Universe International Journal of Interdisciplinary Research
(Peer Reviewed Refereed Journal)

© UIJIR | ISSN (O) – 2582-6417
JULY 2021 | Vol. 2 Issue 2
www.uijir.com

REVIEW THE TECHNIQUE FOR SECURE MOBILE CLOUD COMPUTING DATA USING LIGHT WEIGHT HYBRID ENCRYPTION SCHEME

Author's Name: [1]Mrs. Bhawana Pillai, [2]Mr. Ankit Bijoria

Affiliation: *[1]Associate Professor at LNCTS Group Colleges, Bhopal, Madhya Pradesh, India*

[2]Studen, at LNCTS Group Colleges, Bhopal, Madhya Pradesh, India

E-Mail: ankitbijoria@gmail.com

DOI No. – 08.2020-25662434

Abstract

The Mobile Cloud contains numerous difficulties and problems. The security technique provides support to these service providers and consumer stop protect data. The security technique delivers a secure environment, within which, the consumer communicates with the service provider using Virtual Private Network (VPN). By means of validating and verifying the authorizations provided by the user, the technique guarantees user authentication. Once the customer credentials are verified, the framework permits the user data to be encrypted, processed and stored in the Cloud.

The aim of the proposed hybrid combination of RSA and ECC with PRE algorithm is to accomplish the security for the cloud outsourced data. The algorithm encrypts the data content previously storing it in the storage so that the protection of the data is entirely under the control of the data owner. In this research work to Review the Technique for Secure Mobile Cloud Computing Data Using Light Weight Hybrid Encryption Scheme.

Keywords*: Cloud Computing, Mobile Cloud Computing, Light Weight Data Secure, Cloud Service Provider.*

INTRODUCTION

A Cloud Service Provider (CSP) [1] caters to infinite computing resources for the organization based on the requirement. More computing [2] resources are required during the months of the Olympics. The web traffic remains low for the rest of the year. These types of deviations in terms of resource requirement [4] can be easily handled by the elasticity property of Cloud. A Cloud framework manages and streamlines the resources with metered services. It requires just a short time commitment to utilize the resources such as infrastructure and storage. Mobile Cloud Computing [5] has been developed from different computing paradigms such as time sharing computing, distributed computing, grid computing, utility computing, parallel computing and virtualization. Mobile Cloud is a mixture of software and hardware that offers pervasive and utility [6] computing enabling the setup of resources. Smart phones and laptops have become an integral part of the digital era. Humans are increasingly dependent on mobile devices for their survival, both personal and professional. Mobile Cloud is implemented [7] by a key technology named Virtualization in which a hypervisor produces numerous virtual modules [8]. The greatest advantage of virtualization hypervisor is to mimic the software, hardware, and network resources for improving the utilization of resources. The Mobile Cloud enables the users of mobile devices to perform complex functionalities and data storage via thin clients such as smart phones and tablets. Mobile devices have the constraint of limited battery.

© UIJIR | ISSN (O) – 2582-6417
JULY 2021 | Vol. 2 Issue 2
www.uijir.com

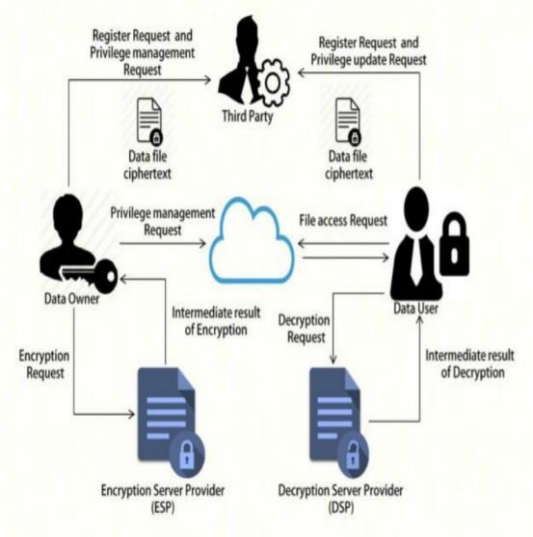

Figure 1: existing secure model for mobile cloud computing [8]

CLOUD DEPLOYMENT MODEL: The Cloud is classified into four different categories depending on the location and type of deployment as

i) Public Cloud
ii) Private Cloud,
iii) Community Cloud
iv) Hybrid Cloud

Public Cloud: In Public Cloud, the infrastructure is managed and operated by a third party service provider for use by the general public. The consumer has no control over the computing resources and the infrastructure. In general, public Cloud [9] service providers such as Amazon, Microsoft, Oracle and Google operate the infrastructure at their data centre with public access through the Internet. Oracle, Amazon, and Microsoft also provide direct connect services known as Oracle Fast Connect, AWS Direct Connect, and Azure Express Route respectively. These resources are shared by several public tenants with optimal cost and flexibility as well.

