44_CITSM2023.pdf

by aida.fitriyani@gmail.com 1

Submission date: 02-Sep-2024 12:45PM (UTC+0800)
Submission ID: 2442943792
File name: 44_CITSM2023.pdf (484.73K)
Word count: 4140
Character count: 22095

Systematic Literature Review: Key Management Service For Securing Encryption Key

1st Aries Susanto
Department of Information Systems
UIN Syarif Hidayatullah Jakarta
South Tangerang, Indonesia
ariesshi@uinjkt.ac.id

2nd Ahnaf Hadi Fathulloh
Department of Digital and Analytics
Mitra Solusi Telematika
Jakarta, Indonesia
ahnafhadi@gmail.com

3rd Nuryasin
Department of Information Systems
UIN Syarif Hidayatullah Jakarta
South Tangerang, Indonesia
nuryasin@uinjkt.ac.id

4th Aida Fitriyani
Department of Informatics
Bhayangkara University Jakarta
Jakarta, Indonesia
aida.fitriyani@gmail.com

***Abstract*—This paper utilizes the Systematic Literature Review (SLR) method to investigate and analyze the key management services employed for securing encryption keys, as well as the benefits of these methods. The research findings support the conclusion that SLR is an effective approach for studying user acceptability of widely explored E-Wallet apps, wireless sensor networks (WSNs), and key generation centers (KGCs). Data regarding the names of encryption keys was collected during the period from 2019 to 2023. Key Management Systems (KMS) are extensively utilized to comprehend and evaluate the factors influencing the Key Management Service for Securing Encryption Key. The analysis focuses on four main topics: the names of encryption keys, methods used for encryption, statistical methods, and the Key Management Service. Comparative analysis emerges as the most commonly employed statistical approach.**

Keywords*— *Key Management Service, Encryption Key, Systematic Literature Review

I. Introduction

In an increasingly digitally connected world, data security is a major concern. One way to protect the confidentiality and integrity of data is by using encryption. Encryption involves converting text or information into a form that cannot be read, except by using the right encryption key. However, strong encryption can only be implemented if encryption key management is done well. Encryption key management involves all aspects related to the generation, storage, distribution, and use of encryption keys used in the process of encrypting and decrypting data. This is where Key Management Service (KMS) plays an important role. KMS is a service specifically designed to manage encryption keys in a secure and efficient manner. The main task of a KMS is to provide facilities to generate, store, change, and distribute encryption keys to authorized users.

One of the main objectives of KMS is to protect encryption keys from security threats. The KMS uses strong methods and algorithms to protect the keys while in storage and while being transferred over the network. This includes the use of advanced encryption techniques, strict access controls, and physical security measures to protect the keys from theft or unauthorized manipulation. In addition, KMS also provides ease of use of encryption keys. The KMS ensures that encryption keys are available when needed and accessed by authorized entities. This includes key lifecycle management, such as key generation, rotation, and destruction in accordance with established security policies. In a business context, KMS is essential for maintaining the confidentiality and integrity of sensitive data. For example, organizations that store customer data, financial data, or industry confidential data, should implement a KMS to ensure that encryption keys are properly protected and managed.

Overall, Key Management Service (KMS) plays a crucial role in data security through effective encryption key management. By adopting a KMS, organizations can ensure that encryption keys are kept secure, available, and used appropriately. This is an important step in maintaining confidentiality, integrity, and trust in the secure transmission and storage of data in the ever-evolving digital world.

II. Methodology

The stages in this research refer to research that has been done previously in this Systematic Literature Review (SLR).

A. Object of research

The object of this research is Key Management Service (KMS) for encryption key security. This research was chosen because data security is one of the crucial aspects in an increasingly digitally connected world. In that context, encryption is a commonly used method to protect data confidentiality and integrity. However, strong encryption can only be achieved if encryption key management is done well. KMS is a system or service designed to manage encryption keys in a secure and efficient manner. Encryption keys are key components in the process of encrypting and decrypting data, and are important for maintaining the confidentiality of encrypted data. Therefore, the object of this research is KMS as a solution in effective encryption key management. This research is important because KMS has a crucial role in maintaining the security of sensitive data in various fields, including business, industry, and the public sector. By examining and understanding more about KMS, this research can provide valuable insights in the development of a more robust and efficient information security system. Moreover, with compliance requirements becoming increasingly stringent and changing frequently, research on KMS can also help organizations meet applicable security and compliance standards, such as GDPR, HIPAA, or other financial sector regulations. In the context of this research, the implementation, reliability, efficiency, and security of the KMS can be analyzed to identify strengths, weaknesses, and potential improvements. Thus, research on KMS for encryption key security makes an important contribution to the development of stronger information security systems and better data protection.

