# References:AES+ECC(2021) 71

**Reference Details:**

1. Shukla, D.K.; Dwivedi, V.K.; Trivedi, M.C. “Encryption algorithm in cloud computing.” Mater. Today Proc*.* **2020**, *37*, 1869–1875. [[CrossRef](http://doi.org/10.1016/j.matpr.2020.07.452)]
2. Yahia, H.S.; Zeebaree, S.R.M.; Sadeeq, M.A.M.; Salim, N.O.M.; Kak, S.F.; Al-Zebari, A.; Salih, A.A.; Hussein, H.A. “Comprehensive survey for cloud computing based nature-inspired algorithms optimization scheduling.” Asian Journal Research Computer Sciences**2021**, 1–16. [[CrossRef](http://doi.org/10.9734/ajrcos/2021/v8i230195)]
3. Qazi, R.; Khan, I.A. “Data security in cloud computing using elliptic curve cryptography.” International Journal Computer Communication Network**2019**, *1*, 46–52. [[CrossRef](http://doi.org/10.31221/OSF.IO/PUJ5V)]
4. Chen, Y.; Liu, H.; Wang, B.; Sonompil, B.; Ping, Y.; Zhang, Z. “A threshold hybrid encryption method for integrity audit without trusted center.” Journal Cloud Computer **2021**, *10*, 3. [[CrossRef](http://doi.org/10.1186/s13677-020-00222-6)]
5. Agrahari, V. “Data security in cloud computing using cryptography algorithms.” International Journal Science Development Research**2020**. Available online:[www.ijsdr.org](http://www.ijsdr.org/) (accessed on 22 October 2021).
6. Abdullahi Ibrahim, A.; Cheruiyot, W.; Kimwele, M.W. “Data security in cloud computing with elliptic curve cryptography core.” International JournalComputer**2017**, *26*, 1–14. Available online: <http://ijcjournal.org/>(accessed on 22 October 2021).
7. Manaa, M.E.; Hadi, Z.G. “Scalable and robust cryptography approach using cloud computing.” Journal Discrete Mathematics Science Cryptography**2020**,

*23*, 1439–1445. [[CrossRef](http://doi.org/10.1080/09720529.2020.1727609)]

1. Madhavi, G.; Samatha, J. “Secure data storage and access of data in cloud using Elliptic curve cryptography.” IEEE Journal**2020**, *11*. Available online: [www.jespublication.com](http://www.jespublication.com/) (accessed on 22 October 2021).
2. Sridharan, S.; Arokiasamy, A. “Effective secure data storage in cloud by using ECC algorithm.” Middle-East journal Science Research**2017**, *25*, 117–127. [[CrossRef](http://doi.org/10.5829/idosi.mejsr.2017.117.127)]
3. Selvam, J.M.; Srivaramangai, P. “Time complexity analysis of cloud authentications and data security: Polynomial based hashing and elliptic curve cryptography.” International Journal Anal. Exp. Modal Anal.**2020**, *12*, 850–860.
4. Manaa, M.E. “Data encryption scheme for large data scale in cloud computing.” Journal Telecommunication Electronics Computer Engineering**2017**, *9*, 1–5.

Available online: <https://jtec.utem.edu.my/jtec/article/view/2759>(accessed on 22 October 2021).

