were used by EU of data security have been outdated and are not effective to protect security to the people regarding their personal information. Therefore, there is a need for the lawmakers to make amendments or bring new law, such as GDPR, to ensure the protection of personal information of people. Nowadays cloud computing services are increasing day by day, and most of the individuals and organisations are also adopting it, so as to keep their personal and private information secure. This shows a need for the development of a new law so as to fulfil the needs of the users, in terms of data security. It has been identified that with the increasing modern technologies, personal information is at high risk, which requires GDPR implementation (Wachter, Mittelstadt and Russel, 2018).

As per the report of Information Commissioners’ Office (2018), GDPR provides eight rights to every individual, these rights are the right to be informed, the right of rectification, the right to access, the right to erasure, the right to data portability, the right to restrict processing, the right to object, and the right to automated decision making. The right to be informed in the GDPR means that individual has the right to be notified when there is any collection or use of the personal data of the individual. This requirement is the key transparency requirement, which exists in GDPR. The right to access means the individual has all the right to access his data. This right is commonly known as the subject access. Right to rectification is provided in GDPR, which means that an individual can rectify any data, which he/she think is incomplete.
Right to erasure is most significant right that GDPR provides in this the individual can ask the personal data to be erased whenever he wants this right, which is also known as ‘the right to be forgotten.’ The service provider has the right to delete all the data physically. The right to restrict processing is a right in which individual has a complete right to suppress restriction on his personal data at any time. This right is not always present as individual can access this right in certain circumstances. The right to data portability is the right, which provides portability of the information that allows an individual to obtain and reuse all the data in their personal use across the different services. Right to object is a right in which, GDPR gives all the individuals the right to object when they want that their personal data to be processed in some specific circumstances. In right to automated decision making GDPR has a provision on automated decision making by the individual that means when a decision is made fully automated without any involvement of human (Information commissioner’s office, 2018).

In the views of Vayena and Blasimme (2017) and Townend (2017), The implementation of GDPR would increase the level of data security, as the individuals can control their data over cloud computing platforms their data at any time if they do not to keep that data on the cloud any more, for ensuring security of personal information. They can also acquire information about the manner in which their personal data is being used. They can also gain information about the location from where their information is being used which is important for any individual to know because they will have surety that their data is not being misused (Vayena and Blasimme, 2017; Townend, 2017).

In a similar manner, it has been stated by Vojković and Milenković (2018) that GDPR is the first regulation that considers biometric data as personal information and
also considers up-to-date technologies under the regulation. As GDPR is also focusing on the use of up-to-date technologies, the threat of cyber-attacks has been reduced to a significant extent, which is beneficial in gaining the confidence of the local public as nowadays everyone, is afraid of cyber-attacks. This shows that the GDPR is a significant regulation that can help the individuals in protecting their personal information to a great extent.

Although GDPR is a significant regulation that helps in personal data protection, there are certain challenges associated with the implication of GDPR and these challenges render impact on the data analysts. From the study of Sarkar et al. (2018), it has been identified that the major challenge that the analysts face is regarding the designing policies for data erasure. This includes analysing the granularity of the data erasure and designing the algorithms that can help in data erasure. Further, data analysts also face challenges regarding the enabling of data erasure. While enabling data erasing service, it is important to ensure that the replicated form of data is erased from the hard drive, in order to protect the personal information, which is the major challenge, faced by the data analysts as the implication of GDPR.

Khan and Gouvia (2017) have asserted several key challenges that are faced by cloud computing analysts in the implementation of GDPR. The approach of GDPR provides uniformity to data protection laws to all the states in EU by providing a single set of rules for data protection, and this law will replace all the persisting laws related to data protection. With the changes in the existing laws, protection directive existing in the current scenario will also have to be changed, as it will not be valid. This is the reason; new protection directive has to be introduced, with compliance to the new rules and regulations provided under GDPR. Application of new protection directive will be a key challenge for the cloud data analysts. In GDPR, the data
controller that is in our case is cloud computing service provider will solely responsible for the security and privacy of the data that is stored on the cloud. It is even more challenging for analysts after the implication of GDPR because now the whole new level of security is required on the cloud computing servers as they are solely responsible for the data loss or breach. GDPR is also applicable to Non-EU countries, which mean if a cloud computing service provider is providing services to an EU resident, then GDPR will apply to the service provider. It is difficult for analysts who are outside the EU to continuously improve the quality to match the quality offered by their competitors, which resides in the EU after the implementation of GDPR. There are severe penalties in GDPR, if any negligence is found regarding the rules and regulations because of that implementation of GDPR will become challenging for data analysts to keep in mind all the rules and regulations. According to the GDPR law, it is mandatory for all the companies and cloud computing service providers to appoint a Data Protection Officer (DPO), which will oversee the maintenance and data security issues. The main responsibility of a DPO is to be independent from the organisation, have professional qualities and proper knowledge related to the maintenance of the data protection law. It will be quite challenging for cloud computing analyst to coordinate with the data control officer as he/she must be having more knowledge as compared to the cloud computing analysts in the organisation (Khan and Gouvia, 2017).

In the views of Rios Velasco et al. (2019), for the cloud-based systems, there are two major issues that have been identified with the implication of GDPR. These two issues include compliance of the regulation and assurance regarding the security aspects. It has been identified that the data analysts with the implementation of GDPR require personal identifiable information so as to maintain the security of the personal
information stored over the cloud. This creates a challenge for the cloud data analysts and creates doubt in the security assurance of personal information stored. In the study, a novel approach has been proposed that is MUCA approach that can help the cloud providers to ensure the security of the personal information regarding SLA-based security (Rios Velasco et al., 2019). From the perspective of Ghasemi et al. (2018), MUCA stands for Multipath forwarding and in-network caching, which is a name-based routing protocol and also with an intra-domain feature. This protocol provides ease to the users, along with scalable support. It helps in computing shortest paths, but also provides learning about the multiple alternative paths that are similar to distance-vector routing protocols. It is also beneficial in reducing the extent of delay regarding content retrieval. The main benefit of MUCA approach is that it is helpful in providing continuous protection to the data that is the major challenge under the implication of GDPR (Ghasemi et al., 2018).

2.5 Key Strategic Measures for Addressing the Challenges Associated with Information Security and GDPR

In the views of Rosado and Mellado (2012), the issue of data loss from the cloud platforms is increasing significantly; thus, it is essential for every service provider to improve their security system to prevent the cloud platforms from the hacking activities. Hackers nowadays are getting more and more advanced regarding the technologies that they have, and with the help of these technologies, they can breach into approximately every kind of data security. This is the major reason for the increase in the number of cyber-crime attacks day by day. The cloud computing analysts are required to implement an effective anti-virus program in order to protect the data of the users from the leakage, damage and from cyber-attack as well (Rosado and Mellado, 2012). In support of this, Safarkhanlou et al. (2015) have stated that
implementation and updating the anti-virus program time-to-time can help the cloud computing analyst to ensure the elimination of the data breach issues. The increased utilisation of internet, email services, and different networks increase the risk of virus attacks, which has an adverse impact on the personal data of individuals. In this relation, anti-virus software plays a significant role in preventing the issues of data theft. The role of anti-virus is significant because they are specifically developed for the purpose of defending the computers and email ids from dangerous malware and threats (Safarkhanlou et al., 2015).

Furthermore, it is also evident from the study that the cloud computing service providers can also enhance their encryption controls, as it can help in improving the security level of cloud platforms and it creates difficulty for the hackers to breach the security levels. It leads to an increase in the level of protection of the user's data (Rosado and Mellado, 2012). In this relation, Rao and Selvamani (2015) have reviewed that data encryption is identified as a significant process, in which the service providers can convert the data into a strong code in order to prevent the data from the unauthorised access and prevent the issue of the data breach. The role of encryption is important in the protection of the data from the unethical practices of hackers. Data encryption create multiple challenges for the hackers to decrypt the data easily; thus, it is crucial for every service provider to encrypt the data appropriately, as it can help in ensuring the data protection (Rao and Selvamani, 2015).

On the contrary, Basta et al. (2013) have stated that regular testing of the functioning of the cloud can be helpful in gaining detailed and relevant information about the issues and lags. The organisations can also hire the ethical hackers in order to check the security level of a cloud platform, as it will be helpful in understanding the key security issues associated with the cloud system and storage space. Employing
the ethical hackers can be helpful for the organisations to increase the level of encryptions on the data of the user that further helps in protecting the user's data from the hackers (Basta et al., 2013). In a similar context, Rathore (2016) and Gregg (2017) have presented their views that the role of ethical hackers is also considered important for the organisations in order to identify the weaknesses in the security system of an organisation. Thus, the organisation can hire ethical hackers in order to strengthen the security system, and it will also help in preventing the data breach. In addition, ethical hackers can be also helpful for the service providers in identifying the activities of illegal hackers and can help the service providers to track them. This can help the service providers to file a complaint against the illegal hackers to the cybercrime authority of the related country, and further, the service providers can ensure the data protection (Rathore, 2016; Gregg, 2017).

