International Journal of Technology 12(5) 1038-1047 (2021)
Received June 2021 / Revised October 2021 / Accepted November 2021

International Journal of Technology

http://ijtech.eng.ui.ac.id

Developing a Blockchain-based Data Storage System Model to Improve Government Agencies' Organizational Performance

Mohammed Ali Berawi[1,2*], Mustika Sari[2], Fikroh Amali Fahmi Addiani[2], Nunik Madyaningrum[2]

[1]*Department of Civil and Environmental Engineering, Faculty of Engineering, Universitas Indonesia, Kampus UI Depok, Depok 16424, Indonesia*
[2]*Center for Sustainable Infrastructure Development, Faculty of Engineering, Universitas Indonesia, Kampus UI Depok, Depok 16424, Indonesia*

Abstract. Confidential documents in possession of government agencies are considered as assets that must be protected. Government agencies have started implementing cloud data storage systems to document data in a centralized network. However, this data storage system has been well-known as being threatened by data security, integrity, and data availability risks. On the other hand, blockchain technology, a decentralized, fast, secure, transparent, and recorded data storage system, is considered as the solution for mitigating these risks. Therefore, this study aims to identify the dominant risk factors of implementing the cloud computing storage system in government agencies potentially impacting its organizational performance and developing a risk-based data storage system that considers blockchain technology. This research used questionnaire surveys, case studies, and expert interviews to obtain its research objectives. The results demonstrated that six dominant risks included data theft and breaches, data corruption caused by virus attacks, limited storage space, data loss caused by system damage, data being accessed without particular access rights, and lack of guarantees from the system when a security threat occurred. A model for the blockchain-based cloud data storage system is proposed to address these risks and to improve the organizational performance of government agencies.

Keywords: Blockchain; Cloud; Data storage system; Government agencies

1. Introduction

To carry out its duties and functions mandated by law, government agencies require thorough data protection systems (Hill, 2014). Confidential documents and classified information in these agencies are considered as government assets that must be protected during use, storage, or transmission of information through the application of policies, education, and technology (Whitman and Mattord, 2018). Therefore, a secure data storage system in government agencies is needed, particularly for agencies that possess confidential data and information in their documents, considering the large volume and the high value of information that must be managed and protected from all possible threats.

Like many other countries, Indonesia has widely implemented cloud storage systems to document data and information in its government agencies. Cloud computing is a scalable

*Corresponding author's email: maberawi@eng.ui.ac.id, Tel.: +62-21-7270029; Fax.: +62-21-7270028
doi: 10.14716/ijtech.v12i5.5237

and reliable platform that requires minimal management effort (Natesan and Chokkalingam, 2019; Wong et al., 2019). However, its security is still prone to cyber-attacks (Vurukonda and Rao, 2016). With the amount of data that keeps increasing every year, data integration and confidentiality have become crucial aspects that the institutions must consider in improving the data storage system (Irion, 2013; Lnenicka and Komarkova, 2019). In a traditional storage system, centralized data control does not guarantee the data's confidentiality, integrity, and authenticity. Therefore, a distributed data storage technology known for protecting data authenticity, confidentiality, and integrity is needed for government agencies (Rajalakshmi et al., 2018).

Digital technology has become one of the factors that influence the organizational performance of governmental agencies (Khin and Ho, 2019). The implementation of data and information storage systems influences the agency's work performance in terms of having the security threat as a risk portfolio borne by the agency (Abd Al Ghaffar, 2020). Therefore, risk factors in the current data storage system and their potential impacts on the government agency's organizational performance need to be examined. The risk-identifying process conducted in this paper was done through a risk management approach to identify the dominant risk factors.

Blockchain is a distributed ledger that uses public-key encryption and consensus protocol verifying the authenticity to record data on nodes called blocks in a secure, transparent, decentralized, cost-effective, and time-efficient manner (Cai, 2018). It can be perceived as a group of people sharing data using no intermediary agents, where trust between all the involved parties can still be built since all parties can see all the occurring transactions in the blockchain network (Berawi et al., 2020). Moreover, with its decentralized nature, the data is controlled by all participants in the network with a consensus protocol that rules the system (Rajalakshmi et al., 2018).