B. Research Method

The stages in the Systematic Literature Review consist of 3 stages of research consisting of the planning stage (planning a review), conducting (conducting a review) and reporting review. The research stages can be seen in the following figure:

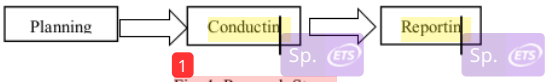

Fig. 1. Research Stages

1) Research Question

A statement of curiosity about a topic that is systematically obtained. The questions used in this research include:

- RQ1: How can KMS overcome the challenges of efficient and scalable encryption key management in complex and large environments?
- RQ2: How can the KMS provide transparency and auditability of encryption key-related activities to support compliance and suspicious activity detection?
- RQ3: How can the KMS address the risk of encryption key loss and provide effective disaster recovery mechanisms to maintain business continuity and data integrity?
- RQ4: How can the KMS address the challenges of facilitating secure collaboration between entities sharing encryption keys, including aspects such as key distribution, setting access rights, and managing security policies?

2) Search process

After formulating the problems and questions that will be used in the research, the next stage is to search for relevant journal papers. The process of searching for journal papers in this study is by accessing the site https://scholar.google.com

3) Inclusion and Exclusion Criteria

This step is completed to determine whether or not the data found is feasible to use in SLR research. a feasibility assessment of particular journal articles that will be used as references, such as:

- Journal papers published in 2019-2023.
- Journal papers are obtained from the site https://scholar.google.com
- The journal should focus on evaluating user satisfaction key management service for securing encryption key.

4) Quality Assessment

This step is completed to determine whether or not the data found is feasible to use in SLR research. a feasibility assessment of particular journal articles that will be used as references such as:

- QA1: Are journal papers published in 2019-2023?
- QA2: Does the journal have adequate citations and references from previous research relevant to the topic of evaluating e-wallet application user satisfaction?
- QA3: Does the journal use appropriate and valid research methods to evaluate user satisfaction with e-wallet applications.

5) Data Collection

- Check out the website at scholar.google.com
- Type the search term "evaluation of user satisfaction with e-wallet applications
- Because the search results have not been filtered, they are still quite wide. To receive the most recent five years of study, enter 2019–2023, then click the search button.

6) Data Analysis

The selected search results will be used to draw conclusions based on descriptions drawn from logical facts that will address the earlier raised queries.

7) Documentation

At this point, the author presents the study findings in a planned manner in a paper that will be published.

III. Result And Discussion

A. Search Process Results and Inclusion and Exclusion Criteria

According to the findings of the search process and inclusion and exclusion criteria, only journal publications pertaining to Key Management Service For Securing Encryption Key were chosen with the criterion of 2019 to 2023. Cryptography Key In addition, as shown in Table I, the journal papers are divided into categories according to the kind of journal.

TABLE I. Searching Proccess Results

No.	Journal Type	Year	Amount
1	IEEE Communications Surveys Tutorials	2019	
2	IEEE Transactions on Dependable and Secure Computing	2021	2
3	E Access	2019	6
4	Concurrency and Computation: Practice and Experience	2019	
5	nputer Communications	2021	`
6	Proceedings of the ACM Conference on Computer and Communications Security	2019	2
7	Wireless Personal Communications	2019	
8	Hoc Networks	2019	2
9	International Conference on Parallel, Distributed and Grid Compu	2020	
10	IEEE Transactions on Cloud Computing	2021	
11	E Internet of Things Journal	2019	
12	IEEE Transactions on Industrial Informatics	2020	
13	Lecture Notes of the Institute for Computer Sciences, Social-Informatics and	2019	

	Telecommunications Engineering, LNICST		
14	IOP Conference Series: Materials Science and Engineering	2019	
15	Proceedings of the 14th EuroSys Conference	2019	
16	International Journal of Communication Systems	2019	
17	IEEE Networking Letters	2019	
18	Advances in Engineering Research	2020	
19	IEEE Transactions on Vehicular Technology	2020	
20	Neural Computing and Applications	2021	
21	Optik	2021	
22	Pusion: Practice and Applications	2021	
23	International Journal of Advanced Intelligence Paradigms	2021	
24	Ad Hoc Networks	2021	2
25	Neural Processing Letters	2022	
26	Emerging Science Journal	2021	
27	Lecture Notes in Networks and Systems	2021	
28	Multimedia Tools and Applications	2021	
29	IEEE Systems Journal	2022	
30	Optics and Lasers in Engineering	2021	
31	Information Sciences	2019	

Quality Assessment Results

The results of the Quality Assessment can be seen in Table II.

