BACA: Jurnal Dokumentasi dan Informasi, Vol. 42, No. 1, 2021
ISSN 0125-9008 (Print); ISSN 2301-8593 (Online)
DOI: 10.14203/j.baca.v42i1.643
SK Dirjen Risbang -Kemristekdikti No 21/E/KPT/2018 (Peringkat 2 SINTA)

Data encryption algorithm AES by using blockchain technology: a review

Taufik Hidayat [1]*; Rahutomo Mahardiko[2]

[1]Department of Computer Engineering, Universitas Wiralodra, Indonesia
[2]Platinumetrix Pte, Ltd, Jakarta, Indonesia
*Correspondence: thidayat.ft@unwir.ac.id

Submission: 27-09-2020; **Review:** 12-11-2020; **Accepted:** 21-04-2021; **Revised:** 17-05-2021

ABSTRACT

Blockchain is used as an encryption algorithm in cryptocurrency, but fewer researches are found to study blockchain for data encryption. Data encryption is needed to protect the data from data theft. We know about data encryption, there are RSA, LEAP, AES, and other algorithms. This research proposed a review of the AES algorithm for data encryption within blockchain technology. The research process is followed by determining the library, then creating relevant questions and criteria. For a good opportunity in the future, this paper generated suggestions and opportunities so that better research can be established in data encryption.

ABSTRAK

Blockchain *digunakan sebagai algoritma enkripsi pada mata uang kripto, tetapi* blockchain *belum banyak digunakan untuk enkripsi data. Enkripsi data digunakan untuk melindungi data dari pencurian. Kita mengetahui tentang enkripsi data, seperti* RSA, LEAP, AES, *dan algoritma yang lain. Penelitian ini bertujuan untuk mengkaji algoritma* AES *bersamaan dengan* blockchain. *Proses riset dengan menentukan perpustakaan digital dan menghasilkan pertanyaan dan kriteria yang relevan. Tulisan ini menghasilkan saran dan kesempatan untuk riset pada enkripsi data di waktu yang akan datang.*

Keywords: Data Encryption; Blockchain; Hybrid Cryptography; AES algorithm; Digital library

1. INTRODUCTION

The development progress of blockchain technology is very fast. There is cryptocurrency utilizing blockchain technology (Qiu, Lu, & Lin 2019). The technology gives efficiency for cryptocurrency, because blockchain technology adopts a peer to peer system (P2P), concious mechanism, encryption algorithm and contract intelligence (Guo et al., 2019). Data form in blockchain is a chain that has a function to validate and store data using node and consensus (Niya et al., 2019). In addition, a chain also can update data using cryptographic method to secure data transfer and access (Lou et al., 2018). Some of demands in transferring and accessing data are security issues (Dave et al., 2019), (Jain & Sejwar, 2017). By using blockchain technology, security field can be increased (Preece & Easton, 2018; Tawalbeh et al., 2015).

In this paper, authors discuss data encryption within blockchain technology. By utilizing blockchain, data protection can be produced (Costa et al., 2019; Pitchay et al., 2015; Sivakumar et al., 2019). Then, many people who are not responsible is difficult to interfere (Tawalbeh et al., 2015; Rotondi et al., 2019). There are many encryption methods often used to secure data (Shimbre & Deshpande, 2015; Sivakumar et al., 2019), such as: RSA, LEAP, AES, and so on (Alharby, Aldweesh, & Moorsel, 2018; Yassein et al., 2017; Tawalbeh & Saldamli, 2019).

The blockchain technology is the main technology for cryptocurrencies, especially Bitcoin (BTC) and Ethereum (ETH) (Bratspies, 2018). The total market capitalization of USD 4.5 billion is being transacted in cryptocurrencies (Peters et al., 2015). Every transaction of cryptocurrency in the world needs to be secured well because all transactions in cryptocurrency have been monitored and sometimes hijacked by theft (Bratspies, 2018), even though the data protection already there in the blockchain technology. For instance, a hacking attack on the largest BTC exchange company made a bankruptcy to the company for the stolen 850,000 BTC (Reddy & Minnaar, 2018).

This theft activity can bring many losses for people who transact the cryptocurrencies and trust for the blockchain technology (Bratspies, 2018). So that, the combination of the blockchain technology and the data encryption is a must to secure well the blockchain. SLR is being held by authors to carry out academically regarding data encryption within blockchain technology. Many SLR researches have been conducted well (Qiu, Lu, & Lin 2019). Clearly, Table 1 explains data encryption study that has been done by previous research.

