International Journal Of Artificial Intelegence Research
Vol 4, No 1, June 2020, pp. 49 - 57
ISSN: 2579-7298

A Systematic Literature Review Method On AES Algorithm for Data Sharing Encryption On Cloud Computing

Taufik Hidayat[a,1,*], Rahutomo Mahardiko[b,2]

[a] *Department of Computer Engineering, Universitas Wiralodra, Indramayu, Indonesia*
[b] *Platinumetrix Pte. Ltd, Jakarta, Indonesia*
[1] *thidayat.ft@unwir.ac.id*;* [2] *rahutomo.mahardiko@gmail.com*
[1] *orcid.org/0000-0002-1811-4714*;* [2] *orcid.org/0000-0001-7324-0556*

* *corresponding author*

ARTICLE INFO

Article history:
Received 16-02-2020
Revised : 03-03-2020
Accepted 24-03-2020

Keywords:
cloud computing
encryption
data sharing
AES Algorithm
systematic literature review

ABSTRACT

Cloud computing is one revolution in information technology (IT) that can share resources, services and data through a network among users. Because users have same rights on the network to transfer data, data are vulnerable to be attacked by unauthorized person. Lately, data security in a system only concentrates on data storage on cloud by utilizing internet security, but a little concentration is found during data transmission. By considering security as a serious problem, an encryption-based proposed system is presented to secure during data transfer. Authors propose an approach to boost system security during data transfer in order to prevent data theft by unauthorized person. To prevent an attack by unauthorized person, Advanced Encryption Standard (AES) will be proposed to secure data transmission and storage in cloud computing. For better future, authors will propose Systematic Literature Review (SLR) to generate suggestions and opportunities in AES cloud computing.

I. Introduction

Cloud computing is an internet-based storage service [1]. The cloud gives services to its user to store data. Because of its services, there is a significant increment in term of storage usage [2]. Wide service and accessible facility are reasons to significant increment effect [3], [4]. Due to high demand on cloud usage [5], every cloud service provider is encouraged to provide data security to its user [6], [7]. To achieve high data safety, there is a proposed model of data security to prevent any unauthorized person from data stealing [8], [9].

Data and information securities are primary challenge in cloud service [10]. Hence, preventive method is encouraged to protect user's data and information [11], [12]. There is a preventive method called encryption to anticipate any intruder [13], [14]. A proposed encryption algorithm involves symmetric cryptographic called key to do encryption and decryption [3], [15], [16]. AES algorithm is proposed for safety during data transfer [17]. The algorithm is believed to be more efficient than other algorithm [17], [18]. There are advantages for applying AES algorithm [19], [8], such as: large scale data to be encrypted and little resource consumption [14]. The algorithm is believed that it can secure on user's data and information [8], [20].

Table 1. Previous Studies of AES Encryption on Cloud Computing

Paper	Year	Research Result
[9]	2015	Secure and resolve data security problem on cloud computing by AES
[20]	2019	Secure data and reduce traffic time by AES encryption
[21]	2018	Heterogeneous model on cloud computing is able to give data security contribution
[22]	2019	Big volumes of private data are collected and need to be secured in cloud
[23]	2019	Security modeling on cloud computing to prevent data theft
[24]	2019	Symmetric encryption scheme is implemented in client before data is uploaded to cloud computing
[25]	2017	Usages of authentication and cryptographic for future security on cloud computing operating system
[26]	2015	Data security problem in distributed data system proposing SHA-1 algorithm to secure data

II. Research Method

This paper will use SLR method. It can be said that it is formal method to review and translate based on specific question [27]. SLR has 3 steps [28], [27]. There are to plan review process, to do review process and to report review process [29], [30]. Authors use several trusted databases for searching relevant paper to support authors' research.

Table 2. Digital Library Journal

No.	Digital Online Library	Website
1.	IEEE Explore	https://ieeexplore.ieee.org/
2.	ScienceDirect	https://www.sciencedirect.com/
3.	Tandfonline	https://www.tandfonline.com/

Table 2 explains some trusted digital library for getting relevant paper. There are "IEEE Xplore"," ScienceDirect"," Tandfonline" from 2014 to 2019. Authors' reason is that those databases have high quality of reputation. Next figure depicts required step in SLR.