Previous studies (Ølnes et al., 2017; Alketbi et al., 2018; Razzaq et al., 2019) argued that blockchain has tremendous potential for government services, as it can help address issues such as human error, data privacy, security, and safety. Research regarding blockchain technology for cloud storage systems has been carried out extensively throughout the world (Tang et al., 2018; Deng et al., 2019; Sharma et al., 2020). However, implementing cloud storage systems adopting blockchain technology in the government sector is remains limited. Therefore, this study attempts to develop a model of the blockchain-based cloud storage system by identifying first the dominant risk factors from the implementation of the cloud storage system in the government agencies, which potentially impact their organizational performance, by taking into account a non-structural government agency in Indonesia as the case study. The findings of this study are expected to contribute insight for policymakers, practitioners, and researchers regarding the adoption of the blockchain mechanism in data storage systems to improve government agencies' organizational performance.

2. Methods

To achieve its objectives, this study was conducted in two stages: first, identifying the dominant risk factors of cloud data storage systems implementation affecting the organizational performance of government agencies, followed by developing the model for the blockchain-based cloud data storage system. A literature review, questionnaire surveys, and expert interviews were conducted in the first stage, while a benchmark study, case study, and expert validation were performed in the second stage.

This study used secondary data sources from previous studies obtained during the literature review process arranged using the ISO/ICE 270001 information security

management systems (ISMS) standard to identify the risks as the variables for the questionnaire, as summarized in Table 1.

Table 1 Risk variable on the implementation of cloud storage system

Aspect	Risks	References
Confidentiality	Data leakage	(Kanade et al., 2015; Selvanathan and Poravi, 2018)
	Theft and data breaches	(Vurukonda and Rao, 2016)
Integrity	Data change or modification	(Vurukonda and Rao, 2016)
	Data corruption caused by virus attacks	(Hussain et al., 2017)
	Unsynchronized uploaded data	(Senthil et al., 2019)
Availability	Internet connection is needed to access data	(Vyas and Modi, 2017)
	Data can only be accessed inside of the local server connection	(Vyas and Modi, 2017)
	Limited storage space	(Vyas and Modi, 2017)
	Data loss caused by system damage	(Vurukonda and Rao, 2016)
Privacy	Unauthorized users can access data	(Selvanathan and Poravi, 2018)
	Data are used for other purposes not in accordance with the organization's objectives	(Selvanathan and Poravi, 2018)
Identification	Data can be accessed without particular access rights (username and password)	(Feng and Chen, 2013)
	Unable to identify the responsible party in case of a data breach	(Feng and Chen, 2013)
Authentication	The system has no user authentication protocol	(Feng and Chen, 2013)
Authorization	The system runs without authorization for the user to access, change, or delete data.	(Vurukonda and Rao, 2016)
	Loss of data due to deletion by unauthorized users	(Vurukonda and Rao, 2016)
Accountability	Unawareness of data changes	(Singh and Lee, 2018)
	The system does not provide data regarding all performed activities and who has carried out these activities.	(Ko, 2014)
	Cannot perform the same data change activities simultaneously	(Feng and Chen, 2013)
Non-Repudiation	No party is responsible for data changes	(Singh and Lee, 2018)
	Cannot pinpoint the error to other users	(Feng and Chen, 2013)
Reliability	Lack of guarantee from the system when a security threat occurs	(Feng and Chen, 2013)

The questionnaires were then administered to the Data and Information Bureau employees of a non-structural government agency investigated as a case study in this research. Although the number of employees in the Bureau was minimal, a total of 20 questionnaire surveys was collected out of 23 questionnaires sent, representing an 86.96% response rate. A more than 30%–40% response rate indicates that the analyzed data were not bias (Moser and Kalton, 2017). The respondents who filled out the questionnaires had the requisite work experience of four to more than 20 years.

The obtained variables were used to identify the dominant risk factors of using cloud storage systems that affect the agency's organizational performance through the quality of the services delivered and included coordination with related agencies, data and information provision, meeting materials and documentation, and report preparation.

The statistical package for social sciences (SPSS) program was used as the primary tool to analyze the correlation and multiple regression relationships of the questionnaire data. These analyses were done to get the coefficients of the independent variables and the influence magnitude on the dependent variables. The correlation coefficient obtained from Spearman rank correlation analysis (Mukaka, 2012) was utilized to measure the

relationship between the risk factors and the agency's organizational performance indicated by the stakeholders' satisfaction. The statistical analysis then produced significance testing (p-value) as the coefficient correlation value (Madyaningarum et al., 2018).

