BIG DATA SERVICES SECURITY AND SECURITY CHALLENGES IN CLOUD ENVIRONMENT

Raed Alsufyani[1], Khursand Jama[1] ,Yulin Yao[2] , Muthu Ramachandran[1] and Victor Chang[1]
[1]*School of Computing, Creative Technologies and Engineering, Leeds Beckett University, Headingley, Leeds LS6 3QR, UK*
{r.alsufyani5478; k.jamal3932}@students.leedsbeckett.ac.uk; { M.Ramachandran; V.I.Chang}@leedsbeckett.ac.uk
[2]*Freelance Consultant, Anastaya, United Kingdom, UK*
yulinyao.forever@gmail.com

Keywords: Cloud computing, big data, security and data storage issues, privacy.

Abstract: This paper explores security issues of storage in the cloud and the methodologies that can be used to improve the security level. This study is concluded with a discussion of current problems and the future direction of cloud computing. Big data analysis can also be classified into memory level analysis, business intelligence (BI) level analysis, and massive level analysis. This research paper is based on cloud computing security and data storage issues that organizations face when they upload their data to the cloud in order to share it with their customers. Most of these issues are acknowledged in this paper, and there is also discussion of the various perspectives on cloud computing issues.

1. INTRODUCTION

Big data represents a new era in data exploration and utilization. Current technologies such as cloud computing and business intelligence (BI) provide a platform for the automation of all processes in data collecting, storage, processing and visualization. Big data is defined as having the following five V properties: volume, velocity and variety which constitute original big data properties. Big data velocity deals with the speed of the data processing of the datasets or the processing of a large volume of data. Big data veracity refers to noise and abnormality in the data as all data elements are not required for analysis. Big data validity deals with the correctness and accuracy of the data considered for analysis. Chen et al. (2010) state the economic case for cloud computing has brought unlimited attention to this technology. Cloud computing providers can mount data centres easily due to their ability to classify and provide computing assets. The emergence of the cloud and big data comes with data security and privacy security concerns. System integrators (SI) have been developing solutions that incorporate the cloud and big data within the enterprise to build elastic, scalable, private cloud solutions. Many organizations are working in the field of cloud computing and invest heavily so that customers get the service at a cost saving. There is a subsequent interest of permit suppliers to achieve better use through measurable multiplexing and to allow clients to avoid acquisition costs through the scale of the active element. Passary (2014) states that organizations of superior data centres are the most likely devotees of the cloud. Leading organizations such as CAP, Infosys, Deutsche Telekom, Disney and others trust and use the cloud on the World Wide Web (WWW) to release information as well as for shopping. Security issues related to cloud computing are a huge concern, and organizations and associations need to be aware of them. Also, this refers to more than a few organizations who are now seeing the problems that frequently occur.

This paper explicates cloud computing to emphasise its definition and classifications in order to explore security issues of storage in the cloud and the methodologies that can be used to increase the security level. The study will focus on cloud security

challenges that organisations still face when storing information in the cloud.

The commonly used definition is that cloud computing is a cluster of distributed computers that offer on-demand resources and services over a networked medium, commonly the Internet (Sultan, 2010). It is worth understanding that it entails the deployment of groups of remote servers and software networks, which allow the centralized storage of data and access to computer services through the Internet (Mokhtar et al., 2013).

2. LITERATURE REVIEW

The concept of a massive computer network was first introduced by J. C. R. Licklider in 1969 who had an obligation to initiate training to improve the Advanced Research Projects Agency Network (ARPANET). The perspective was to unite all people on the Web with the aim that information could be reached always and anywhere.

Chang et al. (2016) says that, as a needed accumulation of data, it is a key factor to securely store the information of the personal computer (PC). The client's main motive for storing data in the cloud is to save costs and have 24/7 information access. The cloud computing service allows users to securely store any type of data in the cloud and then access it from anywhere in the world with Internet access. The basic element of this service is the storage capacity. Also, organizations that provide information to their clients face various issues relevant to cloud security. The Cloud Security Alliance (CSA) is working on cloud security issues, and its members are concerned that there central issues be resolved. The central issues that have dominated the field for many years are privacy, respectability and accessibility.