Private Cloud: Private Cloud is commissioned for a single organization, managed internally or by a third-party and hosted internally or externally. When deploying a private cloud, a significant quantum of resources used in the business is virtualized. Further, the organization needs to re-evaluate [10] the decisions on the extent of their own resources. Private Cloud enhances businesses productivity. With the implementation of Private Cloud, security issues should be explicitly stated, in order to prevent from severe susceptibilities. It is managed by experts who are within the organization and have local control. Private Clouds are more expensive with their relatively high level of security and they can be customized based on user requirements. Private Clouds[11] are classified into two types, namely, i) On Campus Private Cloud, where the Cloud is setup on the premises of the organization and ii) External Host Private Cloud, where the Cloud is hosted by a third party Cloud service providers.

Community Cloud: In Community Cloud, the infrastructure is shared by a particular group or community based on common interests such as vision, mission, and few other compliance Policies [12]. It may be monitored and controlled by third party Cloud service provider and may exist on or off the premises.

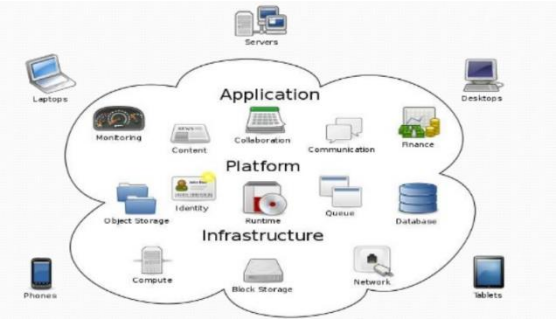

Figure 2: Cloud computing model

Hybrid Cloud: In Hybrid Cloud, organizations may deploy important applications on their Private Cloud [13] and deploy less secure applications in Public Cloud. The combination of Public, Private and Community Cloud is said to be Hybrid Cloud. Hybrid Cloud empowers data and application versatility such as Cloud bursting and load balancing techniques. It lets users to prolong the capacity or the ability of a Cloud service by means of aggregation, integration or customization.

LITERATURE REVIEW

At present, [14] most of the academic and business field is getting adapted to the use of more than one cloud as the use of the cloud increased. Most of the research analysis of government and organizations depends upon the impact of multi-cloud storage. They have a high impact on cloud innovation. Organizations will have to store private and secret data as well as open data relating to their field. So there is need for private and public clouds. Massive pool of data will get stored in the public cloud. The security aspects and privacy preservation attention are very much essential when an organization stores full data in multi-cloud used by multi-user.

[15] storage follows a multi-cloud system. The idea is to mitigate the tampering, illegal manipulation of using the cloud at the same time. When multiple clouds are integrated, only collaborated cloud providers are involved in trust assumptions, thereby confusing the intruder who tries to tamper with the data. A survey[16] of eradication of the deficiency of single cloud multi-cloud is done with the solutions for handling sensitive information which cannot be trusted in a single cloud. There available several security techniques available are adaptable for different types of multi- cloud such as hybrid, federated and multi-cloud[17]. One of the techniques is to split the data and each partition is stored in the different cloud so that it is adequately protected from the malicious intruder as he may not be able to evaluate the splitting strategy which is preserved by FTP. Homomorphic encryption, Attribute-based Encryption (ABE), building a Multi-cloud database model (MCDB), etc. are some of the methods[18] to follow. The authors[19] found a theoretical solution to the problem of trust and cloud conflict. In building an agreement based on trust and behavior, and validation of proxies and digital Signatures [20] using public keys, they found a solution the problem of trust. The second problem which is a proxy conflict to assure the requirement for cloud collaboration is solved by using adaptive algorithms and a scalable conflict resolution [21]. They have used the correlation