Politou, Alepis, and Patsakis (2018) have asserted that to address the challenges related to the implementation of GDPR it is important to firstly understand the rules and regulations that are present in the GDPR regulation. In order to understand GDPR regulation, the cloud computing service provider needs to appoint someone with high knowledge of the law so that it will be easy to comply with GDPR rules and regulations. A challenge that cloud computing service provider face is that when GDPR was implemented in the year of 2018 all previous law related to data security went void. As a reason of that, organisations have to embrace new principles of accountability that are introduced by the GDPR. This challenge could be solved with the help of a professional, which have the understanding of the principles of accountability that are issued by GDPR (Politou, Alepis, and Patsakis, 2018).

According to Rao and Selvamani (2015), the proper implementation of GDPR policies are one of the biggest challenges that is faced by any cloud computing service
provider because no employee has the proper understanding of the policies related to GDPR. In order to address this issue the best possible measure is to have proper training procedure established in the organisation related to the ways to implement the policies issued by GDPR. This training process should be given to all the employees and staff members in the organisation. Another major challenge that is faced by the organisations is that if the rules and regulations are not properly followed or any negligence is found than there is a penalty worth 5% of the annual revenues and maximum fine up to 100 million Euros. This issue can be solved by giving responsibility for monitoring rules and regulations of the GDPR to highest level of management because they are having the better knowledge of the law than anyone else (Rao and Selvamani, 2015).

Rios Velasco et al. (2019), have asserted that data breach notification is a challenge that is faced by the organisations in the current scenario. Data breach notification is a rule, which states that it is essential to report any breach, which can affect the stakeholders. The maximum time that can be taken by the cloud computing service provider is 72 hours for reporting the authority, which require more resource in time and manpower, which can increase the cost of the service. In order to, solve this issue organisation should form new procedures, which readdress the issues, such as poor compliance of the GDPR and conduction of data breaches (Rios Velasco et al. 2019).

2.6 Summary

According to this literature review, it can be summarised that several current trends and practices are going on regarding the aspects of information security in the real world. It has been evident that in the current scenario, the information security related crimes have jumped up to a significant level in the recent years. Due to the
issues of the security breaches, the organisations have been facing increased cost burden of security breaches. Cyber-crime activities are increasing at a fast pace, in the current scenario, which has created challenges for the individuals, as well as the organisations. In order to address this cybercrime issue, many practices are being followed by the organisations. In the organisations that are focused on cloud computing, many challenges are faced by the cloud data analysts. The enhancement in the facility provided by cloud computing service providers is also a reason why there are issues in data security. Some of the organisation also hires ethical hackers to check the level of security that the organisation is having, this measure help in making security better as, if the hacker can hack the system then there is a scope for improvement. It has been examined that in the cloud computing the privacy of the data is a big issue that is faced by the people who are using these cloud computing services. In order to mitigate the issues, the EU government have issued a new law named as GDPR in 2018, regarding the rules and regulation related to data security. Cloud computing analysts face a lot of challenges related to the implementation of GDPR. This study has addressed all the challenges that are faced by either cloud computing analysts or cloud computing service providers and provides all the key measures for addressing the challenges.
Chapter 3: Research Methodology

3.1 Research Paradigm

A paradigm in a research study is regarded as a crucial aspect that helps in depicting the set of beliefs, perspectives, and views on the basis of, which the research study is structured (Mackenzie and Knipe, 2006). It is that part of a research study, which comprises of interconnected practices and helps in defining or illustrating the flow or nature of the research study. Thus, it is important for every researcher to implement the most suitable paradigm in order to have a better understanding of the acquired research data. In this context, the research paradigm is categorised in two primary research paradigms that are applicable for a research study include positivism and interpretivism (Howell, 2012). Both paradigms are completely different in nature and can be used as per the nature of the collected data. Positivism paradigm is considered important in research when the collected data is quantitative in nature because it is used mainly to describe the statistical, factual, and practical data (Pattison, 2013). In addition, in the qualitative study, interpretivism paradigm is used because it is helpful in analysing the human perception and subjective information collected with the consideration of interview and secondary method (Mackenzie and Knipe, 2006).

In the present study, interpretivism paradigm has been incorporated by keeping in mind the qualitative nature of the research. This paradigm helps in identifying the contextual aspects of information security and the challenges that are associated with it. The justification behind using the interpretivism philosophy is that it enables the researchers to subjective information and human perception by considering different subject related concepts and theories. In this relation, the human perception acquired from interview method is interpreted appropriately with the integration of different
previously developed concepts on a similar topic (Leitch, Hill and Harrison, 2010; Thanh and Thanh, 2015). Apart from this, it is further helpful in focusing on conclusion and observation, which is quite necessary, is in this study for the purpose of identifying the key challenges associated with information security and GDPR and analysing its effect on the cloud computing analyst.

3.2 Research Approach

The plans and procedures that are followed in a research study in context with data interpretation, collection, and analysis are all the part of the research approach. Adopting appropriate approach in a research study helps in ensuring that proper flow of information is maintained in the study, which is necessary to conduct it in the right direction (Cash, Stanković and Štorga, 2016). Implementing a suitable research approach is considered essential in order to enrich the validity of the research results. Out of the two main approaches adopted in research study including inductive and deductive, the inductive approach has been employed. It has been found that the main difference between both the approaches is related to the inducting new theories and concepts and testing the theories for the purpose of presenting the useful results for the research study.

An inductive approach in a study helps in accumulating data in research using a theoretical framework by keeping in mind the academic background of the study. It further is crucial in acquiring the data related to the research question and objectives, which is necessary to obtain the intended outcomes. Moreover, the main focus of the inductive approach is to generate new and effective concepts from the collected data and enhance the quality of the results (Creswell and Creswell, 2017). On the other hand, deductive approach is different as compared to the inductive approach, as the deductive approach aimed to test different hypothesis and theories with the
consideration of the acquired data. This indicates that the deductive approach is suitable for quantitative research because in qualitative no hypothesis are developed (McCusker and Gunaydin, 2015). In this study, implementing the inductive approach helped in identifying necessary models and theories associated with Information Security and GDPR, which further would prove to be crucial in exploring the challenges related to this field along with its impact on cloud computing analysts. In regard to this research study, using the inductive approach is found beneficial because it helped in presenting the relevant evidence and it also supports the qualitative research method (Bernard and Bernard, 2012). This approach also helped in extracting the general data with respect to the key challenges associated with information security and GDPR and its impact on the cloud computing analysts that enable the researcher to have a better understanding of the research context (Fereday and Muir-Cochrane, 2006).

3.3 Research Design

Research design acts as a blueprint for research as it helps in properly incorporating varied components associated with a research study. Research design is a process that is helpful in selecting different suitable data collection methods through the subject related information can be obtained (Caruth, 2013). Furthermore, the presence of meaningful as well as logical structure in research is one of the greatest contributions of research design in a study. The two primary designs integrated by researchers include exploratory and descriptive research design (Yin, 2013). In the current research study, exploratory research design has been incorporated due to the qualitative nature of the study. The ability of exploratory research design to provide deeper insight into the concepts of a specific research topic and to facilitate the process of data accumulation in regard to the research problem are some of the major
reasons behind the integration of this design in the study. This design is very suitable for this study, as it can successfully address the research problem of identifying the challenges related to Information Security and GDPR along with the exploration of its impacts. On the other hand, the descriptive research design is not used in this research study because it does not provide accurate results. This type of design is mainly useful in interpreting the data collected from the survey and observation method (Meyers, Gamst and Guarino, 2016).

3.4 Data Collection Tools and Techniques

In a research study, data can be collected using two different methods, first being the primary data collection method and the second being secondary data collection method. Since data collection is the most crucial part of research as it helps in acquiring research objectives and addressing the research problem, so it is crucial to select appropriate data collection tool and technique for the conduction of a research study (Marczyk, DeMatteo and Festinger, 2010). In the views of Minton et al. (2013), the primary data is in the form of numerical and can be collected through the survey, interview, experimentation, and observation method. However, secondary data can be obtained with the use of different relevant sources that incorporate journal articles, online-published articles, and books (Minton et al., 2013).