The cloud data storage system, as the existing storage system currently implemented in the investigated government agency, has several issues that can impact the organizational performance of an agency (Ali et al., 2018; Al Mudawi et al., 2020). The hypothesis is developed based on the effect of risks in using cloud storage systems on the government agencies' organizational performance, as follows:

H_1: There is an effect of risks in cloud data storage systems on the agency's organizational performance

The frequency of occurrence and the magnitude of identified dominant risk factors were determined using risk analysis that was employed in the questionnaire surveys given to the same 20 respondents responding to the previous questionnaire survey. The risk management framework from Project Management Body of Knowledge (PMBOK) was used to determine the risk level by multiplying the frequency and impact of the identified risk factors (Hatmoko et al., 2021). The results were then used to reduce the number of variables taken from the group of risk variables with a significant and high-risk level index. The variables that underwent validity and reliability tests were used as the input for the risk ranking analysis. Furthermore, the average value of the impact and the frequency of risk were multiplied to obtain the risk value. The weighting for risk frequency and risk impact can be seen in Tables 2 and 3. The classification system shown in Table 4 was used to rank the risk values.

Table 2 Frequency weightings (PMBOK, 2017)

Value	Criteria of Frequency	Weight
1	Very low	0.10
2	Low	0.03
3	Moderate	0.50
4	High	0.70
5	Very high	0.90

Table 3 Impact weightings (PMBOK, 2017)

Value	Criteria of Impact	Weight
1	Minimal	0.05
2	Minor	0.10
3	Moderate	0.20
4	Major	0.40
5	Massive	0.80

Table 4 Classification of risk level (PMBOK, 2017)

Risk Level	Justification	Score
High	The main action immediately; measurements from senior management or risk transfer to other party is needed.	0.21-0.72
Medium	Particular action is needed; additional measurement with pattern risk criteria from the management is needed.	0.08-0.20
Low	The measurement from the management is needed by applying appropriate security controls.	0.01-0.07

A benchmarking study to previous research discussing the blockchain-based storage systems was performed in the second stage to develop the conceptual model for a cloud

data storage system that considers blockchain technology. Lastly, in-depth interviews with experts were conducted to strengthen and validate the research outputs by asking about the risk factors and the developed model of blockchain-based cloud storage. Three experts interviewed in this study met the set criteria of having more than 5 years of experience in using the cloud data storage systems. Expert 1 and Expert 2 have 20 years and 14 years of work experience in information systems, respectively, and they both hold a masters' degree, while Expert 3 has 10 years of work experience and holds a bachelor's degree.

3. Results and Discussion

3.1. Dominant Risk Factors Identification

The questionnaire surveys utilized to derive the dominant factors used an ordinal scale ranging from 1 to 5, where 1 indicates that the factor bears no influence, while 5 represents the factor being very influential to the organizational performance of the government agency. The strength and direction of the relationship will be valued if the correlation between these variables is significant. The significance level of the influence of variables can be seen from the value of sig. (2-tailed) from the calculation using the SPSS program, then the relationship between the variables is not significant. Table 5 below summarizes the correlations of the independent variables.

Table 5 The interpretation of correlation size

	Risk Variables	Correlation Coefficient	Sig.(2-tailed)	Result
X1	Data leakage	-0.419	0.066	Weak
X2	Theft and data breaches	-0.515	0.020	Moderate
X3	Data change or modification	-0.402	0.079	Weak
X4	Data corruption caused by virus attacks	-0.515	0.020	Moderate
X5	Unsynchronized uploaded data	-0.487	0.029	Weak
X6	Internet connection is needed to access data	-0.403	0.078	Weak
X7	Data can only be accessed inside of the local server connection	-0.384	0.094	Weak
X8	Limited storage space	-0.617	0.004	Moderate
X9	Data loss caused by system damage	-0.515	0.020	Moderate
X10	Unauthorized users can access data	-0.512	0.021	Moderate
X11	Data are used for other purposes not in accordance with the organization's objectives	-0.634	0.003	Moderate
X12	Data can be accessed without particular access rights (username and password)	-0.674	0.001	Moderate
X13	Unable to identify the responsible party in case of a data breach	-0.512	0.021	Moderate
X14	The system has no user authentication protocol	-0.292	0.211	Weak
X15	The system runs without authorization for the user to access, change, or delete data.	-0.503	0.024	Weak
X16	Loss of data due to deletion by unauthorized users	-0.739	0.000	Moderate
X17	Unawareness of data changes	-0.428	0.060	Weak
X18	The system does not provide data regarding all performed activities and who has carried out these activities.	-0.612	0.004	Moderate
X19	Cannot perform the same data change activities simultaneously	-0.098	0.680	Very weak
X20	No party is responsible for data changes	-0.450	0.046	Weak
X21	Cannot pinpoint the error to other users	-0.394	0.085	Weak
X22	Lack of guarantee from the system when a security threat occurs	-0.524	0.018	Moderate