mechanism to find the dependency of resource segments. The authors have attempted to solve the data privacy issue that arises when information is given to proxies. For this, they use data perturbation and solve by the tradeoff between request and privacy indicates the design of a cost-effective system using LP for minimum cost function. They have also considered QoS maximization. They assumed p as providers who bill cost c per data with expected QoS for the data divided into N chunks[22]. When a request is posed q out of p chunks are needed to satisfy the requirement. The authors have taken care I designing the value of k, N, q, and p in such a way that complete security is provided by not revealing the data location for illegal access. designed a system called Service Operator-aware Trust Scheme (SOTS), whereas system a trusty[23] broker is used for resource matching between clients and the cloud provider. They have done periodically updation of the resource list for the addition of new resources. The system is designed with four modules. The adaptive trust model evaluates the resource priorities based on performance and previous trust information. The resource matching model designs the SLA between the resource manager[24] the rules for the resources. The agent publishes the model to monitor and guarantee the rules. The work of the resource registration module is to add the resource to the cloud index. The limitations that the broker should be trusted by all providers[25], clients and cloud. have proposed for the frame Storage and Retrieval Algorithm[26] that guarantees the reliability of the encrypted data in multiple clouds. It shows the performance as enhancement over the existing system using a share mechanism secretly, thereby protecting the search patterns. When compared to baseline[27] encryption algorithm it shows a low overhead. They use both private and public keys. The reliability along with privacy, all-time availability and data integrity is attained by dividing the data into piece of portion and stored redundantly in the multi-cloud. However, the cost is doubled as it is charged for handling at all location and is cost effective.

PROPOSED METHODOLOGY

The proposed framework provides an authentication mechanism, where, the image selected by the Mobile Cloud user is encrypted using visual cryptography scheme. Then, the encrypted image is divided into three equal image shares and are distributed among three entities, namely, the Mobile Cloud user, network service provider, and Cloud controller[28] to prevent unauthorized access. Further, to increase the security, a secret phrase is embedded into three image shares of the original image using stenography to prevent fraudulent behaviour by any compromised entity. The proposed authentication mechanism shows enhanced security when compared to the previous fingerprint authentication for Mobile Cloud. The proposed methodology is tested with two different mobile devices using Mobile Cloud which is shown to be effective and better in providing security. There are two phases in the proposed authentication mechanism, namely, enrolment phase and login phase. In the enrolment phase, the users while registering with CSP choose their username and password credentials along with other necessary information. After registering with the CSP, the user is redirected to choose secure authentication mechanism. Then, the users are requested to choose a secret image of their own choice and a secret phrase or sentence. The performance evaluation is done based on the proposed Site Key authentication for 30 participants each performing enrolment and login phases. The QoS parameters considered are enrolment time and login time for authentication. the proposed technique is lower when compared with fingerprint authentication for Mobile Cloud. Further, the use of Steganographic with visual cryptography prevents unauthorized hackers from reproducing the image share which adds another level of security

© UIJIR | ISSN (O) – 2582-6417
JULY 2021 | Vol. 2 Issue 2
www.uijir.com

which deters phishing attacks.

Secured Technique For Mobile Cloud: The Mobile Cloud contains numerous difficulties and problems. The security[29]technique provides support to the service providers and consumers to protect data. The security technique delivers a secure environment, within which, the consumer communicates with the service provider using Virtual Private Network (VPN). By means of validating and verifying the credentials provided by the user, the technique guarantees user authentication [30]. Once the user credentials are verified, the technique allows the user data to be encrypted, processed and stored in the Cloud. The typical technique for the Cloud service provider technique.

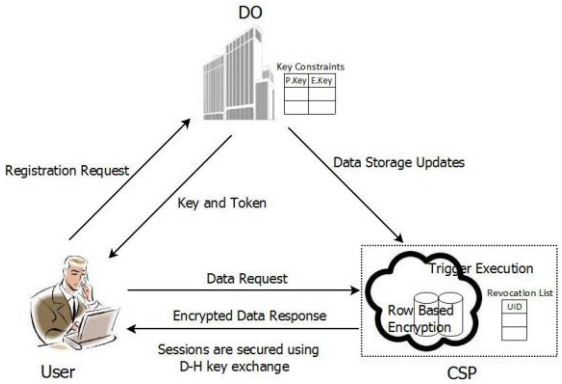

Figure 3: cloud data security process

Security Policies: The technique ensures that security policies are properly planned, documented and distributed among employees. The employee who works in the data centre at the location of service providers should be given proper training on the technologies. The loyalty of the employee to the organization is paramount and the organization has to do frequent background checks on its employees. The organization must impose password modifications at regular time intervals. The software and hardware access rights must not be utilized by the employees of Mobile Cloud[30] service provider without proper and prior approval.