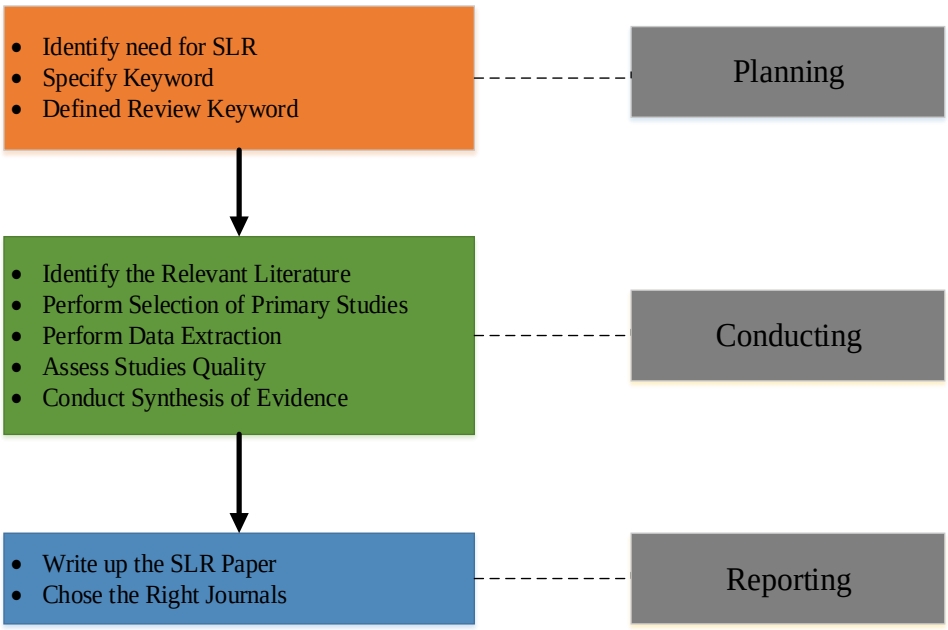


Fig 1. Systematic Literature Review [29]

Before authors process the SLR process in figure 5, it is a need to develop criteria for separating unreliable and reliable papers [31]. To create high rate of paper identification, authors also add some

questions for quality and quantity assessments for high quality papers. Table 3 explains criteria that has been mentioned [32].

Table 3. Criteria of paper identification

ID	Unreliable
U1	The focus of the paper has not been updated with the current conditions
U2	Not English paper
U3	Paper discussion material is not very related to what is sought by researchers
U4	Poor quality of paper by judging
	Reliable
R1	The contents of the paper are still up to date with the current conditions
R2	Paper that discusses the concept of Cloud Computing
R3	Paper that discusses the concept of AES Algorithm
R4	Paper published from 2015 to 2019
	Quality Assessment
QLA1	Results of research?
QLA2	What are strengths of research objectives?
QLA3	Is there enough description in context?
QLA4	Has the paper been reviewed from previous research?
QLA5	Are the methods carried out in accordance?
	Quantity Assessment
QNA1	Is anything measured by numbers?
QNA2	Is there any process to measure?
QNA3	Are there measurement standards?

Based on research criteria in table 3, authors define purposes of SLR research. The criteria can be used to form research question. Question of research is about "AES Algorithm for Data Sharing Encryption On Cloud Computing". Research activity needs to be done in order to find relevant paper with high trusted quality to answer the question. Authors did the research in 2nd March 2020. From the activity, table 4 is the result of paper search.

Table 4. Result of Paper Search in Digital Library

Database Journal	Result Paper
IEEE Explore	22
ScienceDirect	70
Tandfonline	30
Total	122

Table 4 shows research result for “AES Algorithm for Data Sharing Encryption On Cloud Computing”. There are 122 journals for authors’ analysis

III. Research Result and Discussion

Authors create step by step for keyword result. The keyword is obtained based on data encryption in cloud storage.

A. Data Encryption with AES on Cloud Computing Comparison

Authors are interested and encouraged to do SLR because of a need to secure cloud computing. So, this paper resolves problem on cloud data encryption for data sharing. To resolve the problem, authors utilize an approach by determining relevant theme and finding related paper on theme. All collected data are from 3 digital libraries from 2014 to 2019. Authors found related paper regarding

data encryption (30%) and data sharing on cloud computing (10%). SLR comparison for reviewing data encryption on cloud computing can be seen in table 5.

