Blockchain Technology for Addressing Privacy and Security Issues in Cloud Computing

Pardis Moslemzadeh Tehrani[1], Gabriele Kotsis[2] and Andasmara Rizky Pranata[1]
[1]Faculty of Law, University of Malaya, Kuala Lumpur, Malaysia
[2]Head of the Telecooperation Department, Johannes Kepler Universität, Linz, Austria
pardismoslemzadeh@um.edu.my
Gabriele.kotsis@jku.at
andasmararizky@gmail.com

Abstract: Blockchain technology is a recent and important financial technology that has completely transformed business transactions. The adoption of cloud computing in all IT environments due to its efficiency and availability has increased dramatically. Despite attempts to address privacy and security issues, confusion remains in the cloud environment. It is said that blockchains are a promising solution for many distributed applications and have the potential to overcome issues pertaining to the centralized system. The decentralized nature of blockchains provides a new forms of distributed software architectures where users can reach agreement consensually on the shared system without relying on a central integration point. Nonetheless, there are some challenges which need to be evaluated. Accordingly, this study explores how blockchains can curb cloud computing issues from both legal and technical aspects. This article presents the use of blockchain in current cloud storage applications and discusses how blockchain technology can be used to resolve security and privacy challenges. The use of blockchains as a solution for each issue will be proposed by explaining how they can overcome the shortcomings of cloud computing.

Keywords: Blockchain, Cloud Computing, Privacy, Security, Contractual Terms

1. Introduction

Cloud computing has been entrenched in our society due to its various advantages such as the storing of large amounts of data, accessibility, performance of intensive computational operations, etc. It represents an everything-as-a-service business model offering outsourcing services in an economic, scalable and flexible manner that is affordable and attractive to small businesses and individual consumers. Two important types of outsourcing services in cloud namely, storage and computation are widely available for users; however, data security and privacy issues remain of primary concern in the use of outsourcing services. (Zhang & Deng 2018)

The rapid development of cloud computing has raised many concerns over its usage due to the amount of risk or uncertainty inherently embedded in the layers of the protection in cloud storage. As the cloud deals with information that may involve all aspects of personal life tight security needs to be in place to protect individual privacy. Specific requirements on personal protection created by new regulations - particularly General Data Protection Regulation (GDPR) - challenge the effectiveness of the centralized computing model available on public cloud infrastructures. (Stanciu 2017)

The information being collected on an unprecedented scale and big data analysis in this big data era, led to a burgeoning demand for processing big data in a secure way with low cost and high efficiency. Cloud computing services have thus emerged and became popular for big data processing. Various and flexible approaches are offered by cloud service providers to data owners for managing their data sets that are stored remotely in the cloud. However, by nature, cloud storage is not secure. (Liu 2017) They are highly centralized architectures which suffer various technical limitations such as from cyber-attacks and single point of failure. In cloud computing, the data is stored in a centralized AI application which may lead to the possibility of data tampering and breaches as data can be subject to hacking and manipulation due to it being managed and stored in a centralized manner. (Salah et al. 2019)

According to Mungwe (2017), “The two main issues that exist with security and privacy aspects of cloud computing includes loss of control over data and total dependence on the cloud computing provider. (Mungwe 2017) The Council of European Professional Informatics Societies (CEPIS) explains these two issues more clearly: (Hölbl 2017) “First, the data could be compromised by the cloud service provider (CSP) as there are limited ways to confirm the data transparency inside of the CSP. After all, some clouds have functions that enable CSP to take a sneak peek at the data stored in their server. Second, the connection between the server and the user may not be protected, hence no guarantee that all attempt at cybercrime will be repelled. Finally, it will be hard to

delete data permanently. It means that there is no guarantee that the master data that is deleted at the server is totally deleted, or even the master data anymore". CEPIS then notes that "the age of a 'Guaranteed complete deletion of data', if it ever existed, has passed." Typically, cloud users have no control over the cloud storage servers being used, thus giving rise to risks such as data confidentiality, integrity, availability, privacy, cybersecurity, energy consumption, and scalability. (Maroufi et al. 2019)

On the other hand, blockchain is a type of distributed electronic database, a ledger, which can hold any information (e.g., user data records, critical events information, banking transactions or device service history) and sets rules on how this information can be updated. Blockchain technology is used to organize a market network where users can monetize their computing power, applications, and datasets. (Bonhomme et al. 2020). It provides on-demand access to cloud computing resources to support compute-intensive applications in fields such as AI, big data, healthcare, rendering, or FinTech. Transactions in blockchains via a distributed ledger are verified by the consensus of a majority spread throughout the blockchain network. It allows non-trusting members to interact with each other without an intermediary as well as enable all participants to have their own copy of the ledger. Any minimal changes to the ledger will be reflected in all copies.