Cryptography techniques[31] are widely used for ensuring security in cloud using the encryption and decryption processes between the sender and receiver and the symmetric and asymmetric algorithm with the public and private keys. Some of the symmetric algorithms are DES, 3DES, RC5, RC6, Blowfish, and AES[32] with sharing of encryption and decryption key. The asymmetric algorithm is one in which[33] public key is published while the private key is secret. Algorithms RSA and ECC are examples. The main advantage of public key is cryptography is the private key transmitted[34] to the authorized user only. Public Key Infrastructure (PKI) is an earlier technology[35] that was used in cloud and a similar grid environment. It is based on proxy certificates with high credentials and short-term[36] public keys which later were found not suitable for the dynamic environment. Hybrid-Based Cryptography is the traditional algorithm which has gained attention in dealing[37] cloud security issues. When IBC is used the user uses his identity with the public key and is allowed for access without any further authentic check. It allowed flexible key managing and usage.

The main three steps of the cryptographic algorithm are

- Key generation.
- Encryption.
- Decryption.

The digital signature based MD5, SHA-1 is eminently suitable for achieving authentication and non-repudiation. From an analysis of asymmetric algorithms, RSA does better if around [38] is not require to generate the key for every time use instead of the fixed key. Even the signature generation and signature verification time are less for RSA than ECC. ECC is suitable for when a lot of users are accessing with the small session.

CONCLUSION

Encryption and key management are the core techniques to safeguard sensitive data in Mobile Cloud. There is a greater requirement for encrypting private data, for example, passwords, bank details, social security number etc. to be protected against data theft and loss. A feasible solution for ensuring data sensitivity in the Mobile Cloud is by encrypting the data, preventing attempts of unauthorized information access. Consequently, it is essential to restrict organizational data shared in trusted Mobile Cloud over the Internet. Cloud security is enhanced by combining symmetric and asymmetric encryption.

REFERENCES

1. H. S. Alqahtani and G. Kouadri-Mostefaou, "Multi-clouds Mobile Computing for the Secure Storage of Data," 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, 2014, pp. 495-496, doi: 10.1109/UCC.2014.68.
2. J. Zhang, Z. Zhang and H. Guo, "Towards Secure Data Distribution Systems in Mobile Cloud Computing," in IEEE Transactions on Mobile Computing, vol. 16, no. 11, pp. 3222-3235, 1 Nov. 2017, doi: 10.1109/TMC.2017.2687931.
3. A. Awad, A. Matthews, Y. Qiao and B. Lee, "Chaotic Searchable Encryption for Mobile Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 440-452, 1 April-June 2018, doi: 10.1109/TCC.2015.2511747.
4. R. LI, C. Shen, H. He, X. Gu, Z. Xu and C. Xu, "A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 344-357, 1 April-June 2018, doi: 10.1109/TCC.2017.2649685.
5. J. Tsai and N. Lo, "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services," in IEEE Systems Journal, vol. 9, no. 3, pp. 805-815, Sept. 2015, doi: 10.1109/JSYST.2014.2322973.
6. P. Gope and A. K. Das, "Robust Anonymous Mutual Authentication Scheme for n-Times Ubiquitous Mobile Cloud Computing Services," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1764-1772, Oct. 2017, doi: 10.1109/JIOT.2017.2723915.
7. S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay and J. J. P. C. Rodrigues, "Provably Secure Fine-Grained Data Access Control Over Multiple Cloud Servers in Mobile Cloud Computing Based Healthcare Applications," in IEEE Transactions on Industrial Informatics, vol. 15, no. 1, pp. 457-468, Jan. 2019, doi: 10.1109/TII.2018.2824815.
8. Achyuth Ranjan V , K. Karthikayani , P. Jaswanth , Vivekananthan GR, Shankara Lingam, A lightweight secure data sharing scheme V Achyuth Ranjan et.al; International Journal of Advance Research and Development
9. S. Das, M. Khatua, S. Misra and M. S. Obaidat, "Quality-Assured Secured Load Sharing in Mobile Cloud Networking Environment," in IEEE Transactions on Cloud Computing, vol. 7, no. 1, pp. 102-115, 1 Jan.-March 2019, doi: 10.1109/TCC.2015.2457416.
10. H. Cui, X. Yuan and C. Wang, "Harnessing Encrypted Data in Cloud for Secure and

Efficient Mobile Image Sharing," in IEEE Transactions on Mobile Computing, vol. 16, no. 5, pp. 1315-1329, 1 May 2017, doi: 10.1109/TMC.2016.2595573.