Table 1. Previous Studies in Data Encryption Blockchain

Author	Research Findings
Qiu, Lu, & Lin (2019)	Analysis of cryptography using fuzzy method
Guo et al. (2019)	Efficiency during connection through node to node by applying blockchain
Lou et al. (2018)	Blockchain application in trust model NDN (Named Data Networking)
Dave et al. (2019)	Wide application by using blockchain, but less implementation because of some disadvantages
Preece & Easton (2018)	Virtual machine modification inside blockchain programming language
Alharby, Aldweesh, & Moorsel (2018)	Smart contract blockchain for every sector
Zhang et al. (2019)	Data security to deal with blockhain widely
Wang, Tian, & Zhu (2018)	Data encryption to ensure the authenticity of data on the blockchain network
Holtkemper & Wieninger (2018)	Types of company data to be stored in a blockchain network
Nagesh & Thejaswini (2017)	Data security by using AES Algorithm
Bak, Pyo, & Jeong (2019)	Data encryption with EGG integrity blockchain
Yi (2019)	Machine learning algorithm and blockchain encryption for instant message

In the previous research, it was explained that data security is very important and various methods were used (Hidayat & Mahardiko, 2020) so that the data transferred by the sender and receiver is truly authentic without any change (Hidayat, Azzery, & Mahardiko, 2019).

2. LITERATURE REVIEW

2.1 Blockchain Technology

Blockchain is a decentralized block structure. The structure on the blockchain has three systems (Mohsin et al., 2019). The first system is a centered node (Xu, 2018), while the block chain is stored in private mode. The second system is a distributed node (Wang, Tian, & Zhu, 2018), while the blockchain is stored in public mode and on several servers. The third system is a decentralized node, while the blockchain and all blocks are connected to each other (Yang, Chen, & Xiang, 2018; Dave et al., 2019).

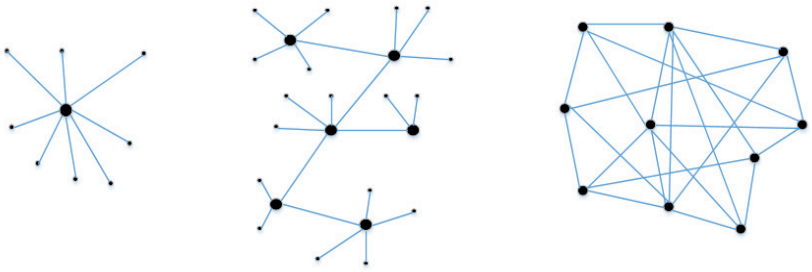


Figure 1. Blockchain Technology (Zhou, Wu, & Zhou, 2017)

2.2 Data Encryption

There is a standard algorithm that is used widely for encryption (Mohsin et al., 2019). The name is Advanced Encryption Standard Algorithm (AES) (Chen, Hu, & Li, 2019). For example, US Federation agency sets standards in processing of data encryption in all fields. The AES algorithm is chosen because it has some advantages (Lee, Dewi, & Wajdi, 2018). First, it is more secure than other encryption (Babrahem & Monowar, 2018). Second, AES algorithm can be determined as symmetrical block cipher (Liu, Gong, & Fan, 2018). Third, AES algorithm can do more than 8-bit (Akhil, Kumar, & Pushpa, 2017). Fourth, it takes a plaintext that has block size 128 bits, 192 bits and 256 bits. Figure 2 is an illustration of the data encryption process with AES algorithm (Surv et al., 2015). AES algorithm secures data during file transfer from server to client (Bhardwaj et al., 2016; Yassein et al., 2017).

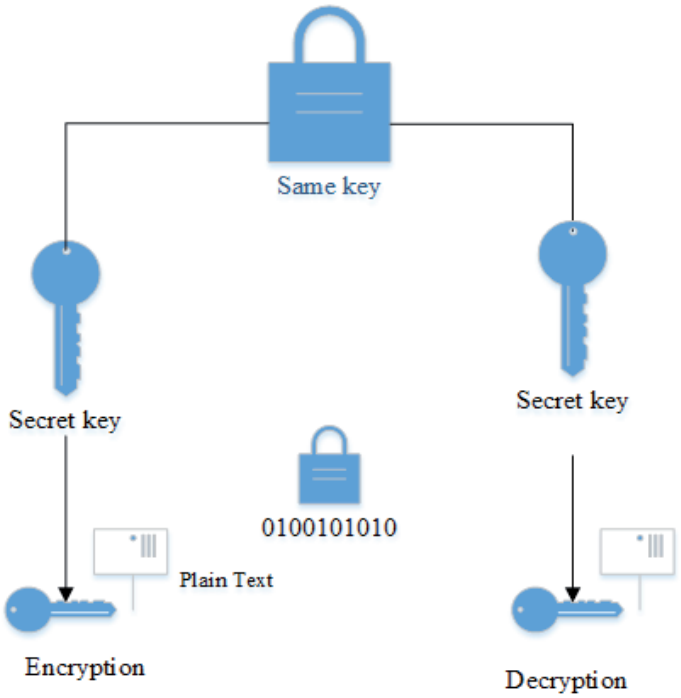
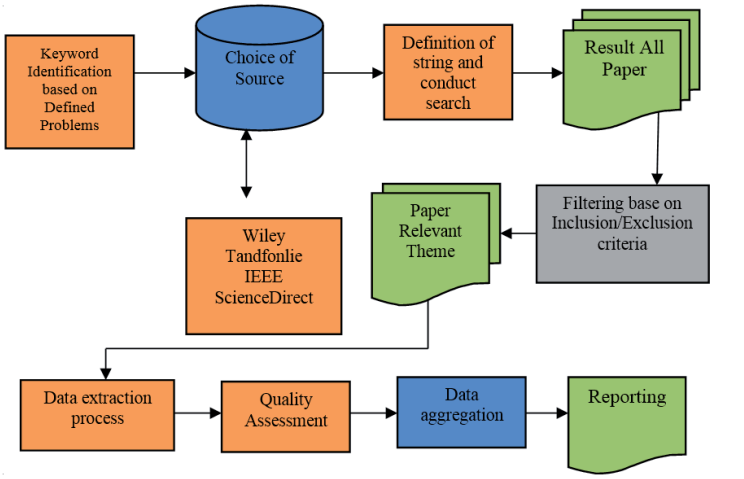