Despite attempts to address privacy and security issues, confusion remains in the cloud environment. (Tehrani et al 2017) It is said that blockchains are a promising solution for many distributed applications and have the potential to overcome issues pertaining to the centralized system. Nonetheless, there are some challenges which need to be evaluated. Accordingly, this study explores how blockchains can curb cloud computing issues from both legal and technical aspects. This article presents the use of blockchain in current cloud storage applications and discusses how blockchain technology can be used to resolve security and privacy challenges. The first part discusses the main privacy concerns of cloud computing in general and how blockchains provide a solution to those concerns. It then identifies other issues that derive from privacy concerns. The use of blockchains as a solution for each issue will be proposed by explaining how they can overcome the shortcomings of cloud computing.

2. Legal Issues Relating to Privacy and Security in Cloud Computing

Data privacy is a major issue in this era of networking system where many users share the same physical storage facilities. Cloud computing is normally used by many networking applications such as IoT, healthcare and smart grids to process and store massively large amounts of data. In fact, a critical requirement for most of these applications that are involved with personal information is privacy. However, the use of multiple clouds and internetworking among them has intensified the issue of privacy of the data. Under a privacy service the user has the right to control and set rules for the data and resources accessed by the network. The data and resource owner can control disclosure of their information, and this is generally done by enabling users to define their access control list (ACL). The following section discusses the challenges currently faced in providing privacy services in cloud storage.

Privacy and security are major issues in cloud applications that do not as yet have industry-wide solutions. The absence of cloud computing standards points to the need for common cloud security, data privacy and ownership policies due to the different approaches taken by service providers. As mentioned previously, cloud providers aim to ensure compliance with the laws and regulations governing the use of the internet by including policies protecting end users. The GDPR, for instance, accords the utmost importance to privacy and end users' data especially when it comes to sensitive information that may affect personal reputations. (Akbar 2018)

A major issue in this respect is the relationship between service providers and end users. Contrary to the common belief that data stored in the cloud belongs to the service provider, it should be remembered that it is still owned by the end user although the provider may own the software. Thus, it is understood that service providers should relinquish power to end users under the terms of the contract since the latter have no other option except to use the cloud due to its convenience and ubiquitous nature. One of the main grievances of end-users is the disowning of liability by cloud providers through the use of a clickwrap agreement. Such a contract in cloud computing upsets the balance between the parties to the agreement. The clickwrap agreement includes terms and conditions which are often unread or overlooked by end users when agreeing to the contract as it is provided separately from the acceptance page.

Another related issue is the presence of internal and external attackers in cloud storage infrastructures. (Privacy in Cloud Computing 2012) Internal attackers are those employed by the cloud service provider, customer, or other third-party provider organization supporting the operations of a cloud service. They have the opportunity to gain further access or support any third party in executing attacks against the confidentiality, integrity and availability of information within the cloud service. (TagElsir et al. 2015) They are deemed attackers as they can access the end user's personal data for their own benefit or profit. Most service providers scan the personal data of their customers in order to place targeted ads based on the information in the data. Moreover, more complex, data and statistics are recorded, bundled and analysed (data mining) for user profile marketing as a means to anticipate future purchases by users. The government is also considered an attacker of personal data. Users need to provide personal information which then enables the government to have massive amounts of personal data that should not be made public. Here, individuals have little or no control over storage and access to their information and this place the privacy of their data at risk. (Salman et al. 2019)

Various articles have discussed how technology size or privacy laws can help check the excessive influence of governments. (Adrian 2013) In Microsoft Corp v United States, (Microsoft Corp. v. United States 2016) the court held that the government cannot compel internet service providers to turn over stored data without a warrant. This is to prevent any unwarranted interception that deviates from grounds of national security. In fact, the court did not address the issue of whether the data resides in a particular country, and it was limited to extra-territorial requirements. Furthermore, in the interest of national security such as in combatting terrorism, governments have extensive legal avenues to access private information stored in the cloud. Essentially, cloud providers might be located in a different country from users which could lead to privacy issues if the cloud computing contract did not provide additional terms stating the level of protection and method of handling the data. (OECD 2014).