Table 5. SLR Data Encryption on Cloud Computing

No.	Description	Data Encryption AES	Data Encryption AES Cloud Computing
1.	Research Question	Up to 10	Only 2
2.	Search Strategy Paper	Keyword based on authors and keyword theme scope	Keyword specific subject scope
3.	Model of String Keyword	5 Model of string	1 Model of string
4.	Resource to be Search Paper	4 Library Digital online	2 Library Digital online
5.	Paper Selection Criteria	4 in unreliable criteria 4 in reliable criteria 5 in quality assessment 3 in quantity assessment	3 in unreliable criteria 3 in reliable criteria 2 in quality assessment 1 in quantity assessment

Table 5 explains relevant paper finding based on determined criteria. That should be done to get suitable paper for analysis.

B. Data Sources for Selection

Authors utilize 3 trusted digital libraries named "Science Direct", "IEEE Explore" and "Tandfonline". Web address for those libraries respectively are sciencedirect.com and ieeexplore.ieee.org. Paper search was done in 2nd March of 2020. Keywords for searching are "AES Algorithm", "Algorithm Data Sharing", "AES Algorithm Data Sharing Encryption Cloud Computing". All keywords are lowercase with space and without quotation mark.

Authors classify those keywords into 3 parts. First part is called Q1 consisting of keywords (AES Algorithm). Second part is called Q2 containing keywords (Algorithm Data Sharing). Third part is called Q3 having keywords (AES Algorithm Data Sharing Encryption Cloud Computing). Authors only use defined keywords and no filter is applied, except span of year to narrow search process.

C. SLR Result

SLR discussion is about "AES Algorithm for Data Sharing Encryption On Cloud Computing". Question on SLR is done for 2014 to 2019. Table 6 is result of paper search on the latest research about authors' question.

Table 6. Search Keyword Result on Digital Library

Digital Library	Keyword	Result Search
IEEE	AES Algorithm	1404
	Algorithm Data Sharing	54
	AES Algorithm Data Sharing Encryption Cloud Computing	22
ScienceDirect	AES Algorithm	969
	Algorithm Data Sharing	345
	AES Algorithm Data Sharing Encryption Cloud Computing	70
Tandfonline	AES Algorithm	2689
	Algorithm Data Sharing	736
	AES Algorithm Data Sharing Encryption Cloud Computing	30

Table 6 is keyword result to answer authors' question. From table 6, there is still a chance to research on "AES Algorithm for Data Sharing Encryption On Cloud Computing" for data sharing encryption. Figure 2 depicts better view for good analysis.