The present qualitative research study has utilised semi-structured interview as the primary data collection method in order to accumulate and identify the views and perspectives of the cloud computing analysts. This method would prove to be crucial in gathering the personal experience and observation of the analysts regarding the Information Security and GDPR related challenges that are faced by them. The main source of interview conduction in this research is a questionnaire comprising of open-ended questions associated with the research topic. The justification behind
using the interview method in this research study is that it provided more detailed and relevant views from the selected respondents with respect to the research topic. There are several advantages associated with the interview method, as in the interview method, the researchers can select the respondents from the particular field and can asked subject related open-ended questions. This can be helpful for researchers to accumulate in-depth data from the respondents. The interview method is considered more proficient in the qualitative research study because it helps in explaining the data more appropriately (Anyan, 2013; Palinkas et al., 2015). In interview process, different questions were asked to the respondents such as trend of the use of cloud computing by the multinational corporations in the UK in the reference to GDPR, benefits of using cloud computing for business data protection, major challenges associated with the information security in cloud computing, and impact of the latest general data protection regulations on work that helped in accumulating the in-depth data from the interviewees (see appendix for full interview schedule).

3.5 Sample Size and Sampling Approach

Sampling is that process in a research study, which helps in selecting a specific group of individuals among a large population in a way that they largely contribute to the acquiring the research findings and objectives (Thompson, 2012). These sampling techniques can be used for the purpose of selecting the appropriate sample population for the process of data collection. Random sampling technique can be used for selecting the respondents randomly from the large population (Martino, Luengo and Míguez, 2018). In addition, the purposive sampling technique is different in nature as compared to random sampling. In purposive sampling technique, the population is selected on the basis of their subject knowledge and working experience in a particular field. In this study, the sample size of the research participants is 6, which
comprises of cloud computing analysts that are operating in the multinational companies of the UK. Purposive sampling approach has been employed in this study to ensure that only those participants are selected who possess proper knowledge and understanding of Information Security and GDPR. As a part of this sampling approach, only cloud computing analysts were selected so as to gain crucial information about their experience and the challenges that they have encountered. In the selection of the sample population, the knowledge and experience of respondents have been analysed prior to conducting the interview. This process helped in selecting the suitable sample population for this research study, which further helped in acquiring reliable and credible data for this research study (Etikan, Musa and Alkassim, 2016).

3.6 Data Analysis Tools

For analysing the secondary and interview data, the thematic method is the most effective and suitable of data analysis. In this study, the data accumulated through the interviews have been analysed with the help of descriptive data analysis method. Under this method, the data was collected through thematic analysis whereby the key responses of the participants were developed into different themes that are in alignment with the research objectives (Jackson, 2008). The utilisation of this method can prove to be effective in clearly denoting the core findings obtained through the research participants along with the support of literature associated with it. Under the thematic method, the research aim, objectives, and research questions are considered in order to develop different relevant themes. These themes helped in analysing the collected data effectively, and credible and authentic results of the research are gained (Fereday and Muir-Cochrane, 2006).
3.7 Ethical Considerations

In an attempt to conduct a research study ethically and without any violation of rules and regulations that can affect its overall authenticity, it is crucial to consider specific ethical considerations (McKee and DeVoss, 2007). In the present research study, it has been ensured that all the ethical aspects associated with research are fulfilled properly for the purpose of extending research validity. In order to maintain confidentiality in this research, the name and personal details of the interview participants were kept hidden from other participants. Apart from this, taking prior consent from the interview participants in this study, their voluntary acceptance for data collection was ensured in this study. Moreover, complete research related information is also provided to every interviewee that includes general information about the interview questionnaire and purpose behind the development of this research study. For such purpose a consent form has been given to the respondents where it is mentioned that they can have a clear right to withdraw from the data collection process any time. In this manner, all the ethical aspects are taken into consideration in this study to affirm its reliability, validity, and authenticity.
Chapter 4: Data Analysis, Findings, and Discussion

4.1 Introduction

The data are aimed to be analysed in this chapter using the thematic method of data analysis, wherein in the light of research aims and objectives, and interview schedule, the themes have been drawn. The findings gathered from analysing the data has been discussed further in this chapter, in the light of the research aims and objectives. This highlights that a systematic procedure is followed in this chapter to examine and analyse, all the gathered data in a meaningful and pertinent manner.

4.2 Thematic Analysis

**Theme 1: Practices of information security prominently employed to protect data from the external users**

The interview participants were asked regarding the ways through which they currently protect the sensitive data from the external users, in their respective organisations. In this regard and on the stated theme diverse views have been gathered. Participant A in this context has asserted that "External threats are faced by our company due to diverse state-sponsored actors and hackers. For protecting data from these external users, we at our organisation focuses on accessing data vulnerabilities and calculating risk scores to determine the severity of each capturing vulnerability. This has been made in numerical form which is translated further in qualitative forms such as high, low or medium".

In arguing to the opinion Participants C, D, and F, all have made significant emphasise on using cloud computing networks to safeguard the data from unauthorised access and illegible use by the external users. In detailed context to this, Participant C has opined that "we integrate cloud computing networks to manage all pertinent organisational data and resources. The reason for integrating it into the
organisation is its role in leveraging organisational processes for creating more robust and secured business procedures that combat risks pertaining to data privacy, security, and availability.” In similar context to this, Participant D has opined that “I think the utilisation of cloud computing in my organisation has supported the organisation significantly in enhancing its data security, productivity, and overall organisational performance. It optimises IT infrastructure of my organisation by providing quick access to all required computing services”. In support of this, Participant F has claimed that “I feel in comparison to traditional data storage process or system, cloud computing is an optimal method of information security. It involves low-budget in the implementation of security systems, cost reduction, flexibility, increases efficiency, requires less knowledge and training to implement and provide security gains to my organisation”. The integration and analysis of diverse opinions of participants have highlighted that that organisation of Participants A, C, D, and F have a positive outlook towards protecting data from the external users using diverse practices. The findings suggested that assessment of data vulnerabilities, integration of cloud computing networks and calculation of risk scores are among the key prominent techniques which are used by the organisations.

In arguing to this, Participant B has opined that the external environment poses a wide array of risks pertaining to data protection from the external users. All these risks are not effectively able to manage by the cloud computing networks as these risks are significantly related to environmental threats, data security, data privacy, business continuity, and data management. So, in my organisation to ensure a high degree of information security, my organisation has adopted several new practices such as a strong tracking system, digital recording, increased information exchange and adoption of new regulations in the UK for information security. The analysis and
interpretation of diverse views of interview participants have highlighted that significant inclination towards practices such as cloud computing, tracking system, digital recording, adoption of new regulations in the UK for information security, accessing data vulnerabilities and calculating risk scores are explored in the UK organisations.

**Theme 2: Trends and usefulness of cloud computing for organisations**

On the stated theme, the interview participants have presented diverse views on the trends in the information security landscape and usefulness of cloud computing for the organisations in the contemporary era. In this context, Participant A has asserted that "Processes based on information security has made the current world business practices faster and efficient by enhancing the interconnectivity between the systems as an outcome to internet-related advancements. In this, the proliferation of mobile devices and smartphones having access to the internet has raised the demand of effective platforms to manage security concerns, and I think in managing these concerns the use of cloud computing platforms would be most optimal". The analysis of the views suggests cloud computing usage has become a key step to manage all security concerns pertaining to current world business practices.

In detailed context to the points, all the other participants have highlighted diverse points regarding the importance of cloud computing for contemporary organisations. Participant B in this context has opined "Cloud computing provides my organisation with a high level of flexibility and efficiency. With the use of cloud computing, flexibility is fostered by enhancing scalability, cloud options, control choices, and tools selection, whereas, on the other hand, cloud computing brings efficiency in business operations by providing my organisation, greater accessibility, savings in costs, integrating high-security procedures and standards, and disaster
recovery". Similar views are presented by Participant F, who claimed that "the use of cloud computing networks enhance the efficiency of business operations by facilitating wide access to data from diverse locations across the world, implementing best standards of security to protect and save the data, and provide tailor-made solutions to my organisation." The analysis and interpretation of participants of B and F have highlighted that cloud computing is significantly useful in raising the high-security standard and ensuring data privacy.

In addition to this, Participant C has asserted that "Cloud computing networks have allowed my organisation and its individuals to store and safeguard their personal and confidential data on cloud-based technologies. It minimises the time involved in storing the data, along with the minimisation of the cost of acquiring additional storage of data." In support to the opinion, Participant E has claimed that "Cloud computing has provided a significant benefit of advanced technology to my organisation by offering flexibility and accessibility to a platform that ensures safety and security of organisational data. It ensures easier recovery of data, increase flexibility and provides an effective platform to share information". In summarising form of the diverse participants' views', Participant D has asserted that "Cloud computing has consolidated three key needs of the present century technology. These are the provision of autonomy to organisations by ensuring cost reduction and high agility". The examination and interpretation of diverse views of participants have highlighted wide usefulness of the integration of cloud computing networks in UK multinational organisations.