Another possible cause leading to a breach in privacy is the leakage in the cloud computing process in regard to the agreement between the processor and sub processor. Where the processor's job is delegated to a sub processor there is major concern over the status of the cloud provider as to whether it rests with the data controller or the data processor. Many providers have chosen to disavow being bound by liabilities that they should carry according to the role they play. Thus, users are the ones who normally bear the consequences if the processor and sub processor did not have a proper contract between themselves. It is important to determine whether a party is controller or processor when processing personal data, as under GDPR both have distinct obligations. (Salmon et al. 2019)

One who uploads data to a cloud computing environment is a controller under a cloud computing system while the operator is the processor. This is a key area in which blockchain and cloud systems differ. As many blockchain systems are operated by all users in a peer-to-peer network environment, it is difficult to define whether users are controllers or processors. It is necessary to consider the extent to which the different participants in the blockchain network are controllers based on their respective activities. Normally, participants who submit personal data to a blockchain are more likely count as controller based according to the GDPR since they determine the details of processing. The nodes, on the other hand, are more likely to be processors as they simply facilitate the blockchain network's operations by merely processing personal data. However, as not all blockchain systems operate in the same way, and there can be different types of participants carrying out various activities, this determination is not definitive and precise. As a representative technology on the anonymity aspect, blockchains can be upgraded to a convenient service that provides stronger security if combined with cloud storage.

2.1 Blockchain as a solution for privacy services

Blockchain technology can resolve some of the issues discussed in the previous section by providing decentralized end-to-end data privacy guarantees. In doing so, it can provide data ownership solutions and dynamically change access rights when required. An ideal blockchain-based data privacy system allows the owner to define the desired ACL through a smart contract that will publish the ACL and the data as blockchain transactions. Thus, many platforms such as Facebook or Google will not own the data as in the past. Instead, they will be a part of the blockchain network, processing data only when the ACL allows them via a permission-less blockchain where policies defining the data access are either based on smart or on data management messages. (Salmon et al. 2019)

Blockchains can be used in different settings to provide privacy services. Salman et al. (2019) investigated six approaches that utilize blockchain technology to assess the privacy service. Four of the six approaches used the blockchain platform. Blockchain-based Data Sharing (BBDS) provides privacy for medical records in a cloud environment. It is helpful in lightweight communication systems including user layer, management layer and storage layer. BBDS fulfils the health care records requirement by simplifying the transaction and block header. The system's interactions are secured by identity-based authentication and encryption techniques. This system is implemented in permissioned blockchain. Another proposed approach implemented for a specific IoT use case is the dynamic fair access for IoT. This system lets users register their new resources and define their access policies through a smart contract associated with these resources. A request for a resource made from user A to user B is directed to a blockchain network. Based on the smart contracts resource, the blockchain denies or grants access and sends feedback to the requester who can update their access based on the feedback. Although this approach has been implemented and confirmed for Bitcoin, indicating its feasibility in providing the right access control list management, drawbacks include its lack of real time support, complexity of the blockchain and inflexible implementation.

2.1.1 Loss of control over data due to unauthorized access

Despite the extensive efforts by experts around the globe, issues relating to the security and privacy of the cloud model remain unresolved. Resolving these issues is critical in order to provide viable options to cloud users while gaining the confidence of end users. Unauthorized access to confidential information is the main security and privacy risk in cloud computing. Such unauthorized access can be gained by both internal and external hackers due to the loss of control over the stored data. It may occur with a third-party auditor which is expected to behave in a responsible manner though, in practice, this may not always be the case. (Liu et al. 2017) The loss of control of data is not the only threat arising from unauthorized access, it also impacts control over the data's lifecycle. Data users need assurance that their data is completely removed from the cloud when it is erased - if there a copy of erased data exists, then the act of erasing would be redundant. Such a scenario indicates that data users have no control over the lifecycle of data as more data will be completely erased only when data users change the service provider. (Pearson & Benameur 2010)