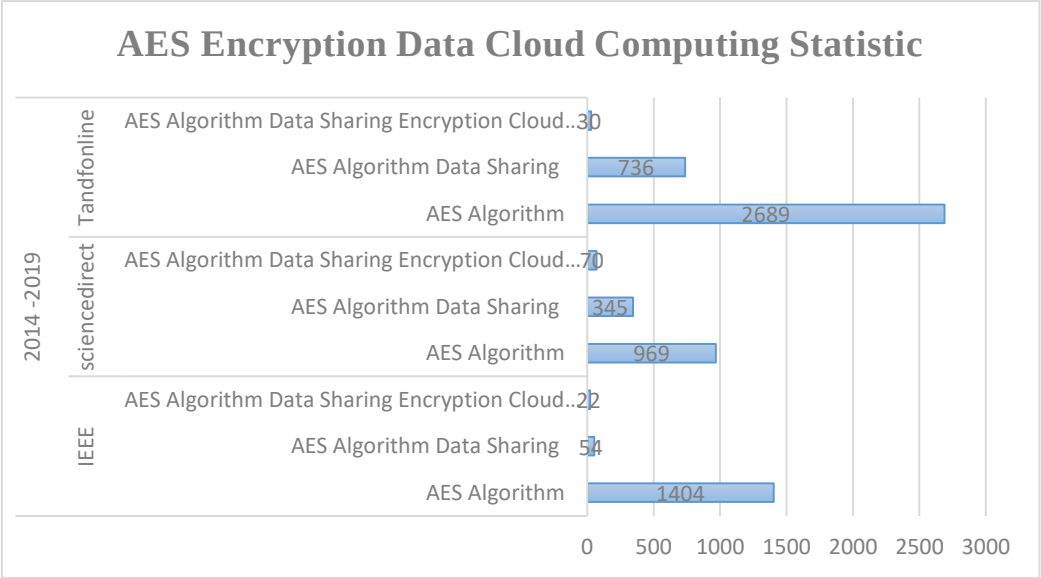


Fig 2. SLR Statistic of AES Encryption on Cloud Computing

D. Encryption Algorithm

To prevent any intruder activity, there is a proposed data security for cloud called encryption [33], [34]. Besides functioning as data security, encryption also concentrates on data transfer [35]. For real-time, all encryption ways are useful, but each encryption has no same pattern to encrypt [13], [36], [37]. For example, Contributory Broadcast Encryption (ConBE) allows a sender to broadcast to any member but require trusted key to decrypt [19], [8], [22]. Group Key Agreement (GKA) protocols enable members to transact common key via internet so that only few members can decrypt data encrypted by shared key [13], [37], [38]. To do that, a sender looking at the public group key can limit decryption to limited members of his choice [36], [39]. Encryption algorithm can be seen in figure 2.

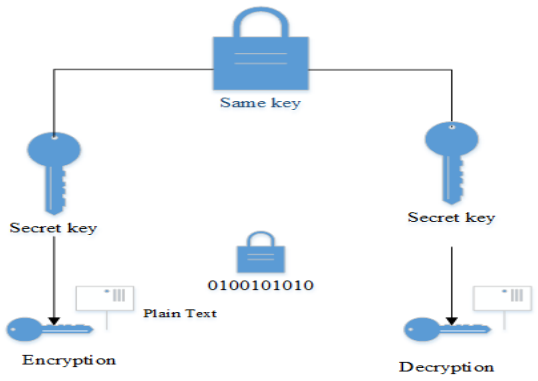


Fig 3. Encryption algorithm [17]

E. Data Sharing on Cloud Computing

Cloud provider has 2 dominant services named data and information services for users [40], [41]. Security on those services creates primary challenges in cloud [42], [43]. Currently, cloud storage is frequently used for data sharing (photo, video, document) in social media [4], [44]. Yet, data sharing in cloud brings another problem for data leakage [10], [45]. To drive the problem, encryption may be applied to each user's data before and after uploading to cloud [13], [7], [46]. Figure 3 describes data sharing.

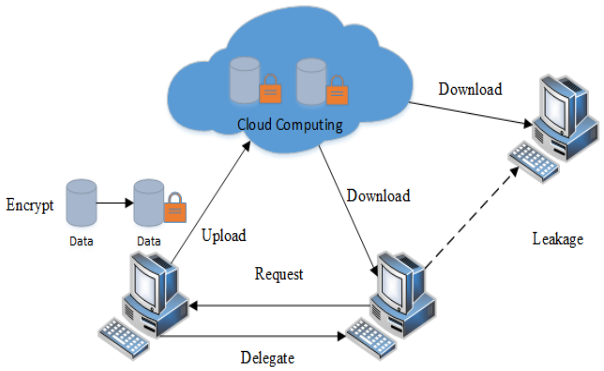
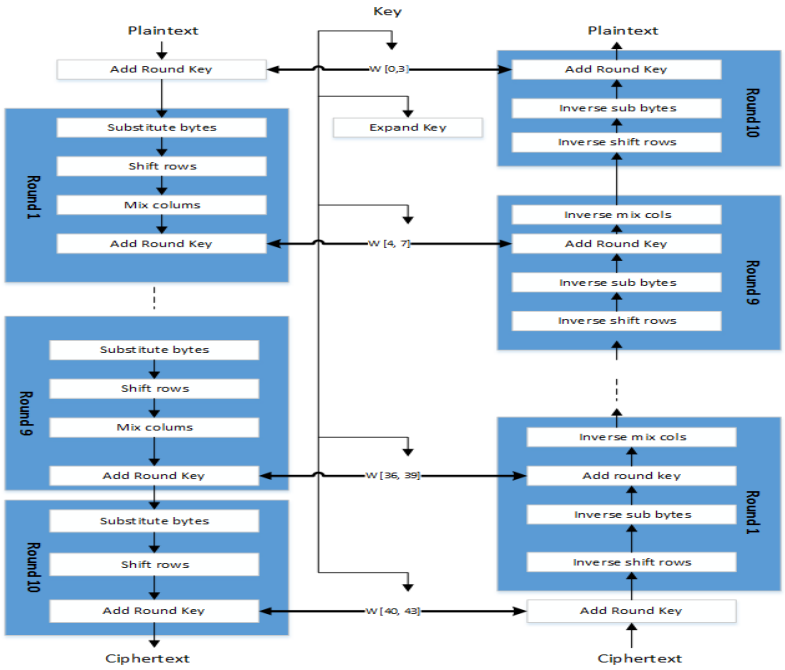