The Sig. (2-tailed) values showed that 14 out of 22 independent variables correlated with the dependent variable. Since the number of respondents was only 20, to obtain a Kaiser Meyer Olkin (KMO) value > 0.5 that is requisite for the adequacy of factor analysis, therefore, risk factors with the highest correlation coefficient analyzed further were X2, X4, X8, X9, X10, X11, X12, X13, X16, X18, and X22.

Regression analysis was then conducted to see the impact of the risk factors on the agency's performance. The regression analysis performed on dominant variables revealed that $t_{count} > t_{table}$, which means H_0 is rejected and H_1 is accepted. The t_{count} was |-3,355| and the degree of freedom (df) = N-1-1 = 20-1-1= 18; therefore, the r_{table} is 2,101. With $t_{count} > t_{table,}$ it can be concluded that there is a risk effect of using cloud data storage systems on government agency organizational performance.

3.2. Risk Analysis

The questionnaire results were then analyzed to determine the frequency and impact of each risk variable, with Table 4 as the guideline to determine the risk level. The risk analysis results can be seen in Table 6.

Table 6 The interpretation of correlation size

Variable	Average Frequency (F)	Average Impact (D)	Risk (FxD)	Risk Level	Rank
X2	0.53	0.45	0.257	high	8
X4	0.62	0.64	0.397	high	2
X8	0.70	0.58	0.406	high	1
X9	0.56	0.58	0.325	high	3
X10	0.57	0.37	0.209	high	10
X11	0.52	0.56	0.291	high	6
X12	0.52	0.37	0.192	high	11
X13	0.56	0.39	0.216	high	9
X16	0.55	0.56	0.308	high	5
X18	0.58	0.54	0.313	high	4
X22	0.58	0.45	0.261	high	7

The selection of the dominant risks in this study utilized a risk rating based on the correlation analysis done previously. These risk variables had to pass the statistical tests that were carried out. Moreover, risk analysis results were then brought to experts for validation. Interviews showed that 66.7% of the experts disagreed with X10, X11, X13, X15, X16, and X18 variables, arguing that they were nonsignificant. Therefore, the six dominant risk factors with the highest rankings included theft and data breaches, data corruption caused by virus attacks, limited storage space, data loss caused by system damage, data being accessed without particular access rights, and lack of guarantees from the system when a security threat occurs.

3.3. Blockchain-based Cloud Storage System Model Development

With its distributed characteristics, blockchain can be an alternative solution to solving problems in implementing cloud data storage systems. In designing the model for a blockchain-based cloud data storage system suitable for implementation in government agencies, it is necessary to know the needs of the data storage system required and its effect on the organizational performance of the agencies.

First, the blockchain type was chosen based on the data storage system requirements for the investigated government agency. Based on the need for the data storage system, the suitable blockchain type was the private blockchain, since it can be used as a platform to store confidential data. The government agency can manage data with three classifications, including: (1) confidential; (2) limited; and (3) temporary, distinguishing the treatment of

data security and restrictions on data access. Temporary data such as the discussion material and document drafts are deleted once they have been updated. Moreover, unknown users cannot access the data storage.

In this case study, three types of data were entered into the blockchain network, including confidential data, limited data, and temporary data (materials for meetings). Furthermore, there are five entities from the government agency that should be accommodated in the blockchain network, namely: (1) the chairperson of the agency; (2) secretary of the agency; (3) Data and Information Bureau personnel; (4) division heads; and (5) secretary to the division heads. Each entity that acts as a node in this private blockchain network is locked based on the restrictions on access rights to data assets and transactions. Thus, data can only be accessed by nodes in accordance with the specified authority. Only the chairperson node and secretary node have the right to access confidential data. However, all nodes can access the limited data.