2.2 Blockchain as a solution for unauthorized access

One of main feature of blockchain is data anonymity. Blockchain is beginning to address access-control challenges and data confidentiality by providing complete out-of-the-box block data encryption and AAA capabilities. Full encryption of blockchain data ensures that it will not be accessible to unauthorized parties while the data is in transit (especially if data flows through untrusted networks). (Piscini, Dalton, & Kehoe 2017) In blockchain, each user only manages its own keys. Blockchain enhances security by maintaining two distinct ledgers, namely those with individually encrypted data and a transaction ledger which stores encryption access keys to the related data. Each access to the data could be restricted to a certain number of attempts and will be recorded and stored. In other words, if a third party needs to access the data, permission is required to access only specific document at specific times. (Lis and Mendel 2019)

2.2.1 Cross border data transfer

Although cloud computing is a centralized setting, it does not necessarily mean that data are physically stored in a single place. Normally, multiple service provider may participate in delivery of the service (Gai, Raymond, Zhu & 2018) in which the data is transferred between cloud service providers. In fact, such a situation is not ideal since the information that the cloud deals with relates to the personal and sensitive data of users and thus raising concerns over their privacy and security. It also increases the risk of cyber-attack by individuals, organized criminals or governments and opens the door for illegal copying of data as there is no transparency in the cloud regarding the act of transfer. Thus, adequate protection is necessary to protect end users' personal and sensitive data. Different countries have different approaches to protecting the privacy of personal and sensitive data. The new GDPR seeks to resolve the abovementioned issues though problems still persist as illustrated in the following discussion. (Tehrani et al 2018).

2.3 Blockchain as a solution for the issue of data transfer

As explained earlier, blockchains employ a decentralized system as opposed to the cloud's centralized system. Blockchains work by directly transferring data, peer to peer (P2P), without any third party regulating the process. This also means that applicable laws in blockchains will be determined based on the stipulations of the contract since the blockchain is located on a decentralized ledger in a network of many computers instead of in a single server. In terms of ambiguity of the place of formation of the smart contract, courts will need to determine a

method for locating the smart contract's place of formation. One might say that in case of malfunction or unpredictable results, no party can be sued owing to the distributed ledger across a large network, and that no central authority can be held accountable for any failure of the agreement. However, the operator of the blockchain could be held accountable if the malfunction is traceable to their action and in determining jurisdiction and choice of law.

2.3.1 Contractual issues

To ensure compliance of users in cloud services, service providers usually require user candidates to "sign" or consent to an agreement prepared by the provider called a clickwrap agreement. A clickwrap agreement is a contract that appears upon or before accessing a certain computer software or online purchase. It is meant to be a legally binding contract between the two parties and is usually signed by checking an "I agree" box or something similar. (Johansson 2014) The agreement contains information of anything that is important for the user to understand and with terms of use of the application or online purchase. As explained in the following section, while the service provider endeavours to comply with GDPR, (Mackie 2020) it does not mean that there are no issues in the process. Clickwrap agreements are more often seen as a way for service providers to comply with the regulation. However, it lacks any actual "agreement" value on the service user as they compel users to accept the contents of the agreement or not use the service. Users often have a minimal understanding of the terms of the agreement. In most cases, they will just agree on the click wrap agreement without actually reading the whole agreement, making them liable for risks that they are not fully aware of.

2.4 Smart contracts in blockchains

The recent innovation of blockchain technology has gone beyond digital currency applications. One of the most notable functions in the system is the smart contract. A smart contract is a feature that will automatically execute a contract in the blockchain agreed to beforehand, thus eliminating the possibility of deception or fraud after the agreement is concluded. Smart contracts save money and provide autonomy, trust, backup, safety, and accuracy to blockchains. They now provide a mechanism to store, evaluate, and update policies on the blockchain thereby creating new opportunities for people to interact, while reducing the need for intermediaries and costs of transactions. A major element of the blockchain based smart contract is the cryptographic key with which the contract is signed and acknowledged. Parties indicate their consent to the terms of the contract by providing their digital signature utilizing the cryptographic key. This process eliminates intermediaries and strengthens the level of accountability for all parties involved in a way not possible with traditional agreements. Smart contracts have numerous advantages over traditional contracts. As the contracts are translated into computer code, the evidence problem will be lessened since the computer cannot consider external evidence and can only run the code it is given. A smart contract is a powerful form of evidence that will not allow the parties involved to dispute unincorporated issues that are not agreed upon. It overcomes the need to have a person in charge of administrating and executing the contract since its terms can easily be converted to computer code and thereby executed automatically. (Pranata & Tehrani 2022).