11. Y. Xie, H. Wen, B. Wu, Y. Jiang and J. Meng, "A Modified Hierarchical Attribute-Based Encryption Access Control Method for Mobile Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 7, no. 2, pp. 383-391, 1 April-June 2019, doi: 10.1109/TCC.2015.2513388.
12. P. K. Tysowski and M. A. Hasan, "Hybrid Attribute- and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds," in IEEE Transactions on Cloud Computing, vol. 1, no. 2, pp. 172-186, July-December 2013, doi: 10.1109/TCC.2013.11.
13. H. Wu, K. Wolter, P. Jiao, Y. Deng, Y. Zhao and M. Xu, "EEDTO: An Energy-Efficient Dynamic Task Offloading Algorithm for Blockchain-Enabled IoT-Edge-Cloud Orchestrated Computing," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2163-2176, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3033521.
14. K. Zhou, M. H. Afifi and J. Ren, "ExpSOS: Secure and Verifiable Outsourcing of Exponentiation Operations for Mobile Cloud Computing," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 11, pp. 2518-2531, Nov. 2017, doi: 10.1109/TIFS.2017.2710941.
15. I. A. Elgendy, W. -Z. Zhang, C. -Y. Liu and C. -H. Hsu, "An Efficient and Secured Framework for Mobile Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 9, no. 1, pp. 79-87, 1 Jan.-March 2021, doi: 10.1109/TCC.2018.2847347.
16. J. L. D. Neto, S. Yu, D. F. Macedo, J. M. S. Nogueira, R. Langar and S. Secci, "ULOOF: A User Level Online Offloading Framework for Mobile Edge Computing," in IEEE Transactions on Mobile Computing, vol. 17, no. 11, pp. 2660-2674, 1 Nov. 2018, doi: 10.1109/TMC.2018.2815015.
17. W. Zhang, Y. Wen and X. Zhang, "Towards Virus Scanning as a Service in Mobile Cloud Computing: Energy-Efficient Dispatching Policy Under ${N}$ -Version Protection," in IEEE Transactions on Emerging Topics in Computing, vol. 6, no. 1, pp. 122-134, Jan.-March 2018, doi: 10.1109/TETC.2015.2471852.
18. Zhang M., Jiang Y., Shen H., Li B., Susilo W. (2019) Cloud-Based Data-Sharing Scheme Using Verifiable and CCA-Secure Re-encryption from Indistinguishability Obfuscation. In: Guo F., Huang X., Yung M. (eds) Information Security and Cryptology. Inscrypt 2018. Lecture Notes in Computer Science, vol 11449. Springer, Cham. https://doi.org/10.1007/978-3-030-14234-6_13
19. Rajawat A.S., Rawat R., Barhanpurkar K., Shaw R.N., Ghosh A. (2021) Blockchain-Based Model for Expanding IoT Device Data Security. In: Bansal J.C., Fung L.C.C., Simic M., Ghosh A. (eds) Advances in Applications of Data-Driven Computing. Advances in Intelligent Systems and Computing, vol 1319. Springer, Singapore. https://doi.org/10.1007/978-981-33-6919-1_5
20. Khan, A.N., Kiah, M.L.M., Ali, M. *et al.* BSS: block-based sharing scheme for secure data storage services in mobile cloud environment. *J Supercomput* **70,** 946–976 (2014). https://doi.org/10.1007/s11227-014-1269-8
21. Khan, A.N., Mat Kiah, M.L., Madani, S.A. *et al.* Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing. *J Supercomput* **66,** 1687–1706 (2013). https://doi.org/10.1007/s11227-013-0967-y
22. Alkatheiri, M.S. PCOS—Privacy-Controlled Offloading Scheme for Secure Service Data

Offloading in Edge-Internet of Things-Cloud Scenario. *Arab J Sci Eng* (2021). https://doi.org/10.1007/s13369-021-05607-6