Figure 2. Process of Encryption in AES (Madhavapandian & MaruthuPandi, 2020)

3. METHOD

3.1 Systematic Literature Review (SLR) Process

SLR process has some steps (Qasem et al., 2019; Salleh et al., 2018; Rosati et al., 2017; Hidayat, Azzery, & Mahardiko, 2019; Hidayat et al., 2020; Hidayat & Mahardiko, 2020; Sharma & Singh, 2017; Al-Ahmad et al., 2019; Christo et al., 2019; Boomija, 2016; Shen & Pena-Mora, 2018). First, we had to define the problems. Secondly, we had to determine keyword based on the defined problems. Thirdly, we chose some trusted libraries as main database. Fourthly, we chose only journal article and paper conference in all those libraries. Fifthly, we got all retrieved papers based on determined keyword. Sixthly, all received papers then were filtered based on theme suitability



and defined criteria. The last, we selected and extracted some papers according to predetermined criteria and quality assessments. Figure 3 shows SLR process that we followed to generate the respected result.

Figure 3. SLR of data encryption within blockchain

3.2 The Defined Problem

This paper has stated that the combination between the blockchain technology and the data encryption is a must to secure well the blockchain. For this purpose, the authors defined several problem statements, such as: definition of the blockchain, definition of the data encryption, and how encrypt the data within the blockchain. Table 2 is the research problem statement.

Table 2. Problem Statements

Research Statements	Research Objectives
What is blockchain technology?	Identify definition of blockchain technology
What is data encryption?	Identify definition of data encryption used widely in the security area
What are the application of data encryption, especially AES algorithm?	Identify the advantages and disadvantages of AES algorithm so that better blockchain security can be enhanced through AES implementation
What is the research contribution for better security in the blockchain?	Identify the contribution that can be implemented for enhancing the security of the blockchain

3.3 Digital Library Assessment

SLR consists of several processes, such as: identification, assessment, and interpretation in order to find research findings in answering predetermined questions (Hidayat, Azzery, & Mahardiko,

2019; Franciscon et al., 2019). The SLR method is a step having some stages. In addition, this systematic approach is to distinguish from traditional literature reviews. By using this protocol, it is a must to avoid subjective processes in the literature review (Lo et al., 2019).

Process of literature review is divided into several sections which have been defined in Figure 3. First step is to determine the objectives of the SLR, to plan and compile a set of questions, to create a method of searching strategies, to create a searching process of criteria and to develop data encryption review. Second step is to identify some literatures that will be examined, to conduct selection and evaluation of literature that has relation to research, to do data extraction, to review quality of literature and to re-write anything obtained from review. Third step is to make a report for the SLR method process after all temporary synthesis has been made.

Table 3. The Trusted Online Library

Digital Online Library	Link Website
Wiley	https://onlinelibrary.wiley.com/
Tandfonline	https://www.tandfonline.com/
IEEE	https://ieeexplore.ieee.org/
ScienceDirect	http://www.sciencedirect.com/

Table 3 explains some libraries that authors use to search papers. We conduct a search on "Wiley", "Tandfonline", "IEEE", and "ScienceDirect" because there are lots of paper in high quality. For the criteria selection on paper, Table 4 is the guidance.