3. Conclusion

Despite major attempts to address privacy and security issues, much uncertainty still persists in the cloud environment. The blockchain system, with its emphasis on decentralization, and the collaboration of individual work units for achieving a common goal, can help overcome all the shortcomings of the centralized system. Some of the issues relating to the use of cloud computing services discussed in this article can be resolved by using the blockchain system. The first issue of concern relates to ownership of data and its implications for the possible loss of control over it. This is mainly due to the existence of internal and external attackers and their ability to have unauthorized access to the data. This issue can be resolved by using blockchain which has as one of its main features data anonymity due to its complete encryption in the system.

The second issue is cross-border data transfers since ambiguity regarding the location of data that is stored in the cloud makes it difficult to ascertain the legal jurisdictions that may apply. In the cloud computing system, data - particularly personal data - transferred between multiple service providers is exposed to the risk of being accessed by unauthorized parties. This issue can be eliminated by using blockchains as they provide strict controls and ensure close monitoring over any potential illegal activity.

The third factor relates to contractual issues. Cloud computing usually "forces" people using its services to agree to the terms via a clickwrap agreement. Among the SLA issues is that the service provider may change the term

and conditions, and while some providers may notify the user of the change others may absolve themselves of any such obligation. This can be solved by using the smart contract in blockchain as it is made by consensus of the users, ensuring total understanding between both sides. A clickwrap agreement is non-negotiable and is seen as a take-it or leave-it option. It simply doesn't have the same capacity of blockchain smart contracts in accommodating the needs of the parties involved.

Blockchain is a promising solution for many distributed applications where trust and transparency are critical factors. The Internet of Things (IoT) platform is a multi-layer technology that enables the management and automation of connected devices within its universe. While many research proposals suggest solution for data sharing in IoT platforms by connecting them to blockchain platforms, most follow a hybrid approach where the cloud provider hosts the data and blockchain to ensure trust distribution and integrity and other related issues. These ideas can be used and are still proving the viability of blockchains in addressing privacy and security issues in cloud computing storage. They could be genuine options for data protection as they have the potential to provide robust and strong cyber security solutions where only legitimate users can see the data and where proof of identity is stored in a cryptographic format.

Acknowledgement

This work was supported by scholarship "Stipendien aus Mitteln des ASEA-Uninet, Projektstipendien SP 24" under The Austrian Agency for International Cooperation in Education & Research (OeAD-GmbH).

Reference

Adrian, A., 2013. How much privacy do clouds provide? An Australian perspective. *Computer Law & Security Review*. 29 (1): 48–57.

Akbar, A., 2018. Exclusion Clauses and the Reasonableness Test_ what you need to know about the latest court of appeal decisions. https://gowlingwlg.com/en/insights-resources/articles/2018/exclusion-clauses-and-the-reasonableness-test/accessed on 15th March 2018

Banu, S., & Kumar, R., 2018. Security in Cloud Computing Using Blockchain Technology. AIJR Proceedings, 1 (NCICCNDA): 422–439. One of the main features of blockchain is that it eliminates third party interferences between the data inside of the blockchain.

Bonhomme., V., et al., 2020. Chainlink and iExec collaborate to address the complex off-chain needs of next-generation decentralized applications, https://medium.com/iex-ec/chainlink-and-iexec-collaborate-to-address-the-complex-off-chain-needs-of-next-generation-702e55ab1ead

Cohn, A., et al., 2017. Smart after All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids, *George Town Technology Review.*

Ferdous, M.S., et al., 2017. Decentralised runtime monitoring for access control systems in cloud federations. in Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS), Atlanta, GA, USA, 2632–2633.

Gai, K., Raymond, K.K., & Zhu, L., 2018. Blockchain-Enabled Reengineering of Cloud Datacenters. *IEEE Cloud Computing*: 21-25.

Hölbl, M., 2011. Cloud Computing: Security and Privacy Issues. https://doi.org/10.1007/978-3-030-11196-0_55.

Hüllmann, T. A., 2018. Are Decentralized Autonomous Organizations the Future of Corporate Governance (Otto Beisheim School of Management). Thesis for: Bachelor of Science in International Business Administration https://doi.org/10.13140/RG.2.2.34344.88327

Johansson, A., 2014. The Enforceability of Clickwrap Agreements. UMEA: UMEA University.

Lis, P., Mendel, J., 2019. Cyberattacks on critical infrastructure: An economic perspective, Economics and Business Review 5 (19): 24-47.