2.1 Security Challenges of Cloud Computing

There are three basic cloud security problems that gain the most attention today: confidentiality, integrity and availability. Whenever administrators work on cloud security, these three aspects must be considered. Confidentiality is about applying a safety shield to prevent access by an unauthorized person. Integrity means protecting the data from access by users who are not approved by their organizations. Availability is about accessing data anytime, anywhere and whenever the user wants. The main difficulties experienced are securing the data and making it available to the customer with security system approval. The security guarantee mechanism begins with validation, approval and coding. Here, there are three security concerns need to be examined: identification and authentication, authorization and encryption.

2.1.1 Identification and Authorization

It is necessary to assign strong passwords for cloud security. Due to this requirement, many users create long, complicated passwords that are extremely difficult to remember. However, the longer and more complex the password, the more difficult security is to break. Human beings do many things in the course of a day and often have many things they need to remember, so it may be very difficult for the user to remember these complex of passwords in order to safely obtain access.

2.1.2 Authentication

The verification procedure ensures that an approved person can access information stored in the cloud. Some clients have access to use the information, but that access may be limited by their employee grade level. They are then not able to access information that is rated above their grade level.

2.1.3 Encryption

Encryption methodology is a strategy that secures sensitive information in the cloud. Conventional encryption is done when exchanging information records, and then it is unscrambled.

Talib et al. (2012) state that, today, focusing on information security is a challenge because information security capacities are more discriminating and more difficult to research because of the expansion of the system's clients. Currently, many issues are important, but a central focus issue is the security of stockpiling data. This is an essential concern of the general population whose transfer of their own information to the cloud requires that they can access that information securely from anywhere.

Yu et al. (2012) argue that construction planned modelling depends on the cloud in two spaces: user space and kernel space. With the help of the Web interface, these are associated with each other. These spaces have different functions in the

core area of the cloud that belong to physical access and control.

Wang et al. (2009) state that data security is the cloud storage theme and it is fundamentally a structure spread limit. In addition, they unveiled a proposed solution to ensure the accuracy of the data of customer cloud data storage, an effective and versatile method to reinforce the element of data security includes the review of squares and the deletion and connection of an annihilation-contingent to help in the assignment of registry codes to give repetition vectors equity and ensure the reliability of the data.

Du et al. (2010) introduced the provision and use of the Run Test, another verification structure of the honesty of an organization to confirm the reliability of the management of the flow of information with the use of cloud systems. The Run Test affirmation of the level of implementation of random data to indicate any pernicious data flow is used to prepare suppliers' organizations for giant scale cloud bases.

Takabi et al. (2010) stated that, in regard to PC security frameworks, it is a distinctive type of recording circumstance. First, he takes into account the customer's security framework and relates courses of action used in the past. To ensure security and customer confidence, you can use different types of modules for the safety system. These modules are used to oversee the affairs of an entity, such as the organization of identity, access control, course of action commitment between different entities, organizational trust between particular fundamentals that belong to the cloud and its customers, ensuring the development, organization, consolidation and semantic heterogeneity between different methodologies.

Zissis et al. (2012) states that cloud computing is the graphical flow and framework of the network. Using the cloud, office clients upload their confidential data. This is less expensive and requires less space than traditional storage methods. This information can be accessed anytime, anywhere in the world. As times passes, more customers become aware of this method, and that increases the number of customers who are using it. The cloud computing system was introduced in 1967 when it was only accessible to influential associations or organizations. In short, there was not much expansion in the number of customers at that time which made the system easy to monitor. As time progressed, however, the customer base expanded due to great demand in such areas as security. Unfortunately, information professionals were soon faced with clients who felt unsafe in the cloud.

A style of computing evolved where massively adaptable skills were needed in the administration of the Internet to serve numerous foreign clients, according to Plummer et al. (2009). There had to be an unbiased and very adaptable authority to oversee an intricate network to facilitate the final and successful use of client applications (Staten, 2008).

The goal of infinitely accessible computer activity was the responsibility that needed to be assumed for customers of the cloud, and the ability to pay for the use of that activity had to become a calculated asset on a temporary basis as required (Armbrust et al., 2009).

A type of parallel frame consists of an accumulation of interconnected, virtualized components and is provisioned and introduced as one or more links to processing assets, taking into account the level of the states of service built through transactions between the provider of management and buyers (Buyya et al., 2009).

2.2 Cloud Storage in a Private Cloud Deployment

Beaty et al. (2009) and Armbrust et al. (2009) argue that exchanges between vendors with different types of cloud systems are not easy to execute. Frequently, the work requires composing additional layers of application programming interface (API), an interface or portal to enable communication. This suggests interesting research on the portability question as some desktop applications to cloud portability are questioned.