Table 4. Selection Criteria for SLR

ID	Exclusion
E1	Books, Review Article, Survey, Discussion, Correspondence letters, Editorial beyond scope of this review
E2	Not English paper
E3	Poor quality of paper by judging
E4	Paper that does not focus on data encryption within blockchain and paper that only discusses blockchain in its abstract
	Inclusion
I1	Full version of conference proceeding and journal articles which discuss in data encryption with blockchain technology
I2	Papers which propose a solution data encryption within blockchain
I3	Paper that only uses English
I4	Papers which are published in 2014 to 2019
	Quantity Assessment
AQN1	Is there any process to measure?
AQN2	Is anything measured by numbers?
AQN3	Measurement standards exist or new proposal?
	Quality Assessment
AQL1	Has the paper been reviewed from previous research?
AQL2	Are the methods carried out in accordance?
AQL3	Is there a lot of discovery?
AQL4	Is there enough description in context?
AQL5	What are strengths of research objectives?
AQL6	Clear research findings?

Based on first part of the research question in Table 2, we determine the purpose of the review. First purpose is to know the definition of the "Blockchain". Second purpose is to understand the definition of the "Data Encryption with AES". The last purpose is to learn the implementation of "AES Data Encryption on the Blockchain Technology". This paper conducted papers search in Wiley, Tandfonline, IEEE Explore and ScienceDirect databases from 2015 to 2019. This activity was conducted on April 12th, 2020 which aimed to find relevant papers related to the theme.

4. RESULTS AND DISCUSSION

4.1 Result of Paper Search by Keyword

SLR discussion is about to answer the Table 2 "Data Encryption Algorithm AES by using Blockchain Technology". Question on SLR is done for 2015 to 2019. Table 5 is result of paper searching on the latest research regarding the question.

Table 5. Result Paper by Keyword

Digital Library Online	Keyword	Result Paper
Wiley	Blockchain	567
	Data Encryption AES	382
	Data Encryption AES Blockchain Technology	21
Tandfonline	Blockchain	487
	Data Encryption AES	178
	Data Encryption AES Blockchain Technology	5
IEEE Explore	Blockchain	991
	Data Encryption AES	779
	Data Encryption AES Blockchain Technology	1
ScienceDirect	Blockchain	1760
	Data Encryption AES	1631
	Data Encryption AES Blockchain Technology	73

Table 5 is keyword result to answer the question. From table 5, there is still a chance to research on "Data Encryption Algorithm AES for blockchain tecnology" for analysis.

Table 6. Summary of Paper in Digital Library for Analysis

Database Journal	Result Paper
Wiley	21
Tandfonline	5
IEEE Explore	1
ScienceDirect	73
Total	100

4.2 SLR Result of Articles

This paper discussion presents SLR about AES data encryption within blockchain technology. Questions on SLR are applied to papers obtained from 2015 to 2019. Figure 4 illustrates a statistical paper about the AES data encryption blockchain research.

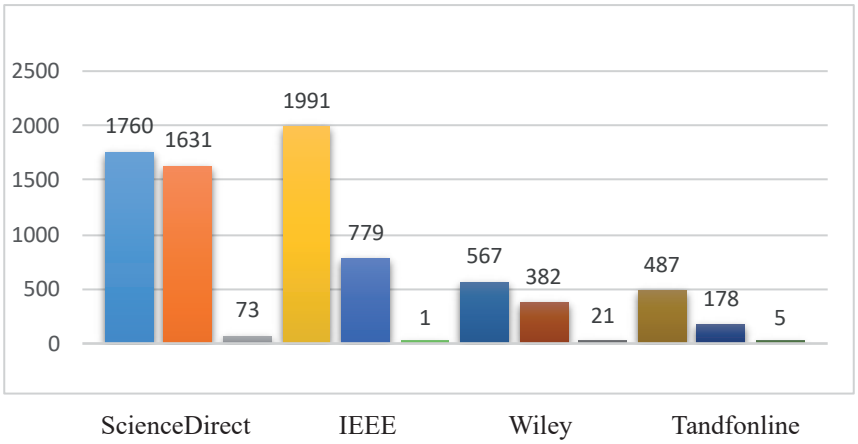


Figure 4. Statistic of data encryption AES blockchain

Based on extracted paper from Wiley, Tandfonline, IEEE Explore and Science Direct with SLR, we get only one paper from IEEE Explore that discusses AES Data Encryption within blockchain technology, meanwhile we received more than 70 papers from Science Direct. Besides that, 21 papers retrieved from Wiley and 5 papers from Tandfonline. With this result, SLR is able to give an academic picture for AES data encryption within blockchain and give an understanding that data encryption may create difficulty to unauthorized people.

4.3 Data Encryption Comparison

We had observed a number of studies related to data encryption. Using keywords like data encryption, blockchain technology and SLR, authors generated result from data encryption within blokchain through additional comments. Here is the data collected from 4 databases, such as: Wiley, Tandfonline, IEEE Explore and Science Direct from 2015 to 2019. This research found a number of studies in data encryption by 30% and technology blockchain by 10%. SLR comparison after a review of data encryption within blockchain can be summarized in a comparison table. SLR table about data encryption can be seen in next table 7.