**Theme 3: Impacts of the latest general data protection regulation (GDPR) on managing information security in the cloud computing environment**
The stated theme is answered through questions 3 and 7, which were asked by the interview and reflected the use of GDPR along with cloud computing, and its implications on work directly. Based on the views gathered, diverse implications both positive and negative of GDPR are examined on managing information security in the present business environment. Introductory views are presented by Participant D who stated that "GDPR provides effective legislation of data protection which has laid down the rules pertaining to processing, storing and managing the large data from the people of the EU. It is crucial for strengthening the EU's data protection, as it enables a high degree of control and presentation of the significant requirement for data processors and controllers, including data protection". In support of the views, Participant C has claimed that "GDPR is a crucial EU legislation which would be highly beneficial for my organisation in the long run for improving and establishing a platform that ensures high security of personal data of individuals. It would help crucially on improving the personal data security which is transmitted through various modern technologies". A similar set of views is reflected in the perception of Participant E who opined that "Implementation of GDPR, I think would produce significant positive implications on the data security levels and individuals which control their personal information and data over the cloud computing platforms. Along with this, the legislation would enable acquisition of information regarding the manner in which personal data is needed to be used, and also my organisation can trace the location from where the information is used by legible and non-legible users". The examination of Participants C, D and E views have highlighted that GDPR would produce significant positive implications on their company and data security level essential to manage a high level of information security in the cloud computing environment.
In arguing to the findings, Participant A has asserted that "I think that to meet the GDPR requirements pertaining to the cloud computing environment, our company need to invest significant resources in manpower and resources for updating their privacy policies, upgrading technology platforms, adjusting data processing and storage procedures and changing advertising practices." In similar context to the views, Participant F has asserted that "GDPR would produce implications on every company, but I feel that the hardest hit will be faced by the organisations which hold and processes a wide range of consumer data, such as marketers, technology firms and the data brokers." A crucial insight to the stated theme is made by Participant B who asserted that "GDPR is expected to produce significant implications on the data architectures and technology platforms that are essential to handle all personal data and manage extensive information. However, it will produce significant implications on the organisation by demanding changes in the existing data architecture and technology platforms, along with re-engineering of present platforms and systems to meet all GDPR's requirement and reduce risk pertaining to non-compliance with GDPR". The analysis and interpretation of diverse participants views have highlighted that the execution of latest general data protection regulation (GDPR) on managing information security in cloud computing environment would have diverse positive, as well as, negative implications.

**Theme 4: Key challenges associated with information security-based processes facing by the cloud computing analysts**

In the contemporary era, cloud computing analysts are facing diverse challenges associated with information security-based processes. This has been examined from the diverse claims of the interview participants. In this context, Participant A has asserted that "Enhancement in cloud computing platforms has raised several concerns
pertaining to data security. This has been, I think due to increasing issues of data leakages, loosening of users’ control the confidential data and ensuring privacy are examined as the key challenges”. In similar context to this, Participant D has opined, that “the challenges are linked to weak measures of cloud security of the services, such as encryption, storing data without controls, and theft of intellectual property. Along with this, the challenges pertaining to violations of compliance and regulatory requirements, loss of control on the end users, malware infections and contractual breaches with business partners or customers.” The views of both the interview participants have reflected that the chances of leaking the data are significantly high in the cloud platforms.

Further, Participant B has put significant emphasises on hacking as a major challenge for cloud computing analysts. The Participant B has opined that “I think hacking is one of the key challenges associated with information security. It has raised the concerns on data security as the illegible activities of hackers have affected the cloud service providers’ capabilities that would make the cloud service vulnerable.” In a similar context, Participant C has stated that "Due to the increase in the utilisation of Internet-based services in the current environment, the cloud computing analyst are confronting varied issues in securing the data of their clients. The unethical activities are increasing by the hackers due to this the cloud computing analyst are unable to control the data loss issue.” In addition to this, Participant E has also presented the views in regards to key challenges associated with information security based processes facing by the cloud computing analysts that "hackers are using more advanced systems as compared to the organisations that create major challenges for the cloud computing analysts to eradicate the issue of data loss. Due to the ineffective security measures, the hackers are easily stealing the confidential data
of their clients, and it is affecting their brand image in the market.” Participant F also said that "using inappropriate security systems and software also create several challenges for the cloud computing analysts to secure the confidential data of their clients. It is important for the organisations to implement the suitable and effective anti-virus that provides enhanced security to the users in protecting their personal data. The data breach is an issue faced by a large number of populations, and their data is used for illegal purposes. The cybercriminals are using the strategy of sending emails with malware to people for getting access to their private data."

**Theme 5: Challenges and implications of GDPR within cloud computing-based processes and for cloud computing analysts**

The selected participants were asked about the challenges and implication of GDPR within cloud computing-based process and for cloud computing analysts. In response to this interview question, Participant B stated that "GDPR is a newly announced regulation that includes different directives that are new for the cloud computing analyst that create challenges for the analysts to understand and implement appropriately. Most of the cloud computing analysts are lacking with detailed and relevant knowledge about the directives of the GDPR, which is affecting their overall efficiency. However, the implication of GDPR would be helpful for the cloud computing analyst to provide more secure services to the users, as the analysts can ensure the users regarding the protection of their data." In a similar context, Participant C also said that "every organisation is bound to work in accordance with the GDPR and protect the privacy of every customer. Before GDPR, the organisations are allowed to use the data of their customers; however, after GDPR came into practice, the organisations that are providing cloud-based services to the customers do not have any control and not allowed to use the customers' confidential data. It is
a challenge of the organisations, as they cannot increase their customer base by accessing the data of other customers. The aim of the GDPR is to ensure the customers that their personal data is secured and cannot be used for any unethical practices. Thus, the organisations have to maintain transparency with the customers and needs to provide necessary information to the customers about their data. Moreover, the cloud computing analysts are also accountable to work in accordance with the new directives of GDPR, which is creating difficulties for them because they are completely unaware of the directives and procedures of GDPR, and due to this, the implication of GDPR might be affected adversely, and it can also create a problem in securing the data of customers."

From the views of both participant B and C, it is depicted that most of the cloud computing analysts are unaware about the new data protection directives of GDPR, which create challenges for the analysts to provide highly secured services to the customers. The cloud computing analysts do not have any specialisation with respect to the GDPR that has impacted the implication, and it can also adversely affect the overall operational services.

In relation to the similar interview question, Participant A also presented the views that "for every organisation, customers privacy must be the first priority; however, the service providers are facing difficulty in securing the data of their customers due to ineffective security systems. In the EU, GDPR has been announced for the purpose of eliminating the issue of data loss and give assurance to the customers that their data will not be shared, used, or leaked. However, in the implications of the GDPR are challenging for cloud computing analysts. GDPR includes several new directives, as the cloud computing analysts have to execute the erasure directive in their security system, which is also a challenge for them because
it requires to change the algorithms and the entire process of data handling. Moreover, changing the algorithms also incur the cost for an organisation, and it also enables the customers to erase their data from the cloud platforms, and they can also ask the service providers to the also erase their data from their hardware. The cloud computing analysts are also not getting consent from the customers to access their data, which is limiting an organisation to increase their customer base.” In addition to this, Participant E said that “as per the guidelines of GDPR, every cloud computing analyst working in an organisation have to maintain transparency and are enforced to reveal their practices as what they are doing with the customer data. This is a major challenge of the organisations to reveal their operation in front of every customer. In addition, they are also facing the challenge as an implication of GDPR that they need to delete the data as per the request of the customers, which is a challenge for the old organisations which is maintaining the customer data from a longer period of time."

With respect to the key challenges and implications of GDPR within cloud computing-based processes and for cloud computing analysts, Participant F said that “non-compliance with GDPR will be considered as a breach of EU guidelines and due to this an organisation has to pay a heavy fine. Moreover, as per the guidelines, an organisation has to maintain the security of customer’s data because any breach of data would be a challenge for the organisations and heavy penalties would be imposed on the organisations. The cloud computing analysts have to follow every guideline of GDPR in their services and protect the data of the customers from any kind of breach.”

As per the response of participant A, E, and F, it is observed that the cloud computing analysts are facing varied challenges as an implication of GDPR. The
cloud computing analysts have to work in the alignment of new directives of GDPR, which is a challenging process for the analysts because they do not have any knowledge and experience of GDPR. Moreover, not following the GDPR guidelines would affect the financial position of an organisation because the EU can ask for a heavy penalty from the organisations.