Chang et al. (2013) state that it is essential to mount an investigation of the Cloud Computing Business Frame (CCBF) that participates in the stages of service as a strategy for design, development, testing, and user support. The type of cloud an organisation adopts will depend on the organisation's needs, volumes, types of services and data it plans to have and use (Chang, 2014).

2.3 Enterprise Portability

Enterprise portability is portability that enables the movement of data, applications and administrations from desktop to clouds and between different clouds. It includes IaaS, PaaS and SaaS usage services. There are different prerequisites for portability in many areas. These kinds of cloud tasks convey their effectiveness and develop client satisfaction. CCBF expects to create an effective cloud design for usages and services with the help of various associations (Chang et al. 2011).

This research concerns the relationship between healthcare and portability. There are two aspects in which portability plays an influential role in the healthcare industry: the migration of previous infrastructure and the development of new platforms that allow cloud service development.

Cloud storage is a private cloud and an initial centre that builds the foundation of IaaS. It allows for the storage of medical databases, graphics and research in a secure setting that belongs to the working community. The Centre then becomes a review of IaaS to PaaS, and this allows for the best management of the organization and its and assets.

3. BIG DATA SECURITY MODEL AND HYPOTHESIS

A hypothesis is a prediction that shows the relationship between two variables. It is a testable prediction about what a researcher expects to happen in the research. There are different ways to obtain the results of research to gain evidence to support a hypothesis. Many researchers draw the hypothesis from a specific theory; some draw it from previous research. For example, consider the relationship between stress and the immune system. One hypothesis could be that stress can have a negative impact on the immune system. If a person is stressed, that person's immune system can be affected. This demonstrates a causal relationship, where one thing can be seen to cause another (Cherry et al. 2015). Similarly, some hypotheses state that what is relevant to cloud computing security also affects the security system.

3.1 Trust

Confidence is another topic of exploration in computer science, related to different areas such as access control and security in PC systems, dependability in scattered frames, fun hypothesis, operator frameworks and arrangements for election creating instability. Perhaps the most notable case was the development of the Trusted Computer System Evaluation Criteria (TCSEC) used from the late 1970s to the mid-1980s. Confidence was used here to persuade users that a framework (model, configuration, or implementation) was correct and safe.

Confidence in the information society is based on various reasons, such as mathematics, learning or social contexts. Trust in a partnership could be described as the confidence a customer has that the association will generate an accurate and reliable authority and the certainty that it will also communicate customer confidence in its ethical reliability, the strength of its operations, the viability of its security systems, and compliance with all regulations and laws. At the same time, it also contains the element of risk. The idea of security refers to a given circumstance, where every single conceivable danger is removed or transformed into an idea of confidence, to be changed according to the two meetings in an exchange instance. This can be portrayed after it happens as 'an element of A is considered to depend on another substance. When it relies on item A, item B will act exactly is not surprising and forced.' Thereafter, a substance can be considered reliable if meetings, or the people involved intrude on that element, depend on its validity. In general, as stated previously, the idea represented can be spoken of with reliability, which refers to the nature of a person or a substance that is worthy of trust. Confidence in the information society is based on distinguishing different things, taking into account math and information or social considerations. The idea of trust in a partnership could be characterized as the conviction of the customer that the association is ready to give accurate and reliable services. A warranty is needed that communicates customer confidence in its ethical honesty, strength of its operation, adequacy of its security components, and fitness and compliance with all regulations and laws, while, at the same time, it also contains the affirmation of a variable risk basis for the party depending on it. The idea of security refers to a particular circumstance where every conceivable danger is destroyed or reduced to an absolute minimum (Zissis et al., 2012).

Rashidi (2012) describes the security of the cloud computing model and presumes that confidence is the main interest of the user.

Hypothesis 1(a): Trust is the factor of belief that is required in the cloud computing organization because it increases the use of its services.

3.2 Security

The three main aspects of security are the confidentiality, availability and integrity of the data or information. Security authentication and good reputation are also essential.

The cloud computing environment provides two types of computing and data storage capabilities. The cloud computing environment, due to its architectural design and unique characteristics, imposes a number of security benefits, including centralization of security, data and process

segmentation, redundancy and high availability. While many risks are effectively countered, due to the infrastructure's singular characteristics, a number of distinctive security challenges are introduced. (Zissis et al., 2012). During the accession and processing of information, customers do not know where the information is saved, but they do know machines run the calculation tasks. The user is concerned with only one thing: security. The user wants to search for and access data at any time and in a safe manner (Zhou, 2014).