Table 7. Data Encryption Comparison

Description	Encryption Data AES	Encryption Data AES Blockchain
Research Question	Up to 7	Only 1
Search Strategy	Keyword based on authors and Keyword based on extraction from the known subset of papers	Keyword based on specific subject
Model of String	5 models	1 model
Resource to be Search	4 libraries	2 libraries
Paper Selection	8 in exclusion criteria	4 in exclusion criteria
	4 in inclusion criteria	4 in inclusion criteria
	9 in quality assessments	6 in quality assessments

Table 7 gives an explanation of paper comparisons related to AES data encryption within blockchain technology. Authors selected and extracted some papers according to predetermined criteria (Table 4) and some assessments (Table 4).

4.4 Journal Review

The number of retrieved papers from 4 trusted digital libraries were 100 papers, we then extracted some papers. Table 7 explains each definition, such as: AES Algorithm, Data Encryption, Blockchain technology and measurements.

Table 8. Result of Journal Review

Paper	Scope					
	AES Algorithm	Data Encryption	Blockhain Technology	Quantity Measurement	Quality Measurement	Experiment
Qiu, Lu, & Lin (2019)	v	v	x	x	v	v
Guo et al. (2019)	x	x	v	v	v	v
Lou et al. (2018)	x	x	v	x	v	v
Dave et al. (2019)	x	x	v	v	x	x
Preece & Easton (2018)	x	x	v	v	v	v
Alharby, Aldweesh, & Moorsel (2018)	x	x	v	v	v	x
Zhang et al. (2019)	x	x	v	v	v	v
Makhdoom et al. (2019)	x	x	x	v	v	x
Li et al. (2020)	x	x	v	v	v	x
Lyu et al. (2020)	x	x	v	v	v	v
Tawalbeh & Saldamli (2019)	x	v	v	v	v	v
Islam & Young- Shin (2020)	x	v	x	v	x	v
Adams (2020)	v	v	v	x	v	v
Costa et al. (2019)	v	v	v	x	v	v
Mohsin et al. (2019)	x	v	v	x	v	v
Wutthikarn & Hui (2018)	x	v	v	x	v	v
Zhou et al. (2017)	x	x	v	v	x	v
Yi (2019)	x	v	v	v	x	v
Yassein et al. (2017)	v	v	x	v	v	v
Yang et al. (2018)	x	x	v	x	v	v
This paper	v	v	v	v	v	v

Twenty papers extracted will guide the opportunity for the work on the blockchain technology using AES algorithm to secure well the cryptocurrency. The research with quantity and quality measuresments (Table 4) also can be followed. So that, the new science and technology for preventing the theft can be achieved.

5. CONCLUSION

By using SLR method, this study brings positive result in blockchain technology area especially in data encryption. The result of journal review indicates that no paper has discussed all defined scopes. In addition, this research contributes to arrange some relevant questions to gain better

understanding in following data encryption especially in AES. This research only reviews data encryption in blockchain by using AES technology. After SLR had been conducted regarding to data encryption within blockchain, this can lead a next research by implementing all defined scopes in journal review.

6. ACKNOWLEDGMENT

The authors thank the Department of Computer Engineering, Universitas Wiralodra for providing support to the author regarding with this research.

REFERENCES

Adams, C. 2020. A Privacy-Preserving Blockchain with Fine-grained Access Control. *Security and Privacy*, *3*(2): 1–9. doi.org/10.1002/spy2.97.

Agarkar, A. & Agrawal, H. 2019. A Review and Vision on Authentication and Privacy Preservation Schemes in Smart Grid Network. *Security and Privacy, 2*(2): 1–18. doi.org/10.1002/spy2.62.

Akhil, K. M., Kumar, M.P., & Pushpa, B.R. 2017. Enhanced Cloud Data Security Using AES Algorithm. In *2017 International Conference on Intelligent Computing and Control (I2C2)*, January:1–5. IEEE. doi.org/10.1109/I2C2.2017.8321820.

Al-Ahmad, A.S., Kahtan, H., Hujainah, F., & Jalab, H.A. 2019. Systematic Literature Review on Penetration Testing for Mobile Cloud Computing Applications. *IEEE Access, 7*: 173524–40. doi.org/10.1109/ACCESS.2019.2956770.

Alharby, M., Aldweesh, A., & Moorsel, A.V. 2018. Blockchain-Based Smart Contracts: A Systematic Mapping Study of Academic Research. In *2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB)*, 1–6. IEEE. doi.org/10.1109/ICCBB.2018.8756390.

Babrahem, A.S., & Monowar, M.M. 2018. Preserving Confidentiality and Privacy of the Patient's EHR Using the OrBAC and AES in Cloud Environment. *International Journal of Computers and Applications*, 7074. doi.org/10.1080/1206212X.2018.1505025.