TABLE II. QUALITY ASSESSMENT RESULTS

No.	Author	Year	QA1	QA2	QA3	Result
1	Galinina, Olga Andreev, Sergey	2020	Yes	Yes	Yes	√
2	Amrita Ghosal & Mauro Conti	2019	Yes	Yes	Yes	√
3	Xiaokang Hu, Jian Li	2019	Yes	Yes	Yes	√
4	Marcus De Ree & Georgios Manta	2019	Yes	Yes	Yes	√
5	R. Velumadhava RaoK. Selvamani1 S. Kanimozhi Annan	2019	Yes	Yes	Yes	√
6	Mingxin Ma, Student Member, IEEE, Guozhen Shi, and Fenghua **Li3**	2019	Yes	Yes	Yes	√
7	Marcus de Ree, Georgios Mantas, Jonathan Rodriguez, Ifiok E. Otung	2020	Yes	Yes	Yes	√
8	Stanislaw Jarecki, Hugo Krawczyk, Jason Resch	2019	Yes	Yes	Yes	√
9	Y. Harold Robinson · E. Golden Julie	2019	Yes	Yes	Yes	√
10	Yasmine Harbi a , Zibouda Aliouat a , Allaoua Refoufia , Saad Harous Abdelhak Boukerram	2019	Yes	Yes	Yes	√
11	Manoj Kumar Shukla, Ashwani Kumar Dubey, Divya Upadhyay	2002	Yes	Yes	Yes	√
12	Lei Zhang	2019	Yes	Yes	Yes	√
13	Waritsirichotedumrong , Yuma Inoshita	2019	Yes	Yes	Yes	√
14	Mohammad Wazid, Member, IEEE, Palak Bagga, Ashok Kumar Das	2019	Yes	Yes	Yes	√
15	Yasmine Harbi , Zibouda Aliouat , Allaoua Refoufia , Saad Harous , Abdelhak Boukerram	2019	Yes	Yes	Yes	√
16	Jing Wang, Libing Wu, Kim-Kwang Raymond Choo, Debiao He	2019	Yes	Yes	Yes	√
17	K. Hamsha(&) and G. S. Nagaraja	2019	Yes	Yes	Yes	√
18	K. Hamsha(&) and G. S. Nagaraja	2019	Yes	Yes	Yes	√
19	John S. Koh, Steven M. Bellovin, Jason Nieh	2019	Yes	Yes	Yes	√
20	Anwar GhaniKhwaja Mansoor	2019	Yes	Yes	Yes	√

	Shahid Mehmood Shehzad Ashraf Chaudhry Arif Ur Rahman Malik Najmus Saqib					
21	Dagang Li–y, Rong Du–, Yue Fu—, Man Ho Auz	2019	Yes	Yes	Yes	√
22	Tao Yu	2021	Yes	Yes	Yes	√
23	Jolfaei, Alireza Kant, shna	2020	Yes	Yes	Yes	√
24	Zhuo Ma, Junwei Zhang, Yongzhen Guo, Yang Liu, Ximeng Liu, Wei	2020	Yes	Yes	Yes	√
25	Varun Prabhakaran,Ashokkumar Kulandasamy	2021	Yes	Yes	Yes	√
26	Mahdi Shariatzadeh, Mohammad Javad Rostami , Mahdi khari	2021	Yes	Yes	Yes	√
27	Shibin David, Andrew , K. Martin Sagayam, Ahmed A. Elngar	2021	Yes	Yes	Yes	√
28	Kiran Mary Matthew, Abdul Quadir Muhammed and Vijayakumar darajan	2019	Yes	Yes	Yes	√
29	Osama A. Kashan a,, Rami Ahmad b, Nour M. ajah c	2021	Yes	Yes	Yes	√
30	Guipeng Zhang · Haoran Xie Zhenguo Yang Xiaohui Tao· Wenyin Liu	2021	Yes	Yes	Yes	√
31	Maitri Patel , Rajan Patel	2021	Yes	Yes	Yes	√
32	Yuan Zhang,	2021	Yes	Yes	Yes	√
33	Heqing Song , Jifei Li , And ng Li	2021	Yes	Yes	Yes	√
34	Pradeep Kumar Singh · Sławomir T. Wierzcho´n Sudeep Tanwar · Maria Ganzha · Joel J. P. C. Rodrigues	2020	Yes	Yes	Yes	√
35	R ing Li1	2019	Yes	Yes	Yes	√
36	Kwame Opuni-Boachie Obour Agyekum , Qi Xia , Emmanuel Boateng Sifah , Christian Nii Aflah Cobblah , Hu Xia , and Jianbin	2021	Yes	Yes	Yes	√
37	Sui, Liansheng Pang, Zhi Cheng, Ying Cheng, Yin Xiao, Zhaolin	2021	Yes	Yes	Yes	√
38	Yuling Luo, Xue Ouyang1, Junxiu Liu	2019	Yes	Yes	Yes	√
39	Xuqi Wang , Xiangguo heng	2019	Yes	Yes	Yes	√
40	Hongbo Li a , Qiong Huang a , Jian Shen b , Guomin Yang c , Willy Susilo c	2019	Yes	Yes	Yes	√

C. Data Analysis

- RQ1: How does key management service forr securing encryption key?
  Based on research done in 2019–2023 about kKey Management Service for Securing Encryption Key, the answers to Research Question 1 (RQ1) led to the development of several applications for encryption keys. Cryptography Key. The outcomes are shown in Table III.