The data in a blockchain network is immutable, unchangeable, and cannot be deleted without mutual consensus; hence, it can help the agency maintain data integrity. Moreover, from a security perspective, data stored in the blockchain cannot be manipulated since it is encrypted and stored in multiple databases. The availability of data in the blockchain can also be guaranteed since each node has data replication. When data in one of the entities' storages is damaged, the rest of the data remains safe; hence, it is less likely to lose data due to system damage. In addition, access rights to data are also divided according to their authorized access to create, read, modify, and delete data.

The existing data storage system at the agency is a centralized system placed on a local server, where only the computers in the Data and Information Bureau are connected to a cloud computing-based data storage system. Since the rest of the involved entities are not connected, they must ask the data owners whenever they need it. In addition to time inefficiency, the process of data transferring is also risky due to the lack of security guarantee. Furthermore, with this unconnected storage system, the data cannot be updated in real time. The diagram of the existing cloud storage system is illustrated in Figure 1.

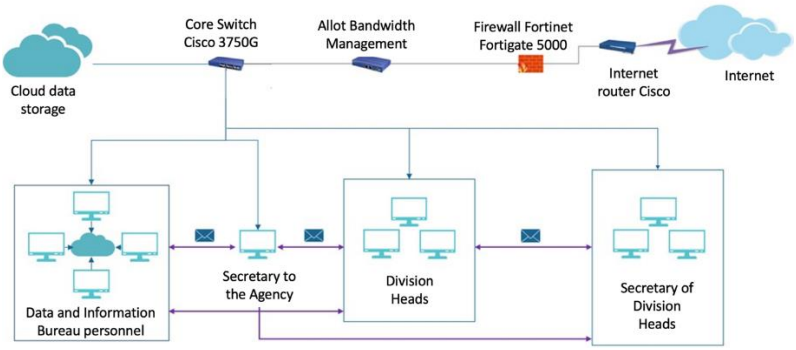

Figure 1 Existing cloud data storage system

After conducting a benchmarking study from previous research (Vyas and Modi, 2017; Tang et al., 2018; Deng et al., 2019), the conceptual blockchain-based cloud storage model was developed. In this private blockchain network, each entity illustrated in the nodes is locked according to restrictions on access rights to data assets and transactions. Thus, data can only be accessed based on the level of authority, where limited data can be accessed by all nodes, while confidential data can only be accessed by particular entities. Figure 2 illustrates the data transactions in the proposed blockchain-based cloud storage system model.

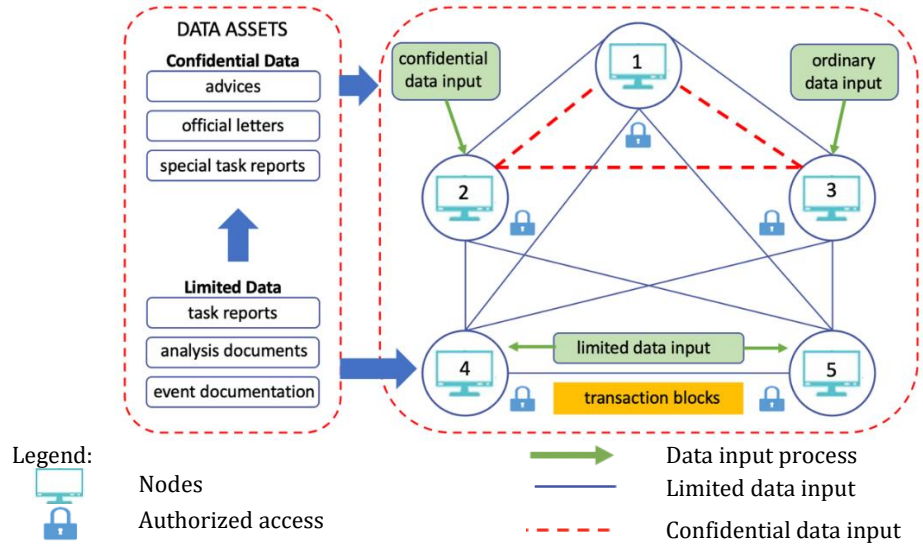

Figure 2 Data transaction in the proposed blockchain-based cloud storage system model

Blockchain mechanism implementation can improve business processes since some processes can be eliminated, such as transfer data processes implemented by unconnected entities. Furthermore, data updated in real time also reduces the processing time. Therefore, when compared to conventional processes using existing cloud data storage systems, adopting blockchain will improve the performance of government agencies in terms of time reduction. Based on the case study and interviews with experts, the proposed model can reduce time for a process of compiling report from an 11 to 4-day process, the comparison for data security aspects and the time performance for compiling a report data in the investigated government agency can be seen in Table 7. This finding is in line with Ølnes et al. (2017), who stated that blockchain technology can increase the efficiency of transaction mechanisms.