Bak, S., Pyo, Y., & Jeong, J. 2019. Protection of EEG Data Using Blockchain Platform. In *2019 7th International Winter Conference on Brain-Computer Interface (BCI)*, 1–3. doi.org/10.1109/IWW-BCI.2019.8737260.

Bhardwaj, A., Subrahmanyam, G.V.B., Avasthi, V., & Sastry, H. 2016. Security Algorithms for Cloud Computing. *Procedia Computer Science, 85*: 535–42. doi.org/10.1016/j.procs.2016.05.215.

Boomija, M.D. 2016. Secure Data Sharing through Additive Similarity Based ElGamal Like Encryption. In *2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*, 652–55. IEEE. doi.org/10.1109/AEEICB.2016.7538370.

Bratspies, R.M. 2018. Cryptocurrency and the Myth of the Trustless Transaction. *Michigan Telecommunications and Technology Law Review, 25*(1): 2–54. doi.org/10.2139/ssrn.3141605.

Chen, S, Wei-Hu, W., & Li, Z. 2019. High Performance Data Encryption with AES Implementation on FPGA. In *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, 149–53. doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00036.

Christo, M.S., Merjora A.A., Sarathy G.P., Priyanka, C., & Kumari R.M. 2019. An Efficient Data Security in Medical Report Using Block Chain Technology. In *2019 International Conference on Communication and Signal Processing (ICCSP),* 0606–10. IEEE. doi.org/10.1109/ICCSP.2019.8698058.

Costa, L., Neto, A., Pinheiro, B., Cordeiro, W., Araújo, R., & Abelém, A. 2019. Securing Light Clients in Blockchain with DLCP. *International Journal of Network Management, 29*(3): e2055. doi.org/10.1002.nem.2055.

Dave, D., Parikh, S., Patel, R., & Doshi, N. 2019. A Survey on Blockchain Technology and Its Proposed Solutions. *Procedia Computer Science, 160*: 740–45. doi.org/10.1016/j.procs.2019.11.017.

Franciscon, E.A, Nascimento, M.P., Granatyr, J., Weffort, M.R., Lessing, O.R., & Scalabrin, E.E. 2019. A Systematic Literature Review of Blockchain Architectures Applied to Public Services. *2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design*, 33–38. doi.org/10.1109/CSCWD.2019.8791888.

Guo, Y., Kun, Lv., Shitang-Yu, S., Zou, J., Zhang, B., & Shao, Z. 2019. A High Performance Blockchain Platform for Intelligent Devices. *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, 260–61. doi.org/10.1109/HOTICN.2018.8606017.

Hassan, H.E.R., Tahoun, M., & ElTaweel, G.S. 2020. A Robust Computational DRM Framework for Protecting Multimedia Contents Using AES and ECC. *Alexandria Engineering Journal, 59*(3): 1275–86. doi.org/10.1016/j.aej.2020.02.020.

Hidayat, T., Azzery, Y., & Mahardiko, R. 2019. Load Balancing Network by Using Round Robin Algorithm: A Systematic Literature Review. *Jurnal Online Informatika, 4*(2): 85–89. doi.org/10.15575/join.v4i2.446.

Hidayat, T., & Mahardiko, R. 2020. A Systematic Literature Review Method on AES Algorithm for Data Sharing Encryption on Cloud Computing. *International Journal of Artificial Intelligence Research, 4*(1): 49–57. doi.org/10.29099/ijair.v4i1.154.

Hidayat, T., Mahardiko, R., & Franky, S.T.D. 2020. Method of Systematic Literature Review for Internet of Things in ZigBee Smart Agriculture. In *2020 8th International Conference on Information and Communication Technology (ICoICT)*, 1–4. doi.org/10.1109/ICoICT49345.2020.9166195.

Holtkemper, D., & Wieninger, S. 2018. Company Data in the Blockchain: A Juxtaposition of Technological Drivers and Potential Applications. *PICMET 2018 - Portland International Conference on Management of Engineering and Technology: Managing Technological Entrepreneurship: The Engine for Economic Growth, Proceedings*, 1–7. doi.org/10.23919/PICMET.2018.8481811.

Islam, A., & Shin, S.Y. 2020. A Blockchain-Based Secure Healthcare Scheme with the Assistance of Unmanned Aerial Vehicle in Internet of Things. *Computers and Electrical Engineering, 84*: 106627. doi.org/10.1016/j.compeleceng.2020.106627.

Jain, G., & Sejwar, V. 2017. Improving the Security by Using Various Cryptographic Techniques in Cloud Computing. In 2*017 International Conference on Intelligent Computing and Control Systems (ICICCS)*, January:23–28. IEEE. doi.org/10.1109/ICCONS.2017.8250721.