Fig 4. Data Sharing Cloud Computing [42]

F. AES Alogrithm

AES algorithm is commonly used for encrypting data [17]. The algorithm is chosen because it is more secure than IDES or 3DES algorithm. AES itself can be described as symmetrical block encryption. All operations inside the algorithm work on 8-bit or more. Cipher block will take plaintext with size 128-bit, 192-bit and 256-bit [38], [47]. Key for encrypting and decrypting is depicted as square matrix of bytes [48], [49]. Figure 4 explains process of AES encryption.



(a) Encryption (b) Decryption

Fig 5. AES Encryption Process [36]

The algorithm supports 128-bit block and 128-bit key, 192-bit key and 256-bit key. It uses 10 series for 128-bit key, 12 series for 192-bit key, 14 series for 256-bit key [50] . For example, each series may use different key series for 128-bit, then it is called real key for AES [8].

IV. Conclusion and Future Work

Based on keyword for searching relevant paper, authors get interesting result. AES algorithm to secure data sharing on cloud can be explored deeply and then well implemented. From what authors believed on 3 trusted libraries, only few papers discuss on AES algorithm for cloud data security. Those papers discussed that data security on cloud not only could impact to data authenticity, but also could prevent any unauthorized person. The use of SLR can help to get better suggestion for further research. In addition, it may contribute to new science in future.

Acknowledgment

The author would like to thank the Department of Computer Engineering, Universitas Wiralodra because for support of this research.

References

[1] B. S. Rawal, "Proxy re-encryption architect for storing and sharing of cloud contents," *International Journal of Parallel, Emergent and Distributed Systems*, vol. 5760, pp. 1–17, Mar. 2018.

[2] J. Gong, Y. Xu, and X. Zhao, "A Privacy-preserving Image Retrieval Method Based on Improved BoVW Model in Cloud Environment," *IETE Technical Review*, vol. 35, no. sup1, pp. 76–84, Dec. 2018.

[3] M. Joshi, K. Joshi, and T. Finin, "Attribute Based Encryption for Secure Access to Cloud Based EHR Systems," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018, vol. 2018–July, pp. 932–935.

[4] D. Pei, X. Guo, and J. Zhang, "A video encryption service based on cloud computing," in *2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC)*, 2017, pp. 167–171.

[5] L. Tawalbeh, N. S. Darwazeh, R. S. Al-Qassas, and F. AlDosari, "A secure cloud computing model based on data classification," *Procedia Computer Science*, vol. 52, no. 1, pp. 1153–1158, 2015.

[6] A. Bhardwaj, G. V. B. Subrahmanyam, V. Avasthi, and H. Sastry, "Security Algorithms for Cloud Computing," *Procedia Computer Science*, vol. 85, no. Cms, pp. 535–542, 2016.

[7] A. Bentajer, M. Hedabou, K. Abouelmehdi, Z. Igarramen, and S. El Fezazi, "An IBE-based design for assured deletion in cloud storage," *Cryptologia*, vol. 43, no. 3, pp. 254–265, 2019.

[8] K. M. Akhil, M. P. Kumar, and B. R. Pushpa, "Enhanced cloud data security using AES algorithm," in *2017 International Conference on Intelligent Computing and Control (I2C2)*, 2017, vol. 2018–Janua, pp. 1–5.

[9] N. Surv, B. Wanve, R. Kamble, S. Patil, and J. Katti, "Framework for client side AES encryption technique in cloud computing," *Souvenir of the 2015 IEEE International Advance Computing Conference, IACC 2015*, pp. 525–528, 2015.