TABLE III. Encryption Key

No.	Encryption Key	Paper	Amount
1	Key Distribution Server (KDS), key hierarchy (LKH)	5	
2	key management	9	

	(MTPKM)		
3	Keyless SSL	3	
4	wireless sensor networks (WSNs)	10 20	2
5		8 2	
6	Advanced Metering Infrastructure (AMI)	2	
7	Key generation center (KGC)	6 17	2
8	AKM-IoV	14	
9	Advanced Encryption Standard (AES)	26	
10	VANET	24	
11	HIPAA's (Health Insurance Portability and Accountability Act)	27	
12	CK	30	
13	EVKAKSE	39	
14	CPA	35	
15	Cloud Secure Storage Mechanism	33	
16	SPADE	32	
17	IIBES	31	
18	SHA-512	38	

- RQ2: What methods are used for key management services to secure encryption keys?
  According to the findings of Research Question 2 (RQ2), it is more prevalent to utilize WSN-based IoT and Key Management Systems (KMS) to examine user acceptance of encryption keys based on research done by in 2019–2023, as indicated in Table IV.

TABLE IV. METHODS

No.	Encryption Key	Paper	Amount
1	Key Hierarchy (LKH)	5 31	2
2	Software Guard Extensions (SGX) and QuickAssist Technology (QAT).	3	1
3	WSN-based IoT	6 10 14 15 20 29 36	7
4	Key Management Systems (KMS)	8 2 12 16 17 27 39	7
5	PGP and S/MIME	19 39	2
6	DB-KMM	24	1

- RQ3: What are the advantages of the method used to analyze the acceptance of the benefits of using Encryption Key on techno y.
  WSN-based IoT refers to wireless sensor networks (WNS) used in the Internet of Things (IoT). In this context, Key Management Systems (KMS) are systems or mechanisms used to manage and secure encryption keys in a WSN-based environment. Encryption keys are used to protect the confidentiality of data transmitted over the wireless sensor network. The link between WSN-based IoT, Key Management Systems (KMS), and Key Management Service (KMS) in the context of encryption key security lies in the use of KMS as a solution for managing and maintaining encryption key security in WSN-based IoT. In a connected and complex environment like IoT, protection of encryption keys is crucial to prevent unauthorized access and protect the confidentiality of data transmitted over wireless sensor networks. Using KMS, organizations can implement security policies, manage key lifecycles, and ensure compliance with applicable security and regulatory requirements, thereby strengthening encryption key security in WSN-based IoT.
- RQ4: What statistical methods are used to analyze user acceptance of ewallet applications?
  From the results of Research Question 4 (RQ4) it evaluate the popularity of e-wallet programs among users?
  According to the findings of Research Question 4 (RQ4), Comparative analysis is more prevalent among the statistical techniques used to study the Key Management Service For Securing Encryption Key in 2019–2023. Using comparative study, encryption key is more prevalent in 2019–2023.

TABLE V. STATISTICAL METHODS

No.	Statistical Methods	Paper	Amount
1	Artificial Neural Network	1,23	2
2	Survei, Comparative analysis	2,4	2
3	Deskriptif, Comparative analysis	5,19	2
4	Comparative analysis	6, 8, 9, 10, 12, 14, 16, 17, 18, 20, 24, 26, 27, 29, 30, 32, 33, 34,35, 36, 37, 39, 40	23
5	Deep neural networks (DNNs), Comparative analysis	13	1
6	HSDL, Comparative analysis	25	1
14	Histogram Analysis, Correlation Analysis, Comparative Analyisi	38	1

IV. CONCLUSION

The SLR method can be used to find and research analyze key management services for securing encryption keys, and the benefits of the methods used. This conclusion can be drawn based on the findings of the research that has been done. When studying user acceptability of the most explored E-Wallet apps, wireless sensor networks (WSNs) and key generation centers (KGC), information on the names of encryption keys is collected. This research was done in 2019–2023. Key Management Systems (KMS), which are used to understand and evaluate what influences the Key Management Service for Securing Encryption Key, are more commonly utilized in the approach used to assess the Key

Management Service for four main topics, including the names of encryption keys, methods and statistical methods used to Encryption Key. Comparative analysis is the statistical approach that is used the most.