Lee, B.H., Dewi, E.K., & Wajdi, M.F. 2018. Data Security in Cloud Computing Using AES under HEROKU Cloud. In *2018 27th Wireless and Optical Communication Conference (WOCC)*, 1–5. IEEE. doi.org/10.1109/WOCC.2018.8372705

Li, Y.N., Feng, X., Xie, J. Feng, H., Guan, Z., & Wu, Q. 2020. A Decentralized and Secure Blockchain Platform for Open Fair Data Trading. *Concurrency Computation, 32*(7): 1–11. doi.org/10.1002/cpe.5578.

Liu, Y., Gong, W., & Fan, W. 2018. Application of AES and RSA Hybrid Algorithm in E-Mail. In *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, 701–3. IEEE. doi.org/10.1109/ICIS.2018.8466380.

Lo, S.K., Liu, Y., Chia, S.Y., Xu,X., Lu, Q., Zhu, L., & Ning, H. 2019. Analysis of Blockchain Solutions for IoT: A Systematic Literature Review. *IEEE Access, 7*(1): 58822–35. doi.org/10.1109/ACCESS.2019.2914675.

Lou, J., Zhang, Q., Qi, Z., & Lei, K. 2018. A Blockchain-Based Key Management Scheme for Named Data Networking. In *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, 141–46. IEEE. doi.org/10.1109/HOTICN.2018.8605993.

Lyu, Q., Qi, Y., Zhang, X., Liu, H., Wang, Q., & Zheng, N. 2020. SBAC: A Secure Blockchain-Based Access Control Framework for Information-Centric Networking. *Journal of Network and Computer Applications, 149*: 102444. doi.org/10.1016/j.jnca.2019.102444.

Madhavapandian, S., & Maruthu, P. 2020. FPGA Implementation of Highly Scalable AES Algorithm Using Modified Mix Column with Gate Replacement Technique for Security Application in TCP/IP. *Microprocessors and Microsystems, 73*: 102972. doi.org/10.1016/j.micpro.2019.102972.

Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. 2019. Blockchain's Adoption in IoT: The Challenges, and a Way Forward. *Journal of Network and Computer Applications, 125*: 251–79. Elsevier Ltd. doi.org/10.1016/j.jnca.2018.10.019.

Mohsin, A.H., Zaidan, A.A., Zaidan, B.B., Albahri, O.S., Albahri, A.S., Alsalem, M.A., & Mohammed, K.I. 2019. Based Blockchain-PSO-AES Techniques in Finger Vein Biometrics: A Novel Verification Secure Framework for Patient Authentication. *Computer Standards & Interfaces, 66* (October): 103343. doi.org/10.1016/j.csi.2019.04.002.

Nagesh, H. R., & Thejaswini, L. 2017. Study on Encryption Methods to Secure the Privacy of the Data and Computation on Encrypted Data Present at Cloud. In *2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC)*, 383–86. IEEE. doi.org/10.1109/ICBDACI.2017.8070868.

Niya, S.R., Schiller, E., Cepilov, I., Maddaloni, F., Aydinli, K., Surbeck, T., Bocek, T., & Stiller, B. 2019. Adaptation of Proof-of-Stake-Based Blockchains for IoT Data Streams. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 15–16. IEEE. doi.org/10.1109/BLOC.2019.8751260

Peters, G.W., Panayi, E., & Chapelle, A. 2015. Trends in Cryptocurrencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective. *The Journal of Financial Perspectives: FinTech, 3*(3): 1–46.

Pitchay, S.A., lhiagem, W.A.A., Ridzuan, F., & Saudi, M.M. 2015. A Proposed System Concept on Enhancing the Encryption and Decryption Method for Cloud Computing. In *2015 17th UKSim-AMSS International Conference on Modelling and Simulation (UKSim)*, 201–5. IEEE. doi.org/10.1109/UKSim/2015.74.

Preece, J. D., & Easton, J.M. 2018. Towards Encrypting Industrial Data on Public Distributed Networks. In *2018 IEEE International Conference on Big Data (Big Data)*, 4540–44. IEEE. doi.org/10.1109/BigData.2018.8622246.

Qasem, Y.A.M., Abdullah, R., Jusoh, Y.Y., Atan, Y., & Asadi, S. 2019. Cloud Computing Adoption in Higher Education Institutions: A Systematic Review. *IEEE Access, 7*: 63722–44. doi.org/10.1109/ACCESS.2019.2916234.

Qiu, J., Lu, X., & Lin, J. 2019. Optimal Selection of Cryptographic Algorithms in Blockchain Based on Fuzzy Analytic Hierarchy Process. In *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, 208–12. IEEE.doi.org/10.1109/CCOMS.2019.8821757.

Reddy, E., & Minnaar, A. 2018. Cryptocurrency: A Tool and Target for Cybercrime. *Acta Criminologica: Southern African Journal of Criminology, 31*(3): 71–92.