Table 7 Security aspects and processing time to compile data on the storage systems

No.	Data Storage System	Security aspects			Processing Time
		Data confidentiality	Data integrity	Data availability	
1.	Cloud storage	Not secured due to no settings for access permission	Low data validity because unauthorized users can modify it	Data is not available on every entity	11 days
2.	Blockchain-based cloud storage	Secured since the system has access right settings	High data validity since data cannot be modified without consensus	Data is always available on every entity	Four days

4. Conclusions

Cloud storage systems used in government agencies to store confidential documents are usually associated with data security, integrity, and availability. Therefore, this study attempted to identify the dominant risk factors in implementing the cloud storage system that affects the government agency's organizational performance, in aiming to develop a framework for a cloud storage system mode that considers blockchain technology.

The development of the blockchain-based cloud storage system model was influenced by six dominant risk factors: theft and data breaches, data corruption caused by virus attacks, limited storage space, data loss caused by system damage, data being accessed without particular access rights, and lack of guarantees from the system when a security threat occurs. It can help improve the government agency's organizational performance by

providing a more efficient data delivery process. The proposed model only needs 4 days to complete a data compilation report in the case study agency compared to the conventional cloud storage system, which required 11 days. This study suggests future research is required to further develop the technical aspects of a blockchain-based storage system that can be implemented for all government agencies.

Acknowledgements

The authors would like to thank the Ministry of Research and Technology, Republic of Indonesia, for the support given to this research.

References

Abd Al Ghaffar, H.-A.N., 2020. Government Cloud Computing and National Security. *Review of Economics and Political Science,* pp. 2631–3561

Al Mudawi, N., Beloff, N., White, M., 2020. Issues and Challenges: Cloud Computing e-Government in Developing Countries. *International Journal of Advanced Computer Science and Applications*, Volume 11(4), pp. 7–11

Ali, K.E., Mazen, S.A., Hassanein, E.E., 2018. A Proposed Hybrid Model for Adopting Cloud Computing in e-Government. *Future Computing and Informatics Journal*, Volume 3(2), pp. 286–295

Alketbi, A., Nasir, Q., Talib, M.A., 2018. Blockchain for Government Services-Use Cases, Security Benefits and Challenges. *In:* 2018 15th Learning and Technology Conference (L&T), pp. 112–119, Jeddah, Saudi Arabia

Berawi, M.A., Radjilun, M.K.Z., Sari, M., 2020. Developing Blockchain-Based Crowdfunding Model for Property Investment. *In:* Second International Scientific Conference, SPBPU IDE 2020, St. Petersburg, Russia, October 22–23, 2020

Cai, C.W., 2018. Disruption of Financial Intermediation by FinTech: A Review on Crowdfunding and Blockchain. *Accounting and Finance*, Volume 58(4), pp. 965–992

Deng, Z., Ren, Y., Liu, Y., Yin, X., Shen, Z., Kim, H. J., 2019. Blockchain-Based Trusted Electronic Records Preservation in Cloud Storage. *Computers, Materials and Continua*, Volume 58(1), pp. 135–151

Feng, J., Chen, Y., 2013. A Fair Non-Repudiation Framework for Data Integrity in Cloud Storage Services. *International Journal of Cloud Computing*, Volume 2(1), pp. 20–43

Hatmoko, J.U.D., Astuti, P.K., Farania, S.N., 2021. Insuring Project Risks: Contractor Expectations versus Insurance Company Policies. *International Journal of Technology*, Volume 12(1), pp. 90–100

Hill, J.F., 2014. The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders. *In:* The Hague Institute for Global Justice, Conference on the Future of Cyber Governance

Hussain, S.A., Fatima, M., Saeed, A., Raza, I., Shahzad, R.K., 2017. Multilevel Classification of Security Concerns in Cloud Computing. *Applied Computing and Informatics*, Volume 13(1), pp. 57–65

Irion, K., 2013. Government Cloud Computing and National Data Sovereignty. *Policy and Internet*, Volume 4(3–4), pp. 40–71