**Theme 6: Key measures for addressing the challenges associated with information security and GDPR**

The interview participants were also asked about key measures for addressing the challenges associated with the information security and implication of GDPR and in the response of this question, Participant B said that "due to the increasing issue of data theft, customers do not trust the service providers of cloud platforms, which has affected their businesses. Thus, it is vital for cloud computing analysts to identify the loophole in their services and try to rectify those issues in order to enrich the security systems. The cloud computing analysts are required to adopt an efficient anti-virus program for securing the cloud platforms from different malware attacks from unethical practitioners." In a similar context, Participant A and C have also presented their views that "time-to-time monitoring is crucial for every cloud-based service providers of their security systems that include algorithm, anti-virus, and antispyware, as it would help the service providers to create challenges for the hackers to control the confidential data of the users. Most of the users of cloud services are facing the issue of data loss, and due to this, they stop using cloud-based services, which is also affecting the business profits of the organisation. Thus, the cloud computing analyst must focus on updating their security systems on a regular basis and can implement more effective anti-virus, and with the use of antispyware, the cloud computing analyst can also identify the location from where the hacking practices are conducted."
The organisations must adopt the GDPR in order to gain the trust of the users because it enables the service providers to facilitate full control to the users over their confidential data. In order to implement the GDPR practices, it is significant for the organisations to understand the new accountability principles of GDPR and change the strategy from theory to practice, as it will help the service providers to enhance the security of the data protection.”

As per the views of Participant B, it is evaluated that the cloud computing analyst should put major emphasis on the finding the loopholes exist in the current security system of an organisation, as it will help in overcoming the loopholes and enhancing the security for data protection. In addition, using the most effective anti-virus is also considered an important aspect for preventing any hacking practices and securing the data of the customers. Moreover, the findings of both participant A and C reflected that it is important for the cloud computing analysts to do regular monitoring of their security systems and must update the anti-virus so that the personal data of the customers can be protected appropriately. In addition to this, the implementation of GDPR would be beneficial for the organisations to

In regard to the similar context, Participant D exhibited that "The cloud computing analysts are losing control over the security of the confidential data of the users due to ineffective firewalls and anti-virus. Thus, in order to gain customer loyalty, data protection must be the first priority of the service providers. The data protection practices can be enhanced by using the highly improved encryption system and two-factor authentication. This creates difficulties for the hackers to access the confidential data of the users. Two-factor authentication is an effective process that strengthens the platforms where the data of users is saved. The two-factor authentication requires a password and facial recognition to access the data of users."
Thus, using this security measure can be helpful for cloud computing analysts to enrich the data protection system. Moreover, different organisations that provide cloud-based services to different people are facing issues in implementing the GDPR due to lack of knowledge and awareness; however, as per the EU, it is vital for every organisation to adopt GDPR for data protection. In this case, the organisations need to acquire detailed knowledge about the procedures and regulations, as it will help in implementing the GDPR more efficiently." Similarly, Participant E and F also presented their views in regard to the key measures for addressing the challenges associated with information security and GDPR that "data encryption is considered important in securing the data from the unethical practices of the hackers. Implementing the data encryption strategy can be helpful in ensuring the data protection of the users' data. The implication of data encryption creates multiple challenges for unethical practitioners to decrypt the data. Moreover, in order to eradicate the issue of data theft, the organisations can hire ethical hackers for strengthening the security system, and it also helps in tracking the hackers and limits their practices. Additionally, as per the GDPR regulation, the organisations cannot use the data of their client with their permission; however, on the basis of GDPR guidelines, the organisations can take consent from their client to use their data. The service providers are required to build a strong relationship with their clients in order to get access to their data."

It is evaluated from the views of Participant D that the cloud computing analysts must use the strategy of two-factor authentication for creating problems for the hackers to get access to the data of people and use them for illegal purpose. From the overall responses of Participants E and F, it is affirmed that utilising the data encryption strategy would be helpful for the service providers to secure the data of
their customers from hackers. Moreover, as per the GDPR guidelines, the service providers are not allowed to access the data of the customers; however, the organisations can develop a strong relationship with the customers and can take consent from the customers in order to gain access over the data of customers.

4.3 Discussion

It has been discussed on the basis of the interview findings that organisations tend to employ various information security measures that play a vital role in enhancing the data security of the organisations by minimising the threat due to external factors and by securing the business procedures. Cloud computing has helped organisations in reducing their costs and efficiency, as it provides a securer platform with optimal use of online storage. The literature supports that using encryption and decryption techniques for securing data, taking regular backups of data, and using relevant methods of data security can help the firm in gaining a secure network for transaction and data transfer. The organisations can develop securer systems for themselves by adopting cloud computing services, as they have a vast set of plans and policies that can secure the data of an organisation from external theft (Krutz and Vines, 2010).

The discussion reflects that cloud computing has enhanced the quality of internet and expanded the storage capacity while ensuring easier access to data using tractable platforms for the multinational organisations that are operating the market of the UK. The enhanced security of data, flexibility, and interconnectivity of networks due to cloud computing has created an added advantage for the systems of these multinational organisations. The literature also supports that the usefulness and importance of cloud computing have increased to a large extent in recent years with the increased awareness regarding the use of data protection plans for ensuring information security. There are various areas in which cloud computing provides tools,
methods, and resources, which can address the storage, interaction, data processing, and interaction needs of an organisation (Assunção et al., 2015).

It interview findings reflect that GDPR is identified as an essential legislation of the EU that has laid effective rules, regulations, and standards for data security, which have up-scaled the data security levels and have had positive implications on the technology platforms and the data architectures for the multinational firms. Although, GDPR also has a few negative implications including the re-engineering of platforms and increased investment in the technological upgrade. In the support of these views, the literature has explored that GDPR will be advantageous for the firms, as it offers the firms to bring consistency in the protection of data and providing an EU-wide policy that enables a more integrated system for the companies (Tikkinen-Piri, Rohunen and Markkula, 2018). It has been reflected in the interviews that there are security-related concerns that have been raised in recent times due to the lack of security and trust in online networks. These networks are prone to hacking and malware attacks, which can lead to data leakage and loss of control over user information. This is also supported in the literature by Song et al. (2012) as data security is becoming more and more challenging. The business leaders are facing a challenge with data accessibility, data security, and data privacy, as the data is stored in the cloud storage databases. The data is prone to theft, as it is maintained and controlled from both the ends; the users can manipulate their data as well as the companies also update the data as and when it is updated in any of the files of the company. The scarcity of resources and huge amount of investment associated with the acquisition of resources and specialised guidance makes it difficult to protect the data of users while ensuring to provide rich services by processing their data.
It has been discussed on the basis of the interview findings that the guidelines of GDPR have strictly stated that only the individuals have the control over their data and they can submit and revoke the information as per their desire and whenever they wish to disassociate from the companies. The literature supports the notion by stating that GDPR will improve the level of data security and standardise the process of user data protection while minimising the data breaches in organisational data, which, in turn, will ensure to safeguard the brand image and increasing the loyalty of customers towards the companies. However, the penalties associated with the non-compliance and inability to protect the user data can bring a business organisation to a state of closure due to the high amount of fines and extreme compensations. The companies that process data in bulk need to employ a data protection officer (DPO) for ensuring data monitoring is conducted securely (Burgess, 2019). It is identified that it is necessary for firms to hire computing analysts and install Anti-Spyware and Anti-Malware software that can eliminate the chances of espionage and theft of the customer’s data. The data must be regularly encrypted using effective algorithms. The literature supports that for addressing the challenges due to GDPR and information security, an organisation must deploy RSA security in its system, which will help the organisation to assess the risks, generate response against breaches, manage the data in a holistic manner, and ensure data privacy (RSA, 2019).

4.4 Summary

It has been analysed on the basis of the overall thematic analysis and the discussion of the findings of the interview that the rules imposed by EU GDPR have significantly influenced the data protection policies, as they have various positive and negative implications over the business organisations. The information security concerns have been raised to a large extent with companies facing threats due to data
theft and espionage. GDPR will help the EU citizens to control and manage their data on their own as well as the companies are also bound to ensure their data privacy and security by employing data protection officer (DPO) as per the guidelines of GDPR. It is also identified that the regulations of GDPR are very strict in the case a company fails to ensure the data security of its customer’s data, as it can also result in the closure of the companies due to heavy fines and compensations.
Chapter 5: Conclusion and Recommendations

5.1 Introduction

The main aim of this research study is to critically analyse of the key challenges associated with information security and GDPR and its impact on cloud computing analysts. In order to address the aim of this research study, several research objectives are formulated in the alignment of the research aim, which has helped in presenting the appropriate information for the research study. The issues of data loss are increasing in the global environment due to the weak security measure adopted by the service providers. For the purpose of presenting the credible results of the research work, the primary method of data collection is utilised, in which the interview is conducted with 6 cloud computing analysts who are working in multinational companies in the UK. The interview process includes different subject related open-ended questions that were helped in accumulating the detailed information about the key challenges related to information security and GDPR. Moreover, for extracting the results from the accumulated data, the thematic method is utilised, in which the interview data is interpreted under different themes, and for enhancing the reliability of the results, the findings are also evident from different existing studies.