Rosati, P., Fox, G., Kenny, D., & Lynn, T. 2017. Quantifying the Financial Value of Cloud Investments: A Systematic Literature Review. *Proceedings of the International Conference on Cloud Computing Technology and Science*, CloudCom-December: 194–201. doi.org/10.1109/CloudCom.2017.28.

Rotondi, D., Saltarella, M., Giordano, G., & Pellecchia, F. 2019. Distributed Ledger Technology and European Union General Data Protection Regulation Compliance in a Flexible Working Context. *Internet Technology Letters, 2*(5): e127. doi.org/10.1002/itl2.127.

Salleh, N.A., Hussin, H., Suhaimi, M.A., & Ali, A.M. 2018. A Systematic Literature Review of Cloud Computing Adoption and Impacts among Small Medium Enterprises (SMEs). *Proceedings - International Conference on Information and Communication Technology for the Muslim World 2018*, 278–84. doi.org/10.1109/ICT4M.2018.00058.

Sharma, P., & Singh, J. 2017. Systematic Literature Review on Software Effort Estimation Using Machine Learning Approaches. In *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)*, 43–47. IEEE. doi.org/10.1109/ICNGCIS.2017.33.

Shen, C., & Pena-Mora, F. 2018. Blockchain for Cities - A Systematic Literature Review. *IEEE Access, 6*: 76787–819. doi.org/10.1109/ACCESS.2018.2880744.

Shimbre, N., & Deshpande, P. 2015. Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm. *Proceedings - 1st International Conference on Computing, Communication, Control and Automation, ICCUBEA*, 35–39. doi.org/10.1109/ICCUBEA.2015.16.

Sivakumar, P.M., Kumar, N., Jayaraj, R., & Kumaran, A.S. 2019. Securing Data and Reducing the Time Traffic Using AES Encryption with Dual Cloud. In *2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)*, 1–5. IEEE. doi.org/10.1109/ICSCAN.2019.8878749.

Surv, N., Wanve, B., Kamble, R., Patil, S., & Katti, J. 2015. Framework for ClientSide AES Encryption Technique in Cloud Computing. *Souvenir of the 2015 IEEE International Advance Computing Conference, IACC,* 525–28. doi.org/10.1109/IADCC.2015.7154763.

Tawalbeh, L., & Saldamli, G. 2019. Reconsidering Big Data Security and Privacy in Cloud and Mobile Cloud Systems. *Journal of King Saud University - Computer and Information Sciences*. doi.org/10.1016/j.jksuci.2019.05.007.

Tawalbeh, L., Darwazeh, N.S., Al-Qassas, R.S., & AlDosari, F. 2015. A Secure Cloud Computing Model Based on Data Classification. *Procedia Computer Science, 52*(1): 1153–58. doi.org/10.1016/j.procs.2015.05.150.

Wang, Z., Tian, Y., & Zhu, J. 2018. Data Sharing and Tracing Scheme Based on Blockchain. Proceeding of 8th International Conference on Logistics, Informatics and Service Sciences, 1–6. doi.org/10.1109/LISS.2018.8593225.

Wutthikarn, R., & Hui, Y.G. 2018. Prototype of Blockchain in Dental Care Service Application Based on Hyperledger Composer in Hyperledger Fabric Framework. In *2018 22nd International Computer Science and Engineering Conference (ICSEC)*, 1–4. IEEE. doi.org/10.1109/ICSEC.2018.8712639.

Xu, Y. 2018. Section-Blockchain: A Storage Reduced Blockchain Protocol, the Foundation of an Autotrophic Decentralized Storage Architecture. *Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems*, December: 115–25. doi.org/10.1109/ICECCS2018.2018.00020.

Yang, C., Chen, X., & Xiang, Y. 2018. Blockchain-Based Publicly Verifiable Data Deletion Scheme for Cloud Storage. *Journal of Network and Computer Applications, 103*: 185–93. doi.org/10.1016/j.jnca.2017.11.011.

Yassein, M.B., Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y. 2017. Comprehensive Study of Symmetric Key and Asymmetric Key Encryption Algorithms. In *2017 International Conference on Engineering and Technology (ICET)*, January:1–7. IEEE. doi.org/10.1109/ICEngTechnol.2017.8308215.

Yi, H. 2019. Securing Instant Messaging Based on Blockchain with Machine Learning. *Safety Science, 120*: 6–13. doi.org/10.1016/j.ssci.2019.06.025.

Zhang, M., Wang, S., Zhang, P., He, L., Li, X., & Zhou, S. 2019. Protecting Data Privacy for Permissioned Blockchains Using Identity-Based Encryption. In *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, 602–5. IEEE. doi.org/10.1109/ITNEC.2019.8729244.

Zhou, N., Wu, M., & Zhou, J. 2017. Volunteer Service Time Record System Based on Blockchain Technology. *Proceedings of 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference, IAEAC*, 610–13. doi.org/10.1109/IAEAC.2017.8054088.