ACKNOWLEDGMENT

The author would like to thank various parties who have supported the author in completing this research as well as possible.

REFERENCES

[1] O. Galinina, S. Andreev, I. Conference, and D. Hutchison, *Internet of Things , Smart Spaces , and Next Generation*, vol. 1, no. 18. 2019.

[2] A. Ghosal and M. Conti, "Key Management Systems for Smart Grid Advanced Metering Infrastructure: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2831–2848, 2019.

[3] X. Hu *et al.*, "STYX: A Hierarchical Key Management System for Elastic Content Delivery Networks on Public Clouds," *IEEE Trans. Dependable Secur. Comput.*, vol. 18, no. 2, pp. 843–857, 2021.

[4] M. De Ree, G. Mantas, A. Radwan, S. Mumtaz, J. Rodriguez, and I. E. Otung, "Key Management for beyond 5G Mobile Small Cells: A Survey," *IEEE Access*, vol. 7, pp. 59200–59236, 2019.

[5] R. Velumadhava Rao, K. Selvamani, S. Kanimozhi, and A. Kannan, "Hierarchical group key management for secure data sharing in a cloud based environment," *Concurr. Comput. Pract. Exp.*, vol. 31, no. 12, pp. 1–16, 2019.

[6] M. Ma, G. Shi, and F. Li, "Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario," *IEEE Access*, vol. 7, no. c, pp. 34045–34059, 2019.

[7] M. de Ree, G. Mantas, J. Rodriguez, I. E. Otung, and C. Verikoukis, "DISTANT: DIStributed Trusted Authority-based key manageNT for beyond 5G wireless mobile small cells," *Comput. Commun.*, vol. 176, pp. 218–233, 2021.

[8] S. Jarecki, H. Krawczyk, and J. Resch, "Updatable oblivious key management for storage systems," *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 379–393, 2019.

[9] Y. Harold Robinson and E. Golden Julie, "MTPKM: Multipart Trust Based Public Key Management Technique to Reduce Security Vulnerability in Mobile Ad-Hoc Networks," *Wirel. Pers. Commun.*, vol. 109, no. 2, pp. 739–760, 2019.

[10] Y. Harbi, Z. Aliouat, A. Refoufi, S. Harous, and A. Bentaleb, "Enhanced authentication and key management scheme for securing data transmission in the internet of things," *Ad Hoc Networks*, vol. 94, p. 101948, 2019.

[11] M. K. Shukla, A. K. Dubey, D. Upadhyay, and B. Novikov, "Group key management in cloud for shared media sanitization," *PDGC 2020 - 2020 6th Int. Conf. Parallel, Distrib. Grid Comput.*, pp. 117–120, 2020.

[12] L. Zhang, "Key Management Scheme for Secure Channel Establishment in Fog Computing," *IEEE Trans. Cloud Comput.*, vol. 9, no. 3, pp. 1117–1128, 2021.

[13] W. Sirichotedumrong, Y. Kinoshita, and H. Kiya, "Pixel-Based Image Encryption without Key Management for Privacy-Preserving Deep Neural Networks," *IEEE Access*, vol. 7, no. Ml, pp. 177844–177855, 2019.

[14] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "AKM-IoV: Authenticated Key Management Protocol in Fog Computing-Based Internet of Vehicles Deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8804–8817, 2019.

[15] S. Mesmoudi, B. Benadda, and A. Mesmoudi, "SKWN: Smart and dynamic key management scheme for wireless sensor networks," *Int. J. Commun. Syst.*, vol. 32, no. 7, pp. 1–23, 2019.

[16] J. Wang, L. Wu, K. K. R. Choo, and D. He, "Blockchain-Based Anonymous Authentication with Key Management for Smart Grid Edge Computing Infrastructure," *IEEE Trans. Ind. Informatics*, vol. 16, no. 3, pp. 1984–1992, 2020.

[17] K. Hamsha and G. S. Nagaraja, *Threshold Cryptography Based Light Weight Key Management Technique for Hierarchical WSNs*, vol. 276. Springer International Publishing, 2019.

[18] S. Yan, "Research on Implementation Method of Key Management Based on Data Encryption Technology," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 677, no. 4, 2019.

[19] J. S. Koh, S. M. Bellovin, and J. Nieh, "Why Joanie can encrypt: Easy email encryption with easy key management," *Proc. 14th EuroSys Conf. 2019*, 2019.

[20] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, and M. Najmus Saqib, "Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key," *Int. J. Commun. Syst.*, vol. 32, no. 16, pp. 1–18, 2019.