5.2 Conclusion

It is concluded from the overall data findings that in the global business environment most of the organisations are confronting several challenges in protecting the data of their clients. In the current environment, a large number of individuals and organisations are using cloud-based services for strengthening their personal and confidential data. However, with the increase in the use of cloud-based services, the cases of data theft also increased, as hackers are acquiring the data of different people through illegal practices for their personal use. The utilisation of the
cloud computing network is increasing by the number of organisations for the purpose of enhancing the level of data security. Another purpose of using cloud computing is to reduce the cost incurred in different hardware that performs the same function of storing personal and confidential data. This indicates that cloud computing has a significant advantage; however, there are several disadvantages associated with the use of cloud computing, which is affecting the privacy of the people. The major challenge associated with cloud computing is related to privacy and data security. The personal data stored by individuals or organisations over different cloud platforms can be hacked easily by hackers, and they can even use the data for their personal use.

From the overall data findings, it has been concluded that the cases of the data breach are significantly increased by the hackers. There are several reasons due to which the data is breached from the cloud platforms such as inappropriate programming, ineffective anti-virus and firewalls, and software vulnerabilities. The service providers are completely responsible for facilitates effective and secure services to their customers. However, the service providers and users are not sure about the security of their data because the cybercrime activities are rising significantly. In cloud computing, the service providers are responsible for safeguarding the data of the users in order to retain the users for a longer period of time. However, the clients are losing control over their confidential data, which is creating the biggest challenge for the service providers to protect the data of their clients. For the purpose of protecting the data of the users, the European Union has announced GDPR that aimed to provide full control to the users over their data stored in the cloud. There are several benefits associated with GDPR for the citizens of EU, as the implementation of GDPR would be beneficial for the organisations to ensure the users that their data is secured. With the implementation of GDPR, organisations
can provide more secure and improved services. Implementation of GDPR is mandatory for the organisations, which are operating in the EU countries. The core principle of GDPR is to maintain transparency with the users. As per the guidelines of GDPR, the users have a complete right to control their data, as they can ask the service providers to erase their data from the cloud platforms. However, the cloud computing analysts are facing challenged with information security and implication of GDPR, which is affecting their overall efficiency. GDPR is a new regulation, which is implemented in the year 2018 and due to this; most of the cloud computing analysts are unaware about the procedures and policies of GDPR, which is limiting them to properly regulate the GDPR in their security system. In addition, it is also concluded that another challenge for the cloud computing analyst is that they need of design policies regarding data erasure that includes designing the algorithms of data erasures. The purpose of this policy is to enable the users to erase the data from the cloud as well as from the hard drive of an organisation where the data is stored.

From the overall data findings, it has been concluded that there are varied strategic measures that can be helpful in addressing the challenges associated with information security and GDPR. In order to prevent the issue of a data breach, the cloud computing analysts are required to focus on improving their security system be replacing the old one with the updated one. Utilising the updated anti-virus software can be helpful in protecting the confidential data of the users. Thus, it is vital for cloud computing analysts to monitor their security systems and enhance the securities with time so that the issue of a data breach can be eradicated. Furthermore, antispyware is another strategy that can be used for tracking hackers. This strategy can enable the service providers to locate the hackers and file a complaint against them, which leads to securing the data of the clients. The cloud computing analyst can
also implement the two-factor authentication for enriching the security levels. The two-factor authentication restricts the unauthorised person to get access to the personal data of other individuals. The cloud computing analysts can also use the data encryption strategy for creating a challenge for hackers to use the personal information of others. Encrypting the data of users is a most strategy for securing the confidential information of the individuals.

It has been concluded that from the data findings that it is important for every organisation operating in the countries of the EU to adopt GDPR to provide more effective and secure services to the citizens of the EU. The GDPR includes new data protection directives that create challenges for the cloud computing analysts to understand the directive and change their existing procedures with new. In this relation, the organisations must conduct a training programme for their employees, as it would be helpful for enhancing the employees’ knowledge and capabilities to work in accordance with the directives of GDPR.

5.3 Study Limitation

At the time of developing this research study, different limitations occurred, as collecting the specific data about the GDPR is a challenging task because there are limited numbers of relevant and authentic studies are developed. In addition, conducting the interview was a time-consuming process, as an initial stage, most of the cloud computing analysts did not take interest for the interview, as convincing the employees working in multinational companies of the UK was a bit difficult that has consumed a lot of time. Moreover, the interviewees agreed for the interview as per their availability and interest, which has affected the completion of the entire research work at an expected time period.
5.4 Recommendations

- It has been identified that cloud data analysts face a major issue of handling personal information over the cloud system, with the implication of GDPR. This issue creates doubt regarding the security of personal information, which is required with the implementation of GDPR. In order to address this issue, it is required that the organisation focuses on the implementation of an algorithm or a system that can assure the cloud data analysts regarding the handling and security of personally identifiable information. This system must be easily understandable and easy to handle as complex systems can create risk regarding the security of personal information. With regard to the implementation of a new approach or system to ensure data security, data analysts must be provided with equivalent knowledge regarding the new system and the complete procedure to adopt the new system into usage (Chen and Zhao, 2012). It can be stated that with the adoption of a new approach or system, data security can be maintained to a great extent.

- The organisations which are working in the countries of the European Union are required to develop effective training programmes for their employees in order to enhance their knowledge about the policies and procedures of the GDPR. Most of the cloud computing analysts facing issues in working in accordance with the regulations of GDPR, which degrades their overall productivity towards the organisational performance. Thus, providing training would be beneficial for organisations to motivate the employees to work according to the regulation of GDPR and provide more improved services to their clients (Chen and Zhao, 2012).
Another major challenge faced by the cloud data analysts is regarding the application of data erasure, which helps in overwriting the existing information, to prevent it from leakage or theft. It is possible in the case of data erasure that the replicated information is not deleted from the hard drive, which may lead to theft of personal information of people. It is important that while applying the technique of data erasure, cloud data analysts focus on certain aspects, which can help in the application of the technique in an effective manner and also it is ensured that the replicated personal information is permanently deleted from the hard drive. Thus, it is important for cloud data analysts that particular standards are developed regarding the application of data erasure, which must be based on the needs of the organisation. This will ensure the effective implementation of data erasure technique. This standard must also involve a methodology, which must be ensured by the cloud data analysts that after the application of the technique, the methodology is checked for ensuring that all the personal details have been erased and overwritten throughout the device (Voigt and Bussche, 2017).

With the implementation of GDPR in the current scenario, it has been identified that the application of existing laws has been modified to GDPR. Thus, the cloud data analysts have to develop a new protection directive, which is different from that applied to previous laws of data security. This will ensure effective implementation of GDPR for data security. However, the new protection directive can create a challenge for the cloud data analysts in understanding the new directive and implementing it smoothly (Khan and Gouvia, 2017). Thus, for mitigating this challenge, it is important that the analysts are provided with appropriate knowledge and training so that they can
have a better understanding of the new directive. For the training sessions, professionals can be hired for providing training sessions so that data security can be maintained through new protective directive under the implementation of GDPR.

5.5 Future Implications

- For every future researcher, it is crucial to understand the suitability of the data collection methods because it helps in acquiring the detailed and subject related data for the research study. While developing the present research study, it has been observed that most of the researchers used a secondary method for the purpose of collecting the data, which has adversely affected their results. The present research study is carried out with the use of the primary method, in which the real-time and factual data was collected through the interview method (Tracy, 2012; Brannen, 2017). The interview data helped in presenting the effective and credible outcomes of the research study. In this relation, the future researchers must consider the primary method along with secondary, as it will help in enhancing the reliability of the research by presenting the practical results. In addition to this, it is equally important to select the data analysis method in accordance with the nature of the collected data. Adopting the interview method can help the researchers to collect the data from the respondents who belong to the similar field on which the research is carried out (Creswell and Creswell, 2017). This will be helpful for future researchers to obtain relevant and useful information from the selected respondents for the research work. If the future researchers are collecting the data through the interview method, they can use the thematic method, as it will enable them to interpret the data more efficiently.
• Future researchers are also recommended to present in-depth literature information in the research study. In order to present detailed information about the research context, it is important to conduct a detailed exploration of the previously developed researchers on a similar topic. This will help in having a proper understanding of the research subject, and it will also help in enhancing the credibility and authenticity of the research study. Moreover, the future researchers are also suggested to avoid copying the work of other researchers because copy and pasting the work of other researchers is considered as an offence. Avoiding plagiarism will be helpful in enriching the level of validity and authenticity of the research work (Tracy, 2012).
References


Experimental Design Research: Approaches, Perspectives, Applications


Team, I.P. 2017. EU general data protection regulation (GDPR): an implementation and compliance guide. IT Governance Ltd.