23. Rajawat A.S., Rawat R., Shaw R.N., Ghosh A. (2021) Cyber Physical System Fraud Analysis by Mobile Robot. In: Bianchini M., Simic M., Ghosh A., Shaw R.N. (eds) Machine Learning for Robotics Applications. Studies in Computational Intelligence, vol 960. Springer, Singapore. https://doi.org/10.1007/978-981-16-0598-7_4
24. Bedi, R.K., Singh, J. & Gupta, S.K. MWC: an efficient and secure multi-cloud storage approach to leverage augmentation of multi-cloud storage services on mobile devices using fog computing. *J Supercomput* **75,** 3264–3287 (2019). https://doi.org/10.1007/s11227-018-2304-y
25. Arvind, K.S., Manimegalai, R. Secure data classification using superior naive classifier in agent based mobile cloud computing. *Cluster Comput* **20,** 1535–1542 (2017). https://doi.org/10.1007/s10586-017-0797-4.
26. Amin, R.u., Inayat, I., Shahzad, B. *et al.* An empirical study on acceptance of secure healthcare service in Malaysia, Pakistan, and Saudi Arabia: a mobile cloud computing perspective. *Ann. Telecommun.* **72,** 253–264 (2017). https://doi.org/10.1007/s12243-016-0553-4.
27. Dhanya N.M., Kousalya G. (2015) Adaptive and Secure Application Partitioning for Offloading in Mobile Cloud Computing. In: Abawajy J., Mukherjea S., Thampi S., Ruiz-Martínez A. (eds) Security in Computing and Communications. SSCC 2015. Communications in Computer and Information Science, vol 536. Springer, Cham. https://doi.org/10.1007/978-3-319-22915-7_5.
28. Anand Singh Rajawat Sumit Jain Kanishk Barhanpurkar,(2021) Fusion protocol for improving coverage and connectivity WSNs, IET Wireless Sensor Systems, https://doi.org/10.1049/wss2.12018
29. Tribedi D., Sadhukhan D., Ray S. (2019) Cryptanalysis of a Secure and Privacy Preserving Mobile Wallet Scheme with Outsourced Verification in Cloud Computing. In: Mandal J., Mukhopadhyay S., Dutta P., Dasgupta K. (eds) Computational Intelligence, Communications, and Business Analytics. CICBA 2018. Communications in Computer and Information Science, vol 1031. Springer, Singapore. https://doi.org/10.1007/978-981-13-8581-0_33.
30. Kim, HW., Jeong, YS. Secure Authentication-Management human-centric Scheme for trusting personal resource information on mobile cloud computing with blockchain. *Hum. Cent. Comput. Inf. Sci.* **8,** 11 (2018). https://doi.org/10.1186/s13673-018-0136-7.
31. Raj, S., Arunkumar, B. Enhanced encryption for light weight data in a multi-cloud system. Distrib Parallel Databases (2021). https://doi.org/10.1007/s10619-021-07340-3.
32. Kiraz, M.S. A comprehensive meta-analysis of cryptographic security mechanisms for cloud computing. J Ambient Intell Human Comput 7, 731–760 (2016). https://doi.org/10.1007/s12652-016-0385-0
33. Naeem, R.Z., Bashir, S., Amjad, M.F. et al. Fog computing in internet of things: Practical applications and future directions. Peer-to-Peer Netw. Appl. 12, 1236–1262 (2019). https://doi.org/10.1007/s12083-019-00728-0
34. Ghorbel, A., Ghorbel, M. & Jmaiel, M. Privacy in cloud computing environments: a survey and research challenges. J Supercomput 73, 2763–2800 (2017).

https://doi.org/10.1007/s11227-016-1953-y
35. Mousavi, S.K., Ghaffari, A., Besharat, S. et al. Security of internet of things based on cryptographic algorithms: a survey. Wireless Netw 27, 1515–1555 (2021). https://doi.org/10.1007/s11276-020-02535-5
36. Zhao, Y., Ren, M., Jiang, S. et al. An efficient and revocable storage CP-ABE scheme in the cloud computing. Computing 101, 1041–1065 (2019). https://doi.org/10.1007/s00607-018-0637-2
37. Singh, S., Sharma, P.K., Moon, S.Y. et al. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J Ambient Intell Human Comput (2017). https://doi.org/10.1007/s12652-017-0494-4
38. Nawrocki, P., Sniezynski, B. Autonomous Context-Based Service Optimization in Mobile Cloud Computing. J Grid Computing 15, 343–356 (2017). https://doi.org/10.1007/s10723-017-9406-2
39. Khanna, N., Sachdeva, M. OFFM-ANFIS analysis for flood prediction using mobile IoS, fog and cloud computing. Cluster Comput 23, 2659–2676 (2020). https://doi.org/10.1007/s10586-019-03033-w
40. Mandal, M. Anonymity in traceable cloud data broadcast system with simultaneous individual messaging. Int. J. Inf. Secur. (2020). https://doi.org/10.1007/s10207-020-00512-9