[21] Nurbojatmiko, A. Susanto, E. Shobariah. "Assessment of ISMS based on standard ISO/IEC 27001: 2013 at Diskominfo Depok City." In International Conference on Cyber and IT Service Management (CITSM), pp. 1-6, April 2016.

[22] A.Susanto, L. Latifah, Nuryasin, A. Fitriyani. "Decision support systems design on sharia financing using Yager's fuzzy decision model." In International Conference on Cyber and IT Service Management (CITSM), pp. 1-4, August 2017.

[23] D. Li, R. Du, Y. Fu, and M. H. Au, "Meta-Key: A Secure Data-Sharing Protocol Under Blockchain-Based Decentralized Storage Architecture," *IEEE Netw. Lett.*, vol. 1, no. 1, pp. 30–33, 2019.

[24] T. Yu, *A two-station radio navigation method using the solution of redundant equation*, vol. 34, no. July. 2020.

[25] A. Jolfaei and K. Kant, "Privacy and Security of Connected Vehicles in Intelligent Transportation System," *Proc. - 49th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Networks - Suppl. Vol. DSN-S 2019*, pp. 9–10, 2019.

[26] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, and W. He, "An Efficient Decentralized Key Management Mechanism for VANET with Blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5836–5849, 2020.

[27] V. Prabhakaran and A. Kulandasamy, "Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection," *Neural Comput. Appl.*, vol. 5, 2021.

[28] M. Shariatzadeh, M. J. Rostami, and M. Eftekhari, "Proposing a novel Dynamic AES for image encryption using a chaotic map key management approach," *Optik (Stuttg).*, vol. 246, no. June, 2021.

[29] S. David, J. Andrew, K. Martin Sagayam, and A. A. Elngar, "Augmenting security for electronic patient health record (ePHR) monitoring system using cryptographic key management schemes," *Inf. Comput Pract. Appl.*, vol. 5, no. 2, pp. 51–61, 2021.

[30] K. M. Matthew, A. Q. Muhammed, and V. Varadaraja, "An improved key management scheme in cloud storage," *Int. J. Adv. Intell. Paradig.*, vol. 14, no. 3–4, pp. 197–203, 2019.

[31] O. A. Khashan, R. Ahmad, and N. M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks," *Ad Hoc Networks*, vol. 117, no. February, p. 102448, 2021.

[32] G. Zhang, H. Xie, Z. Yang, X. Tao, and W. Liu, "BDKM: A Blockchain-Based Secure Deduplication Scheme with Reliable Key Management," *Neural Process. Lett.*, vol. 54, no. 4, pp. 2657–2674, 2022.

[33] M. Patel and R. Patel, "Improved identity based encryption system (Ibes): A mechanism for eliminating the key-escrow problem," *Emerg. Sci. J.*, vol. 5, no. 1, pp. 77–84, 2021.

[34] Y. Zhang, C. Xu, N. Cheng, and X. Shen, "Secure Password-Protected Encryption Key for Deduplicated Cloud Storage Systems," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 4, pp. 2789–2806, 2022.

[35] H. Song, J. Li, and H. Li, "A Cloud Secure Storage Mechanism Based on Data Dispersion and Encryption," *IEEE Access*, vol. 9, pp. 63745–63751, 2021.

[36] R. Li, "Fingerprint-related chaotic image encryption scheme based on blockchain framework," *Multimed. Tools Appl.*, vol. 80, no. 20, pp. 30583–30603, 2021.

[37] K. O. B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia, and J. Gao, "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain," *IEEE Syst. J.*, vol. 16, no. 1, pp. 1685–1696, 2022.

[38] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems," *IEEE Access*, vol. 7, no. c, pp. 38507–38522, 2019.

[39] X. Wang, X. Cheng, and Y. Xie, "Efficient Verifiable Key-Aggregate Keyword Searchable Encryption for Data Sharing in Outsourcing Storage," *IEEE Access*, vol. 8, pp. 11732–11742, 2020.

[40] H. Li, Q. Huang, J. Shen, G. Yang, and W. Susilo, "Designated-server identity-based authenticated encryption with keyword search for encrypted emails," *Inf. Sci. (Ny).*, vol. 481, pp. 330–343, 2019.