Liu, B., et al., 2017. Blockchain based Data Integrity Service Framework for IoT data, 2017 IEEE 24th International Conference on Web Services, 25-30 June 2017. 468-475. DOI: 10.1109/ICWS.

Liu, B., et al. Blockchain based Data Integrity Service Framework for IoT data, 2017 IEEE 24th International Conference on Web Services, 25-30 June 2017. 468-475. DOI: 10.1109/ICWS.2017.54.

Mackie. J.,2020. Clickwrap in the EU". https://www.termsfeed.com/blog/clickwrap

Madrid Resolution, International Standards on the Protection of Personal Data and Privacy, International Conference of Data Protection and Privacy Commissioners. 5 November 2009. www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf accessed 6th February 2017

Microsoft Corp. v. United States 829 F.3d 197 (2d Cir. 2016)

Maroufi. M., et al., 2019. On the Convergence of Blockchain and Internet of Things (IoT) Technologies, *Journal of Strategic Innovation and Sustainability* (14) 1. DOI: https://doi. /10.33423/jsis.v14i1.990

Mungwe, R.E.M., 2017. Legal and Privacy Issues with Cloud Computing in Small and Medium Size Enterprises. *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS) 37*(1): 44-51.

OECD., 2014. Cloud Computing: The Concept, Impacts and the Role of Government Policy & quot; OECD Digital Economy Papers, No. 240, OECD Publishing, Paris. http://dx.doi.org/10.1787/5jxzf4lcc7f5-en

Pranata, A. R., & Tehrani, P. M., 2022. The Legality of Smart Contracts in a Decentralized Autonomous Organization (DAO). In Regulatory Aspects of Artificial Intelligence on Blockchain (pp. 112-131). IGI Global.

Pearson, S. & Benameur, A., 2010. Privacy, Security and Trust Issues Arising from Cloud Computing. 2nd IEEE International Conference on Cloud Computing Technology and Science. 693-792.

Piscini, E., Dalton, D., & Kehoe, L., 2017. Blockchain and Cyber Security. Deloitte.

Privacy in Cloud Computing. ITU-T Technology Watch Report. March 2012. https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf.

Rohrmann, C.A., et al., 2015. Some Legal Aspects of Cloud Computing Contracts, *Journal of International Commercial Law and Technology* (10) 1.

Salah, K., Rehman, M.H.U., Nizamuddin, N. and Al-Fuqaha, A., 2019. Blockchain for AI: Review and open research challenges. IEEE Access 7: 10127-10149. DOI: 10.1109/ACCESS.2018.2890507

Salman, T., et al., 2019. Security Services Using Blockchains: A State-of-the-Art Survey, *IEEE Communications Surveys & Tutorials* (21) 1.

Salmon, J., et al., 2019. Fresh Ideas about Business in Emerging Markets. www.ifc.org/thoughtleadership

Stanciu, A., 2017. Blockchain based distributed control system for edge computing. In 2017 21st International Conference on Control Systems and Computer Science (CSCS) (pp. 667-671). IEEE. DOI: 10.1109/CSCS.2017.102.

TagElsir, T., et al., 2015. Internal & external attacks in cloud computing environment from confidentiality, integrity and availability points of view. *IOSR Journal of Computer Engineering* (IOSR-JCE) 17 (2): 93-96. http://www.iosrjournals.org/iosr-jce/papers/Vol17-issue2/Version-5/N017259396.pdf accessed 6th March 2019.

Tehrani, P. M., Sabaruddin, J. S. B. H., & Ramanathan, D. A., 2018. Cross border data transfer: Complexity of adequate protection and its exceptions. Computer law & security review, 34(3), 582-594.

Tehrani, P. M., Sabaruddin, J. S. B. H., & Ramanathan, D. A., 2017. The problem of binary distinction in cloud computing and the necessity for a different approach: Positions of the European Union and Canada. Computer law & security review, 33(5), 672-684.

Truong, H., et al., 2019. Towards Secure and Decentralized Sharing of IoT Data, *Proceedings of the 2nd IEEE International Conference on Blockchain*, Atlanta, USA, 2019.

Zhang, Y., Deng, R., Liu, X. and Zheng, D., 2018. Outsourcing service fair payment based on blockchain and its applications in cloud computing. *IEEE Transactions on Services Computing*.