[10] S. Amamou, Z. Trifa, and M. Khmakhem, "Data protection in cloud computing: A Survey of the State-of-Art," *Procedia Computer Science*, vol. 159, pp. 155–161, 2019.

[11] M. D. Boomija, "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)*, 2016, pp. 652–655.

[12] N. Sehgal, Y. Xiong, W. Mulia, S. Sohoni, D. Fritz, and J. Acken, "A Cross Section of the Issues and Research Activities Related to Both Information Security and Cloud Computing," *IETE Technical Review*, vol. 28, no. 4, p. 279, 2011.

[13] B. Cui, Z. Liu, and L. Wang, "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage," *IEEE Transactions on Computers*, vol. 65, no. 8, pp. 2374–2385, Aug. 2016.

[14] Salma, R. F. Olanrewaju, K. Abdullah, Rusmala, and H. Darwis, "Enhancing Cloud Data Security Using Hybrid of Advanced Encryption Standard and Blowfish Encryption Algorithms," in *2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT)*, 2018, pp. 18–23.

[15] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," in *2017 International Conference on Engineering and Technology (ICET)*, 2017, vol. 2018–Janua, pp. 1–7.

[16] C. Sur, Y. Park, and K. H. Rhee, "An efficient and secure navigation protocol based on vehicular cloud," *International Journal of Computer Mathematics*, vol. 93, no. 2, pp. 325–344, Feb. 2016.

[17] Y. Yuan, Y. Yang, L. Wu, and X. Zhang, "A High Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation," in *2018 IEEE International Conference on*

Electron Devices and Solid State Circuits (EDSSC), 2018, pp. 1–2.

[18] S. A. Pitchay, W. A. A. Alhiagem, F. Ridzuan, and M. M. Saudi, "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)*, 2015, pp. 201–205.

[19] A. S. Babrahem and M. M. Monowar, "Preserving confidentiality and privacy of the patient's EHR using the OrBAC and AES in cloud environment*," *International Journal of Computers and Applications*, vol. 7074, 2018.

[20] P. Sivakumar, M. NandhaKumar, R. Jayaraj, and A. S. Kumaran, "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)*, 2019, pp. 1–5.

[21] S. Alonso-Monsalve, F. García-Carballeira, and A. Calderón, "A heterogeneous mobile cloud computing model for hybrid clouds," *Future Generation Computer Systems*, vol. 87, pp. 651–666, 2018.

[22] J. Domingo-Ferrer, O. Farràs, J. Ribes-González, and D. Sánchez, "Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges," *Computer Communications*, vol. 140–141, no. December 2018, pp. 38–60, May 2019.

[23] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," *Computer Science Review*, vol. 33, pp. 1–48, 2019.

[24] N. Mohammed and N. Ibrahim, "Implementation of new secure encryption technique for cloud computing," *ICCISTA 2019 - IEEE International Conference on Computing and Information Science and Technology and their Applications 2019*, pp. 1–5, 2019.

[25] S. Ojha and V. Rajput, "AES and MD5 based secure authentication in cloud computing," *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017*, pp. 856–860, 2017.

[26] N. Shimbre and P. Deshpande, "Enhancing distributed data storage security for cloud computing using TPA and AES algorithm," *Proceedings - 1st International Conference on Computing, Communication, Control and Automation, ICCUBEA 2015*, pp. 35–39, 2015.

[27] Fitroh and D. N. Utama, "Synthesizing a soft system methodology use in information systems research field: A systematic review," *2017 5th International Conference on Information and Communication Technology, ICoIC7 2017*, vol. 0, no. c, pp. 1–4, 2017.

[28] C. Soledad, "Methodology for Systematic Literature Review applied to Engineering and Education," *2018 IEEE Global Engineering Education Conference (EDUCON)*, pp. 1370–1379, 2018.

[29] P. Sharma and J. Singh, "Systematic Literature Review on Software Effort Estimation Using Machine Learning Approaches," in *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)*, 2017, pp. 43–47.

[30] T. Hidayat, Y. Azzery, and R. Mahardiko, "Load Balancing Network by using Round Robin Algorithm: A Systematic Literature Review," *Jurnal Online Informatika*, vol. 4, no. 2, pp. 85–89, 2019.

[31] N. A. Salleh, H. Hussin, M. A. Suhaimi, and A. Md Ali, "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, ICT4M 2018*, pp. 278–284, 2018.