44_CITSM2023.pdf

ORIGINALITY REPORT

42%	33%	39%	25%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Lisa Maharani, Yusuf Durachman, Suci Ratnawati. "Systematic Literature Review Method for Evaluation of User Experience on Ticket Booking Applications", 2021 9th International Conference on Cyber and IT Service Management (CITSM), 2021 Publication	4%
2	www.hindawi.com Internet Source	2%
3	dspace.dtu.ac.in:8080 Internet Source	1%
4	file.techscience.com Internet Source	1%
5	Jamuna S. Murthy, G. M. Siddesh, K. G. Srinivasa. "Cloud Security - Concepts, Applications and Practices", CRC Press, 2024 Publication	1%
6	Aries Susanto, Fazrin Al Banjari, Eva Khudzaeva, Aida Fitriyani. "Antecedents of Loyalty Formation on Mobile-based Travel	1%

Use", 2021 9th International Conference on Cyber and IT Service Management (CITSM), 2021
Publication

7	ejournal.uin-suska.ac.id Internet Source	1 %
8	Submitted to Napier University Student Paper	1 %
9	americaspg.com Internet Source	1 %
10	gala.gre.ac.uk Internet Source	1 %
11	Hao Ran Chi, Ayman Radwan. "Multi-Objective Optimization of Green Small Cell Allocation for IoT Applications in Smart City", IEEE Access, 2020 Publication	1 %
12	Submitted to Study Group Australia Student Paper	1 %
13	d197for5662m48.cloudfront.net Internet Source	1 %
14	dr.ntu.edu.sg Internet Source	1 %
15	qspace.qu.edu.qa Internet Source	1 %

16	Man Chun Chow, Maode Ma. "A lightweight traceable D2D authentication and key agreement scheme in 5G cellular networks", Computers & Electrical Engineering, 2021 Publication	1 %
17	Qingyang Zhang, Dongfang Sui, Jie Cui, Chengjie Gu, Hong Zhong. "Efficient Integrity Auditing Mechanism With Secure Deduplication for Blockchain Storage", IEEE Transactions on Computers, 2023 Publication	1 %
18	Yanjie Song, Zhiliang Zhu, Wei Zhang, Hai Yu, Yuli Zhao. "Efficient and Secure Image Encryption Algorithm Using a Novel Key-Substitution Architecture", IEEE Access, 2019 Publication	1 %
19	downloads.hindawi.com Internet Source	1 %
20	Submitted to University of Ulster Student Paper	1 %
21	ijeecs.iaescore.com Internet Source	1 %
22	Yoga Samudra, Tohari Ahmad. "Quality Control on Interpolation-based Reversible Audio Data Hiding using Bit Threshold", 2022 International Conference on Data Science and Its Applications (ICoDSA), 2022	1 %

Publication

23	www.ijiser.com Internet Source	1 %
24	publikationen.bibliothek.kit.edu Internet Source	1 %
25	Lei Zhang, Wendie Han, Rui Zhang, Lulu Wang, Xinyu Meng. "Identity-Based Key Management Scheme for Secure Discussion Group Establishment in DOSNs", IEEE Transactions on Information Forensics and Security, 2023 Publication	1 %
26	computingonline.net Internet Source	1 %
27	export.arxiv.org Internet Source	1 %
28	Aytaj Badirova, Shirin Dabbaghi, Faraz Fatemi Moghaddam, Philipp Wieder, Ramin Yahyapour. "A Survey on Identity and Access Management for Cross-Domain Dynamic Users: Issues, Solutions, and Challenges", IEEE Access, 2023 Publication	1 %
29	Shanshan Li, Chunxiang Xu, Yuan Zhang, Jianying Zhou. "A Secure Two-Factor Authentication Scheme From Password-Protected Hardware Tokens", IEEE	1 %

	Transactions on Information Forensics and Security, 2022 Publication	
30	www.techscience.com Internet Source	1 %
31	Albakri, Ashwag. "Lightweight Cryptographic Protocols for Mobile Devices", University of Missouri - Kansas City, 2020 Publication	1 %
32	Submitted to Pontificia Universidad Catolica del Ecuador - PUCE Student Paper	1 %
33	www.degruyter.com Internet Source	1 %
34	www.studocu.com Internet Source	1 %
35	Submitted to Mississippi State University Student Paper	<1 %
36	Shanshan Li, Chunxiang Xu, Yuan Zhang, Yicong Du, Xinsheng Wen, Kefei Chen, Jianfeng Ma. "Efficient Data Retrieval Over Encrypted Attribute-Value Type Databases in Cloud-Assisted Ehealth Systems", IEEE Systems Journal, 2021 Publication	<1 %

37	D. Sowmyadevi, I. Shanmugapriya. "Unsupervised machine learning based key management in wireless sensor networks", Measurement: Sensors, 2023 Publication	<1 %
38	Victor R. Kebande, Ali Ismail Awad. "Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions", ACM Computing Surveys, 2023 Publication	<1 %
39	www.foi.se Internet Source	<1 %
40	cibgp.com Internet Source	<1 %
41	mdpi-res.com Internet Source	<1 %
42	Submitted to University of Southampton Student Paper	<1 %
43	Hongbo Li, Qiong Huang, Jian Shen, Guomin Yang, Willy Susilo. "Designated-server identity-based authenticated encryption with keyword search for encrypted emails", Information Sciences, 2019 Publication	<1 %
44	Submitted to UIN Syarif Hidayatullah Jakarta Student Paper	