Kanade, M., Mule, M., Shuaib, M., 2015. Improving Cloud Security using Data Partitioning and Encryption Technique. *International Journal of Engineering Research and General Science*, Volume 3(1), pp. 1245–1252

Khin, S., Ho, T.C.F., 2019. Digital Technology, Digital Capability and Organizational Performance: A Mediating Role of Digital Innovation. *International Journal of Innovation Science*, Volume 11(2), pp. 177–195

Ko, R.K.L., 2014. *Data accountability in cloud systems*. Security, privacy and trust in cloud systems. Edited by Surya Nepal and Mukaddim Pathan. Heidelberg, Germany, Springer

Lnenicka, M., Komarkova, J., 2019. Developing a Government Enterprise Architecture Framework to Support the Requirements of Big and Open Linked Data with the Use of Cloud Computing. *International Journal of Information Management*, Volume 46, pp. 124–141

Madyaningarum, N., Berawi, M.A., Miraj, P., 2018. Relationship between Leadership and Commitment with Quality Performance on U-Th-REE Processing Pilot Plant Construction in BATAN. *Eksplorium*, Volume 39(1), pp. 59–66

Moser, C.A., Kalton, G., 2017. *Survey Methods in Social Investigation (Second).* Aldershot: Dartmouth Publishing Company Ltd

Mukaka, M.M., 2012. A Guide to Appropriate Use of Correlation Coefficient in Medical Research. *Malawi Medical Journal*, Volume 24(3), pp. 69–71

Natesan, G., Chokkalingam, A., 2019. Optimal Task Scheduling in the Cloud Environment using a Mean Grey Wolf Optimization Algorithm. *International Journal of Technology*, Volume 10(1), pp. 126–136

Ølnes, S., Ubacht, J., Janssen, M., 2017. Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing. *Government Information Quarterly*, Volume 34(3), pp. 355–364

PMBOK., 2017. *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*. Pennsylvania: Project Management Institute, Inc

Rajalakshmi, A., Lakshmy, K.V, Sindhu, M., Amritha, P.P., 2018. A Blockchain and IPFS Based Framework for Secure Research Record Keeping. *International Journal of Pure and Applied Mathematics*, Volume 119(15), pp. 1437–1442

Razzaq, A., Khan, M.M., Talib, R., Butt, A.D., Hanif, N., Afzal, S., Raouf, M.R., 2019. Use of Blockchain in Governance: A Systematic Literature Review. *International Journal of Advanced Computer Science and Applications*, Volume 10(5), pp. 685–691

Selvanathan, N., Poravi, G., 2018. Comparative Study on Decentralized Cloud Collaboration (DCC). *In*: The 3rd International Conference for Convergence in Technology, Pune, India

Senthil, S., Kamalakannan, T., Shanthi, C., Radhakrishnan, D., 2019. Study on Cloud Storage and its Issues in Cloud Computing. *International Journal of Management, Technology and Engineering*, Volume 9(1), pp. 976–981

Sharma, P., Jindal, R., Borah, M.D., 2020. Blockchain Technology for Cloud Storage: A Systematic Literature Review. *ACM Computing Surveys*, Volume 53(4), pp. 1–32

Singh, I., Lee, S.W., 2018. Comparative Requirements Analysis for the Feasibility of Blockchain for Secure Cloud. *Communications in Computer and Information Science*, Volume 809, pp. 57–72

Tang, Y., Zou, Q., Chen, J., Li, K., Kamhoua, C.A., Kwiat, K., Njilla, L., 2018. ChainFS: Blockchain-Secured Cloud Storage. *In:* IEEE International Conference on Cloud Computing, CLOUD, 2018-July, CA, USA

Vurukonda, N., Rao, B.T., 2016. A Study on Data Storage Security Issues in Cloud Computing. *Procedia Computer Science*, Volume 92, pp. 128–135

Vyas, J., Modi, P., 2017. Providing Confidentiality and Integrity on Data Stored in Cloud Storage by Hash and Meta-data Approach. *International Journal of Advance Research in Engineering*, Volume 4(5), pp. 38–50

Whitman, M.E., Mattord, H.J., 2018. *Principles of Information Security*. Cengage Learning

Wong, T.S., Chan, G.Y., Chua, F.F., 2019. Preventing and Rectifying Cloud Quality of Service Violation through Adaptive Resource Scaling and Replication. *International Journal of Technology*, Volume 10(7), pp. 1395–1406