[32] P. Rosati, G. Fox, D. Kenny, and T. Lynn, "Quantifying the Financial Value of Cloud Investments: A Systematic Literature Review," *Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom*, vol. 2017–Decem, pp. 194–201, 2017.

[33] K.-L. Tsai, F.-Y. Leu, and S.-H. Tsai, "Data Encryption Method Using Environmental Secret Key with Server Assistance," *Intelligent Automation & Soft Computing*, vol. 22, no. 3, pp. 423–430, Jul. 2016.

[34] M. I. S. Reddy and A. P. S. Kumar, "Secured Data Transmission Using Wavelet Based

Steganography and Cryptography by Using AES Algorithm," *Procedia Computer Science*, vol. 85, no. Cms, pp. 62–69, 2016.

[35] J. C. S. do. Anjos *et al.*, "Fast-Sec: an approach to secure Big Data processing in the cloud," *International Journal of Parallel, Emergent and Distributed Systems*, vol. 34, no. 3, pp. 272–287, 2019.

[36] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, O. Farras, and J. A. Manjon, "Contributory broadcast encryption with efficient encryption and short ciphertexts," *IEEE Transactions on Computers*, vol. 65, no. 2, pp. 466–479, 2016.

[37] L. Yu, D. Zhang, L. Wu, S. Xie, D. Su, and X. Wang, "AES Design Improvements Towards Information Security Considering Scan Attack," *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, pp. 322–326, 2018.

[38] V. Dilna and C. Babu, "Area optimized and high throughput AES algorithm based on permutation data scramble approach," *International Conference on Electrical, Electronics, and Optimization Techniques, ICEEOT 2016*, pp. 3056–3060, 2016.

[39] W. Al Etaiwi and S. Hraiz, "Structured encryption algorithm for text cryptography," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 21, no. 7–8, pp. 1559–1572, 2018.

[40] B.-H. Lee, E. K. Dewi, and M. F. Wajdi, "Data security in cloud computing using AES under HEROKU cloud," in *2018 27th Wireless and Optical Communication Conference (WOCC)*, 2018, pp. 1–5.

[41] N. Agarwal, A. Rana, and J. P. Pandey, "Guarded dual authentication based DRM with resurgence dynamic encryption techniques," *Enterprise Information Systems*, vol. 13, no. 3, pp. 257–280, 2019.

[42] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 6, pp. 996–1010, Nov. 2019.

[43] M. Hossain, R. Khan, S. Al Noor, and R. Hasan, "Jugo: A generic architecture for composite cloud as a service," *IEEE International Conference on Cloud Computing, CLOUD*, pp. 806–809, 2017.

[44] M. Morales-Sandoval, A. K. Vega-Castillo, and A. Diaz-Perez, "A Secure Scheme for Storage, Retrieval, and Sharing of Digital Documents in Cloud Computing Using Attribute-Based Encryption on Mobile Devices," *Information Security Journal: A Global Perspective*, vol. 23, no. 1–2, pp. 22–31, Jan. 2014.

[45] M. Bahrami and M. Singhal, "A light-weight permutation based method for data privacy in mobile cloud computing," *Proceedings - 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2015*, pp. 189–196, 2015.

[46] R. Dowsley, A. Michalas, M. Nagel, and N. Paladi, "A survey on design and implementation of protected searchable data in the cloud," *Computer Science Review*, vol. 26, pp. 17–30, Nov. 2017.

[47] P. Kumar and S. B. Rana, "Development of modified AES algorithm for data security," *Optik*, vol. 127, no. 4, pp. 2341–2345, Feb. 2016.

[48] Ritambhara, A. Gupta, and M. Jaiswal, "An enhanced AES algorithm using cascading method on 400 bits key size used in enhancing the safety of next generation internet of things (IOT)," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, 2017, pp. 422–427.

[49] S. Madhavapandian and P. MaruthuPandi, "FPGA implementation of highly scalable AES algorithm using modified mix column with gate replacement technique for security application in TCP/IP," *Microprocessors and Microsystems*, vol. 73, p. 102972, 2020.

[50] Y. Liu, W. Gong, and W. Fan, "Application of AES and RSA Hybrid Algorithm in E-mail," in *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, 2018, pp. 701–703.