Hypothesis 2(a): Security is the main aspect of the cloud service as it provides a satisfactory environment.

Hypothesis 2(b): Security is the combination of confidentiality, integrity and availability that helps increase the security level.

3.3 Privacy

Privacy refers to the declaration of, or adherence to, various standards, both legal and illegal. In Europe, this is often understood as consistency with the rules of information safety in regards to one's private life. In the European environment, this is understood commonly as normative, consistent and safe information, despite the fact that there would be exceptionally intricate issues of cloud computing over the full range of security and administrative architectures and insurance of privacy of individual information. Recognized security standards give a valuable guide and name the components: consent, purpose of the restriction, legitimacy, transparency, information security and participation of the data subject (Robinson et al., 2010).

Hypothesis 3(a): Privacy is integral to data safety on the cloud as it increases user confidence and satisfaction.

3.4 Long term viability

Often, clients will require the reputation of a cloud supplier to be well established and of long duration. They want to find out about the risks of cloud experiences, such as outages, crashes or other problems. 'Preferably, calculation cloud provider should never go belly up or get won by a larger organization. In any case, it must be ensured the customer about the information remain available even after such an occasion.' (Rashida, 2012).

Hypothesis 4 (a): Long-term viability is strongly identified with customer confidence in cloud computing.

Hypothesis 4(b): Long-term viability reduces dissatisfaction and builds user trust.

4. METHODOLOGY AND RESULTS

The methodology section addresses cloud computing security and security challenges. Secondly, it includes some relevant literature reviews about cloud computing and how it has impacted organizations. Thirdly, the data are presented like a hypothesis instrument validation and refinement process. The last step is the explanation of the hypothesis testing results.

4.1 Survey Questions

Survey question were designed based on the hypothesis and are presented in this section. During the research, it was found that many organizations use the cloud computing storage facility for business, and some are totally based on this facility. So, to get the appropriate results, it was necessary to develop a questionnaire that presents questions relevant to this research and are easy for the respondent to answer. Two types of questionnaires are part of this study. The first is for that population who has knowledge about this field and also has education and work experience. The second questionnaire is for those who have less knowledge about this field, are part of this facility but are not frequent users.

The chosen technique is a review that shows the issues surrounding cloud computing data storage. For this, we need to examine security issues that organizations still face. There are numerous associations and organizations who are utilizing office cloud computing, yet they continue to have many security issues regarding information storage and access to the cloud. The majority of the associations maintain their organizations completely with cloud computing administration, so security issues are extremely important to them because numerous endorsers are utilizing their services subsequent to getting the association's participation. In addition, organizations encourage clients to use cloud computing in their offices to satisfy the general population's request for it.

4.2 Data Collection

Two methods were used to collect the data from the respondents. The first questionnaire, made by using SurveyMonkey, consists of ten questions. After creating the questionnaire, we distributed it to university students and, secondly, sent it online to many students in the United Kingdom. This

questionnaire is for students who have. Some of these are also part of organizations who do use cloud computing storage in their businesses. Data were gathered from multiple sources at various points in time. Over 100 people answered the questionnaire and sent their replies. The total number of respondents is 107, of which 101 attempted to answer all the questions. This means that the 90% response rate makes this a valid sample size.

This research is based on cloud computing security and data storage issues so that many of the questions are relevant to security. The questionnaire is the main part of the research, and it is very important to find the respondents' points of view about people or consumers who stop using the cloud computing facility. A total of 93% of the respondents said that security concerns stop people from using cloud computing because every user and organization wants the data that is stored in the cloud to be secure. One question asked respondents which is the one most worrisome issues about cloud computing. A total of 70% of the respondents named physical and network security. All the results showed that organizations and users want to use this facility, but they are more concerned about the security issues. They want privacy and do not want to their personal and confidential information compromised.