Appendices

Appendix 1: Interview Questionnaire

Q1. Do you think that organisational data is sensitive? How do protect your organisational data from the external users?

Q2. To what extent your organisation is using cloud computing? In what aspects, cloud computing is useful for organisation?

Q3. According to you, what are the current trend of the use of cloud computing by the multinational corporations in the UK in the reference to GDPR?

Q4. Do you think that cloud computing is better than traditional data storage approaches? If yes, How? Explain briefly?

Q5. In your opinion, what are the benefits of using cloud computing for business data protection?

Q6. In your opinion, what are the major challenges associated with the information security in cloud computing?

Q7. What is the impact of the latest general data protection regulations on your work?

Q8. According to you, what are prospective ways provided by GDPR of managing information security in cloud computing environment?
Appendix 2: Interview Transcripts

Interviewee A
Shanavas Hussain
Senior Cloud SME

Q1. Do you think that organisational data is sensitive? How do protect your organisational data from the external users?
Yes, organisational data quite sensitive. For protecting data from these external users, we at our organisation focuses on accessing data vulnerabilities and calculating risk scores to determine the severity of each capturing vulnerability. This has been made in numerical form which is translated further in qualitative forms such as high, low or medium”.

Q2. To what extent your organisation is using cloud computing? In what aspects, cloud computing is useful for organisation?

   for every organisation, customers privacy must be the first priority; however, the service providers are facing difficulty in securing the data of their customers due to ineffective security systems. In this perspective, cloud computing can be proved quite effective measure.

Q3. According to you, what are the current trend of the use of cloud computing by the multinational corporations in the UK in the reference to GDPR?

   In the UK, information security related legal arrangements such as GDPR has made the current world business practices faster and efficient by enhancing the interconnectivity between the systems as an outcome to internet-related advancements and now companies are using Cloud computing freely. In the EU, GDPR has been
announced for the purpose of eliminating the issue of data loss and give assurance to the customers that their data will not be shared, used, or leaked.

Q4. Do you think that cloud computing is better than traditional data storage approaches? If yes, How? Explain briefly?

*External threats are faced by our company due to diverse state-sponsored actors and hackers. The cloud computing allows us to ensure that only authorised person is having access to the data.*

Q5. In your opinion, what are the benefits of using cloud computing for business data protection?

*In this, the proliferation of mobile devices and smartphones having access to the internet has raised the demand of effective platforms to manage security concerns, and I think in managing these concerns the use of cloud computing platforms would be most optimal*

Q6. In your opinion, what are the major challenges associated with the information security in cloud computing?

*Enhancement in cloud computing platforms has raised several concerns pertaining to data security. This has been, I think due to increasing issues of data leakages, loosening of users’ control the confidential data and ensuring privacy are examined as the key challenge*

Q7. What is the impact of the latest general data protection regulations on your work?

*The implications of GDPR allows our organisation to make the work smooth and information more secured.*

Q8. According to you, what are prospective ways provided by GDPR of managing information security in cloud computing environment?
Time-to-time monitoring is crucial for every cloud-based service providers of their security systems that include algorithm, anti-virus, and antispyware, as it would help the service providers to create challenges for the hackers to control the confidential data of the users.
Interviewee B
Rajesh Ravi
Cloud Developer

Q1. Do you think that organisational data is sensitive? How do you protect your organisational data from the external users?
Yes, it is, and we use password and coding system for protecting such data.

Q2. To what extent your organisation is using cloud computing? In what aspects, cloud computing is useful for organisation?
Yes, we have started to use cloud computing measures frequently. Cloud computing provides my organisation with a high level of flexibility and efficiency.

Q3. According to you, what are the current trend of the use of cloud computing by the multinational corporations in the UK in the reference to GDPR?
GDPR is a newly announced regulation that includes different directives that are new for the cloud computing analyst that create challenges for the analysts to understand and implement appropriately. Most of the cloud computing analysts are lacking with detailed and relevant knowledge about the directives of the GDPR, which is affecting their overall efficiency. However, the implication of GDPR would be helpful for the cloud computing analyst to provide more secure services to the users, as the analysts can ensure the users regarding the protection of their data.

Q4. Do you think that cloud computing is better than traditional data storage approaches? If yes, How? Explain briefly?
In comparison to traditional data storage, the cloud computing prevents the issue of data lost and destruction as the data is not stored at physical location.

Q5. In your opinion, what are the benefits of using cloud computing for business data protection?
With the use of cloud computing, flexibility is fostered by enhancing scalability, cloud options, control choices, and tools selection, whereas, on the other hand, cloud computing brings efficiency in business operations by providing my organisation, greater accessibility, savings in costs, integrating high-security procedures and standards, and disaster recovery.

Q6. In your opinion, what are the major challenges associated with the information security in cloud computing?

_I think hacking is one of the key challenges associated with information security. It has raised the concerns on data security as the illegible activities of hackers have affected the cloud service providers’ capabilities that would make the cloud service vulnerable._

Q7. What is the impact of the latest general data protection regulations on your work?

_GDPR will produce significant implications on the organisation by demanding changes in the existing data architecture and technology platforms, along with re-engineering of present platforms and systems to meet all GDPR’s requirement and reduce risk pertaining to non-compliance with GDPR._

Q8. According to you, what are prospective ways provided by GDPR of managing information security in cloud computing environment?

_Due to the increasing issue of data theft, customers do not trust the service providers of cloud platforms, which has affected their businesses. Thus, it is vital for cloud computing analysts to identify the loophole in their services and try to rectify those issues in order to enrich the security systems. The cloud computing analysts are required to adopt an efficient anti-virus program for securing the cloud platforms from different malware attacks from unethical practitioners._
Q1. Do you think that organisational data is sensitive? How do protect your organisational data from the external users?

*Of course, organisational data is sensitive. For protecting our organisational, data we integrate cloud computing networks to manage all pertinent organisational data and resources.*

Q2. To what extent your organisation is using cloud computing? In what aspects, cloud computing is useful for organisation?

We are using cloud computing quite intensively to save our data. *Cloud computing networks have allowed my organisation and its individuals to store and safeguard their personal and confidential data on cloud-based technologies.*

Q3. According to you, what are the current trend of the use of cloud computing by the multinational corporations in the UK in the reference to GDPR?

*The cloud computing analysts have also become accountable to work in accordance with the new directives of GDPR, which is creating difficulties for them because they are completely unaware of the directives and procedures of GDPR, and due to this, the implication of GDPR might be affected adversely, and it can also create a problem in securing the data of customers.*

Q4. Do you think that cloud computing is better than traditional data storage approaches? If yes, How? Explain briefly?

*Yes, in my opinion cloud computing is an effective approach to data storage and in our organisation, we have already integrated it in our operational framework.*
reason for integrating it into the organisation is its role in leveraging organisational processes for creating more robust and secured business procedures that combat risks pertaining to data privacy, security, and availability.

Q5. In your opinion, what are the benefits of using cloud computing for business data protection?

*I believe that cloud computing minimises the time involved in storing the data, along with the minimisation of the cost of acquiring additional storage of data."

Q6. In your opinion, what are the major challenges associated with the information security in cloud computing?

*Due to the increase in the utilisation of Internet-based services in the current environment, the cloud computing analyst are confronting varied issues in securing the data of their clients. The unethical activities are increasing by the hackers due to this the cloud computing analyst are unable to control the data loss issue.*

Q7. What is the impact of the latest general data protection regulations on your work?

*The aim of the GDPR is to ensure the customers that their personal data is secured and cannot be used for any unethical practices. Thus, the organisations have to maintain transparency with the customers and needs to provide necessary information to the customers about their data.*

Q8. According to you, what are prospective ways provided by GDPR of managing information security in cloud computing environment?