		<1 %
45	Submitted to Swinburne University of Technology Student Paper	<1 %
46	uyats.uludag.edu.tr Internet Source	<1 %
47	Aries Susanto, Israhadi Tri Hutama, Elsy Rahajeng, Aida Fitriyani. "Determinants of Continuance Use Intention of Mobile-based Electronic Ticketing", 2020 8th International Conference on Cyber and IT Service Management (CITSM), 2020 Publication	<1 %
48	Submitted to BATANGAS STATE UNIVERSITY Student Paper	<1 %
49	dblp.org Internet Source	<1 %
50	dora.dmu.ac.uk Internet Source	<1 %
51	eprint.iacr.org Internet Source	<1 %
52	Liansheng Sui, Zhi Pang, Ying Cheng, Yin Cheng, Zhaolin Xiao, Ailing Tian, Kemao Qian, Asundi Anand. "An optical image encryption based on computational ghost imaging with	<1 %

sparse reconstruction", Optics and Lasers in Engineering, 2021
Publication

53	Osama A. Khashan, Rami Ahmad, Nour M. Khafajah. "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks", Ad Hoc Networks, 2021 Publication	<1 %
54	bradscholars.brad.ac.uk Internet Source	<1 %
55	dblp.dagstuhl.de Internet Source	<1 %
56	ojs.unud.ac.id Internet Source	<1 %
57	www.ajol.info Internet Source	<1 %
58	www.mdpi.com Internet Source	<1 %
59	"Proceedings of Second International Conference on Computing, Communications, and Cyber-Security", Springer Science and Business Media LLC, 2021 Publication	<1 %
60	Mingxin Ma, Guozhen Shi, Fenghua Li. "Privacy-Oriented Blockchain-Based	<1 %

Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario", IEEE Access, 2019
Publication

61	Mohammad Wazid, Palak Bagga, Ashok Kumar Das, Sachin Shetty, Joel J. P. C. Rodrigues, Youngho Park. "AKM-IoV: Authenticated Key Management Protocol in Fog Computing-Based Internet of Vehicles Deployment", IEEE Internet of Things Journal, 2019 Publication	<1 %
62	Pankaj Kumar, Hari Om. "Multi-TA model-based conditional privacy-preserving authentication protocol for fog-enabled VANET", Vehicular Communications, 2024 Publication	<1 %
63	Victor R. Kebande, Ali Ismail Awad. "Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions", ACM Computing Surveys, 2024 Publication	<1 %
64	docslib.org Internet Source	<1 %
65	www.researchgate.net Internet Source	<1 %

66	Sanjeev Kumar Dwivedi, Ruhul Amin, Satyanarayana Vollala, Muhammad Khurram Khan. "B-HAS: Blockchain-Assisted Efficient Handover Authentication and Secure Communication Protocol in VANETs", IEEE Transactions on Network Science and Engineering, 2023 Publication	<1 %
67	XiaoKang Hu, Jian Li, ChangZheng Wei, WeiGang Li, Xin Zeng, Ping Yu, Haibing Guan. "STYX: A Hierarchical Key Management System Oriented to Elastic Content Delivery Networks on Public Clouds", IEEE Transactions on Dependable and Secure Computing, 2019 Publication	<1 %
68	dblp1.uni-trier.de Internet Source	<1 %
69	jurnal.ucy.ac.id Internet Source	<1 %
70	ouci.dntb.gov.ua Internet Source	<1 %
71	oulurepo.oulu.fi Internet Source	<1 %
72	www.sciencegate.app Internet Source	<1 %

73	www2.mdpi.com Internet Source	<1%
74	Subhabrata Rana, Fatemeh Khoda Parast, Brett Kelly, Yang Wang, Kenneth B. Kent. "A comprehensive survey of cryptography key management systems", Journal of Information Security and Applications, 2023 Publication	<1%
75	de Ree, Marcus Johannes Maria. "Decentralized Key Management for Beyond 5G Network Coding-Enabled Mobile Small Cells", University of South Wales (United Kingdom), 2023 Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		

44_CITSM2023.pdf

Article Error You may need to use an article before this word. Consider using the article **the**.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word. Consider using the article **the**.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word. Consider using the article **the**.

Missing "," You may need to place a comma after this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to remove this article.

Hyph. You may need to add a hyphen between these two words.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to remove this article.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 3

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 4

PAGE 5

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 6