Measure	Item	Count	Percent
Awareness of Cloud Computing Term			
	Yes	**94**	89.5%
	No	**6**	5.7%
	Not Sure	**5**	4.8%
Security Professionals Warn Against Cloud			
	Agree	**97**	91.5%
	Not Agree	**4**	3.8%
It Is Safe to Store Data			
	Agree	**78**	73.6%
	Not Agree	**11**	10.4%
	Not Sure	**15**	14.2%
Awareness about Cloud Security Alliance			
	Yes	**83**	79%
	No	**14**	13.3%
	Don't Know	**8**	7.6%
How Secure Is Cloud Computing			
	Very Poor	**1**	1%
	Poor	**6**	5.7%
	Fair	**68**	64.8%
	Good	**14**	13.3%
	Very Good	**16**	15.2%
It Protects the Data Single-handedly			
	Agree	**86**	81.1%
	Not Agree	**15**	14.2%
Important Aspects of Cloud Security Policy			
	Firewall	**43**	41%
	Anti-Virus	**13**	12.4%
	Authentication	**48**	45.7%
	Other	**1**	1%
What Stops You from Using Cloud Computing			
	Security concerns	**98**	93.3%
	Loss of control of data and systems	**29**	27.6%
	It is still an evolving concept	**8**	7.6%
	Hard to integrate with in-house systems	**19**	18.1%
	Availability concerns	**19**	18.1%
	Performance issues	**33**	31.4%
	Other	**0**	0%
What Do You See as the Other Benefits			
	Improved data security	**84**	80.8%
	Increased storage capacity		56
	Scalability and flexibility - meets the needs of the business	**21**	20.2%
	Ability to access data and applications from anywhere	**19**	18.3%
	Removal of non-core activity so IT staff can focus on	**13**	12.5%

	adding value		
	Ease of software updates	**27**	26%
	Online back-up integrity	**11**	10.6%
Issues That Are More Concentrated			
	Guarantees for Peak Loads	**9**	8.7%
	Support and Management of Incidents	**7**	6.7%
	Quality of Service in general	**15**	14.4%
	Physical and Network Security	**73**	70.2%
	Other	**0**	0%
Evaluating Cloud Technology for Business			
	Yes, we are evaluating it now	**73**	68.9%
	Yes, we have plans to evaluate in the next 12 months	**23**	21.7%
	No, we have no plans to evaluate or implement it	**10**	9.4%

4.3 Data Analysis of the Data Collection

This section is about the analysis of data collection. Table 3 shows the resulting values of the mean, standard deviation and P-value that supports the hypothesis. The resulting values of the P-values must be less than 0.05 to indicate the accuracy of the results of the data

Serial No.	**Mean**	**Standard Deviation**	***P-Value***	**Remarks**
TR1	3.80	0.80	0.04	TR section has the high Standard deviation values.
TR2	3.60	0.60	0.03	
SE1	4.00	0.70	0.04	
SE2	4.30	0.40	0.02	
SE3	4.40	0.30	0.03	
SE4	4.70	0.20	0.02	
SE5	3.90	0.40	0.03	SE section has the lowest standard deviation values
PR1	3.70	1.00	0.05	
PR2	3.50	0.80	0.03	PR section has the highest standard deviation values.
LT1	3.40	0.50	0.04	
LT2	3.30	0.20	0.03	LT section has the lowest standard deviation values.

For the first section of the hypothesis (TR1 to TR2), the mean values are 3.80 to 3.60 where the standard deviation values are 0.60 to 0.80, and that represents a significant range. The p-values of TR1 to TR2 are less than 0.05 which indicates that the probability of the null hypothesis is low. The second category has values from SE1 to SE2 in which mean values are 3.90 to 4.70 and where the standard deviation values are 0.20 to 0.70. This section has the lowest p-values which means its results are more accurate and most of the participant's views are the same in the more than 100 sample size. Further analysis showed that, for the third section with PR1 to PR2, the mean values are 3.50 to 3.70, where the standard deviation values are 0.80 to 1.00. The p-values are 0.03 to 0.05. In this section, some participants totally agreed with this hypothesis. The fourth and last hypothesis section is LT1 to LT2 in which the mean values are 3.30 to 3.40. The standard deviation values are 0.20 to 0.50 where p-values are 0.03 to 0.04. Many points of view of the participants are positive, and that helps to determine the results. A possible explanation for some of our results may be the lack of adequate differences, but most of the responses connect to the research questions.