*Most of the users of cloud services are facing the issue of data loss, and due to this, they stop using cloud-based services, which is also affecting the business profits of the organisation. Thus, the cloud computing analyst must focus on updating their security systems on a regular basis and can implement more effective anti-virus, and with the
use of antispyware, the cloud computing analyst can also identify the location from where the hacking practices are conducted. The organisations must adopt the GDPR in order to gain the trust of the users because it enables the service providers to facilitate full control to the users over their confidential data. In order to implement the GDPR practices, it is significant for the organisations to understand the new accountability principles of GDPR and change the strategy from theory to practice, as it will help the service providers to enhance the security of the data protection.
Interviewee D
Jinesh pattel
It System Admin

Q1. Do you think that organisational data is sensitive? How do protect your organisational data from the external users?

*Organisations are having diversified and crucial information which are sensitive by nature as it directly affects company’s performance. For protecting it, we save all the information on cloud with password protection.*

Q2. To what extent your organisation is using cloud computing? In what aspects, cloud computing is useful for organisation?

*We are using cloud computing for saving important information only. I think, it provides additional security and protection to our crucial data.*

Q3. According to you, what are the current trend of the use of cloud computing by the multinational corporations in the UK in the reference to GDPR?

*I think, GDPR provides effective legislation of data protection which has laid down the rules pertaining to processing, storing and managing the large data from the people of the EU. It is crucial for strengthening the EU’s data protection, as it enables a high degree of control and presentation of the significant requirement for data processors and controllers, including data protection*

Q4. Do you think that cloud computing is better than traditional data storage approaches? If yes, How? Explain briefly?

*I think the utilisation of cloud computing in my organisation has supported the organisation significantly in enhancing its data security, productivity, and overall organisational performance. It optimises IT infrastructure of my organisation by providing quick access to all required computing services*.
Q5. In your opinion, what are the benefits of using cloud computing for business data protection?

*Cloud computing has consolidated three key needs of the present century technology. These are the provision of autonomy to organisations by ensuring cost reduction and high agility*. "

Q6. In your opinion, what are the major challenges associated with the information security in cloud computing?

*The challenges are linked to weak measures of cloud security of the services, such as encryption, storing data without controls, and theft of intellectual property. Along with this, the challenges pertaining to violations of compliance and regulatory requirements, loss of control on the end users, malware infections and contractual breaches with business partners or customers*.

Q7. What is the impact of the latest general data protection regulations on your work?

*Now our organisation is bound to work in accordance with the GDPR and protect the privacy of every customer. Before GDPR, the organisations are allowed to use the data of their customers; however, after GDPR came into practice, the organisations that are providing cloud-based services to the customers do not have any control and not allowed to use the customers' confidential data. It is a challenge of the organisations, as they cannot increase their customer base by accessing the data of other customers.*

Q8. According to you, what are prospective ways provided by GDPR of managing information security in cloud computing environment?

*The cloud computing analysts are losing control over the security of the confidential data of the users due to ineffective firewalls and anti-virus. Thus, in order to gain*
customer loyalty, data protection must be the first priority of the service providers. The data protection practices can be enhanced by using the highly improved encryption system and two-factor authentication. This creates difficulties for the hackers to access the confidential data of the users. Two-factor authentication is an effective process that strengthens the platforms where the data of users is saved. The two-factor authentication requires a password and facial recognition to access the data of users. Thus, using this security measure can be helpful for cloud computing analysts to enrich the data protection system. Moreover, different organisations that provide cloud-based services to different people are facing issues in implementing the GDPR due to lack of knowledge and awareness; however, as per the EU, it is vital for every organisation to adopt GDPR for data protection. In this case, the organisations need to acquire detailed knowledge about the procedures and regulations, as it will help in implementing the GDPR more efficiently.
Interviewee E  
Mubaher Muhammed  
Soft Ware test Eng  
Q1. Do you think that organisational data is sensitive? How do protect your organisational data from the external users?

YES, *some of the organisational data is sensitive which requires high degree of protection. For protecting such data, in our organisation, we do not give access of such data to anyone. Only top-level managers and department heads can access this data.*

Q2. To what extent your organisation is using cloud computing? In what aspects, cloud computing is useful for organisation?

*Our organisation is using cloud computing aggressively for all the operations as cloud computing allows our company to have secured and convenient system for data protection.*

Q3. According to you, what are the current trend of the use of cloud computing by the multinational corporations in the UK in the reference to GDPR?

*Implementation of GDPR, I think would produce significant positive implications on the data security levels and individuals which control their personal information and data over the cloud computing platforms. Due to this crucial aspect, UK’s multinationals are using cloud computing effectively. As per the guidelines of GDPR, every cloud computing analyst working in an organisation have to maintain transparency and are enforced to reveal their practices as what they are doing with the customer data. This is a major challenge of the organisations to reveal their operation in front of every customer. In addition, they are also facing the challenge as an implication of GDPR that they need to delete the data as per the request of the*
customers, which is a challenge for the old organisations which is maintaining the customer data from a longer period of time

Q4. Do you think that cloud computing is better than traditional data storage approaches? If yes, How? Explain briefly?

I think, cloud computing is more convenient approach as it allows the access to data to all the authorised user which reduces the requirements of sending files to different users.

Q5. In your opinion, what are the benefits of using cloud computing for business data protection?

I think, saving of time in data saving, and retrieval is the main benefit of using cloud in operation.

Q6. In your opinion, what are the major challenges associated with the information security in cloud computing?

    hackers are using more advanced systems as compared to the organisations that create major challenges for the cloud computing analysts to eradicate the issue of data loss. Due to the ineffective security measures, the hackers are easily stealing the confidential data of their clients, and it is affecting their brand image in the market.

Q7. What is the impact of the latest general data protection regulations on your work?

The implementation of GDPR in my work would enable acquisition of information regarding the manner in which personal data is needed to be used, and also my organisation can trace the location from where the information is used by legible and non-legible users”.

Q8. According to you, what are prospective ways provided by GDPR of managing information security in cloud computing environment?
Data encryption is considered important in securing the data from the unethical practices of the hackers. Implementing the data encryption strategy can be helpful in ensuring the data protection of the users' data. The implication of data encryption creates multiple challenges for unethical practitioners to decrypt the data.
Interviewee F
Rakesh Sukumaran
Cloud Architect
Q1. Do you think that organisational data is sensitive? How do protect your organisational data from the external users?
Yes, organisational data is sensitive, and we focus on using firewalls, password protection to prevent any external access to data.
Q2. To what extent your organisation is using cloud computing? In what aspects, cloud computing is useful for organisation?
Our organisation has just implemented cloud computing in operation. I think, cloud computing will allow us to save time in data saving and protect it from external threat.
Q3. According to you, what are the current trend of the use of cloud computing by the multinational corporations in the UK in the reference to GDPR?
In the UK, companies are required to be aligned with GDPR requirements. The non-compliance with GDPR will be considered as a breach of EU guidelines and due to this an organisation has to pay a heavy fine. Moreover, as per the guidelines, an organisation has to maintain the security of customer's data because any breach of data would be a challenge for the organisations and heavy penalties would be imposed on the organisations. The cloud computing analysts have to follow every guideline of GDPR in their services and protect the data of the customers from any kind of breach.
Q4. Do you think that cloud computing is better than traditional data storage approaches? If yes, How? Explain briefly?
I feel in comparison to traditional data storage process or system; cloud computing is an optimal method of information security. It involves low-budget in the implementation of security systems, cost reduction, flexibility, increases efficiency, requires less knowledge and training to implement and provide security gains to my organisation”.

Q5. In your opinion, what are the benefits of using cloud computing for business data protection?

The use of cloud computing networks enhances the efficiency of business operations by facilitating wide access to data from diverse locations across the world, implementing best standards of security to protect and save the data, and provide tailor-made solutions to my organisation.”

Q6. In your opinion, what are the major challenges associated with the information security in cloud computing?

I think, using inappropriate security systems and software also create several challenges for the cloud computing analysts to secure the confidential data of their clients. It is important for the organisations to implement the suitable and effective anti-virus that provides enhanced security to the users in protecting their personal data. The data breach is an issue faced by a large number of populations, and their data is used for illegal purposes. The cybercriminals are using the strategy of sending emails with malware to people for getting access to their private data

Q7. What is the impact of the latest general data protection regulations on your work?

GDPR would produce implications on every company, but I feel that the hardest hit will be faced by the organisations which hold and processes a wide range of consumer data, such as marketers, technology firms and the data brokers."
Q8. According to you, what are prospective ways provided by GDPR of managing information security in cloud computing environment?

In order to eradicate the issue of data theft, the organisations can hire ethical hackers for strengthening the security system, and it also helps in tracking the hackers and limits their practices. Additionally, as per the GDPR regulation, the organisations cannot use the data of their client with their permission; however, on the basis of GDPR guidelines, the organisations can take consent from their client to use their data. The service providers are required to build a strong relationship with their clients in order to get access to their data.