5. CONCLUSION

As many people are fully aware, the cloud and big data have data security and privacy concerns. This is why system integrators have been building

solutions that incorporate the cloud and big data within an enterprise to build elastic, scalable private cloud solutions. The cloud has glorified the as-a-service model by hiding the complexity and challenges involved in building an elastic, scalable self-service application. The same is required for big data processing. Cloud computing is a promising application and innovation of these times. This combination of findings provides some support for the conceptual premise that the barriers and obstacles to the rapid development of cloud computing are issues of safety and security of information. Data storage and process cost reduction are mandatory requirements of any association, while the research of information and data reliability is now mandatory in each of the associations when making choicesThis research has raised many questions in need of further investigation. The cloud and its administration have some impact on the significance of what the vendor of cloud services provides for the certification of data.

6. REFERENCES

Archer, J., Cullinane, D. and Puhlmann, N. et al (2009). *Security Guidance for Critical Areas of Focus in Cloud Computing*, 2.1.

Alsufyani, R. and Chang, V., 2015. Risk Analysis of Business Intelligence in Cloud Computing.

Bell, J. (1993). *The Irish troubles*. New York: St. Martin's Press.

Bell, J. (1999). *Doing your research project*. Buckingham [England]: Open University Press.

Biggam, J. (2008). *Succeeding With Your Master's Dissertation*. Maidenhead: McGraw-Hill International (UK) Ltd.

Chang, V., 2014. *A proposed model to analyse risk and return for Cloud adoption*. Lambert Acedemic Publishing.

Chang, V., Ramachandran, M., Yao, Y., Kuo, Y.H. and Li, C.S., 2016. A resiliency framework for an enterprise cloud. *International Journal of Information Management*, *36*(1), pp.155-166.

Chang, V. (2014). The Business Intelligence as a Service in the Cloud. *Future Generation Computer Systems*, 37, pp.512-534.

Chang, V., 2015. Towards a Big Data system disaster recovery in a Private Cloud. Ad Hoc Networks, 35, pp.65-82.

Chang, V., Walters, R.J. and Wills, G.B., 2015. Cloud Computing and Frameworks for Organisational Cloud Adoption. *Delivery and Adoption of Cloud Computing Services in Contemporary Organizations*, p.1.

Chang, V., Kuo, Y.H. and Ramachandran, M., 2016. Cloud Computing Adoption Framework–a security framework for business clouds. *Future Generation Computer Systems*.57, pp24-41

Chang, V., John Walters, R. and Wills, G. (2011). Cloud Storage in a private cloud deployment: Lessons for Data Intensive research.

Chang, V., Walters, R.J. and Wills, G., 2013. The development that leads to the Cloud Computing Business Framework. *International Journal of Information Management*, *33*(3), pp.524-538.

Chen, Y., Paxson, V. and Katz, R. (2010). *What's New About Cloud Computing Security?*.

Mohamed Talib, A., Atan, R., Abdullah, R. and AzrifahAzmi Murad, M. (2012). Towards a Comprehensive Security Framework of Cloud Data Storage Based on Multi Agent System Architecture. *Journal of Information Security*, 03(04), pp.295-306.

Mohamed Talib, A., Atan, R., Abdullah, R. and AzrifahAzmi Murad, M. (2012). Towards a Comprehensive Security Framework of Cloud Data Storage Based on Multi Agent System Architecture. *Journal of Information Security*, 03(04), pp.295-306.

Passary, S. (2014). *Cloud computing is the future but not if security problems persist*. [online] Tech Times. Available at: http://www.techtimes.com/articles/8449/20140615/cloud-computing-is-the-future-but-not-if-security-problems-persist.htm [Accessed 11 May 2015].

Passary, S. (2014). *Cloud computing is the future but not if security problems persist*. [online] Tech Times. Available at: http://www.techtimes.com/articles/8449/20140615/cloud-computing-is-the-future-but-not-if-security-problems-persist.htm [Accessed 11 May 2015].

Ramireddy, S et al. (2010). *Privacy and Security Practices in the Arena of Cloud Computing - A Research in Progress*.

Rashidi, A. (2012). A Model for User Trust in Cloud Computing. *International Journal on Cloud Computing: Services and Architecture*, 2(2), pp.1-8.

Robinson, N., Valeri, L., Cave, J., Starkey, T., Graux, H., Creese, S. and Hopkins, P. (2010). The Cloud: Understanding the Security, Privacy and Trust Challenges. *SSRN Electronic Journal*.

(2012). *A Descriptive Literature Review and Classification of Cloud Computing Research*.

Zhou, Z. (2014). *Data Security and Privacy in Cloud Computing*.

Zissis, D. and Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), pp.583-592.