1. Astuti, N.R.D.P.; Aribowo, E.; Saputra, E. “Data security improvements on cloud computing using cryptography and steganogra- phy.” IOP Confrence Series Material Science Engineering**2020**, *821*, 012041. [[CrossRef](http://doi.org/10.1088/1757-899X/821/1/012041)]
2. Awad, W.S. “A framework for improving information security using cloud computing.” International Journal Advance Research Engineering Technology**2020**, *11*, 264–280. [[CrossRef](http://doi.org/10.34218/IJARET.11.6.2020.024)]
3. Kumar, V.; Ahmad, M.; Kumari, A. “A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS.” Telemat. Inform.**2018**, *38*, 100–117. [[CrossRef](http://doi.org/10.1016/j.tele.2018.09.001)]
4. Singla, S.; Singh, J. “Cloud computing security using encryption technique.” International Journal Advance Research Computer Engineering Technology**2013**, *2*, 673.
5. Almorsy, M.; Grundy, J.; Müller, I. “An analysis of the cloud computing security problem.” *arXiv* **2016**, arXiv:1609.01107.
6. Jena, O.P.; Tripathy, A.; Swagatam, S.; Rath, S. “ Dual encryption model for preserving privacy in cloud computing.” Advance Mathematics Science Journal**2020**, *9*, 6667–6678. [[CrossRef](http://doi.org/10.37418/amsj.9.9.24)]
7. Arockia, P.; Dharani, N.; Aiswarya, R.; Shailesh, P. “Cloud data security using elliptic curve cryptography.” International Research Journal Engineering Technology **2017**, *4*, 32–36.
8. Li, Y.; Gai, K.; Qiu, L.; Qiu, M.; Zhao, H. “Intelligent cryptography approach for secure distributed big data storage in cloud computing.” Information Science.**2017**, *387*, 103–115. [[CrossRef](http://doi.org/10.1016/j.ins.2016.09.005)]
9. Saeed, Z.R.; Ayop, Z.; Azma, N.; Rizuan Baharon, M. “Improved cloud storage security of using three layers cryptography algorithms.” International Journal Computer Science Information Security**2018**, *16*, 34–39.
10. Al-Dhuraibi, Y.; Paraiso, F.; Djarallah, N.; Merle, P. “Elasticity in cloud computing: State of the art and research challenges.” IEEETrans. Serv. Comput.**2017**, *11*, 430–447. [[CrossRef](http://doi.org/10.1109/TSC.2017.2711009)]
11. Hosam, O.; Ahmad, M.H. “Hybrid design for cloud data security using combination of AES, ECC and LSB steganography.” International Journal Computer Science Engineering**2019**, *19*, 153. [[CrossRef](http://doi.org/10.1504/IJCSE.2019.100236)]
12. Shantha, A.; Renita, J.; Edna, E.N. “Analysis and implementation of ECC algorithm in lightweight device.” In Proceedings of the 2019 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 4–6 April 2019; pp. 305–309. [[CrossRef](http://doi.org/10.1109/iccsp.2019.8697990)]
13. Varghese, S.; Vigila, S.M.C. “A varied approach to attribute based access model for secure storage in cloud.” In Proceedings of the 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 17–18 March 2017; pp. 1–4. [[CrossRef](http://doi.org/10.1109/iciiecs.2017.8276130)]
14. Hodowu, D.K.M.; Korda, D.R.; Ansong, E.D. “An enhancement of data security in cloud computing with an implementation of a two-level cryptographic technique, using AES and ECC algorithm.” International Journal Engineering Research Technology**2020**, *9*, 639–650.
15. Lee, B.-H.; Dewi, E.K.; Wajdi, M.F. “Data security in cloud computing using AES under HEROKU cloud.” In Proceedings of the 2018 27th Wireless and Optical Communication Conference (WOCC), Hualien, Taiwan, 30 April–1 May 2018; pp. 1–5. [[CrossRef](http://doi.org/10.1109/wocc.2018.8372705)]
16. Zhu, Y.; Fu, A.; Yu, S.; Yu, Y.; Li, S.; Chen, Z. “New algorithm for secure outsourcing of modular exponentiation with optimal checkability based on single untrusted server.” In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6. [[CrossRef](http://doi.org/10.1109/icc.2018.8422482)]
17. Bhardwaj, K.; Chaudhary, S. “Implementation of elliptic curve cryptography in ‘C’ ”. International Journal Emerging Technology**2012**, *3*, 38–51.
18. Ogiela, U. “Cognitive cryptography for data security in cloud computing.” Concurrent Computer Present Expression**2019**, *32*, e5557. [[CrossRef](http://doi.org/10.1002/cpe.5557)]
19. Sood, S.K. “A combined approach to ensure data security in cloud computing.” Journal Networking Computer Application**2012**, *35*, 1831–1838. [[CrossRef](http://doi.org/10.1016/j.jnca.2012.07.007)]
20. Mendonca, S.N. “Data security in cloud using AES”. International Journal Engineering Research Technology**2018**, *7*. [[CrossRef](http://doi.org/10.17577/IJERTV7IS010104)]
21. Suresha, R.G. “Enhancing security in cloud storage using ecc algorithm.” International Journal Science Research**2013**, 2–8. Available online: [https:](https://www.ijsr.net/archive/v2i7/MDIwMTM3NA%3D%3D.pdf)[//www.ijsr.net/archive/v2i7/MDIwMTM3NA==.pdf](https://www.ijsr.net/archive/v2i7/MDIwMTM3NA%3D%3D.pdf) (accessed on 22 October 2023).
22. Abbas, S.; Maryoosh, A.A. “Improving data storage security in cloud computing using elliptic curve cryptography.” IOSR Journal Computer Engineering **2015**, *17*, 48–53.
23. Barati, M.; Aujla, G.S.; Llanos, J.T.; Duodu, K.A.; Rana, O.F.; Carr, M.; Rajan, R. “Privacy-Aware cloud auditing for GDPR compliance verification in online healthcare.” IEEE Trans. Ind. Information **2021**, *1*. [[CrossRef](http://doi.org/10.1109/tii.2021.3100152)]
24. Mahto, D.; Yadav, D.K. RSA and ECC: “A comparative analysis.” International Journal Applied Engineering Research**2017**, *12*, 9053–9061.
25. Vidakovic, D.; Parezanovic, D. “Generating keys in elliptic curve cryptosystems.” *arXiv* **2013**, arXiv:1309.0245.

(**Aryan wala mene add kiya hai**)

1. Aryan, Chaithanya Kumar and Durai Raj Vincent P M “ Enhanced diffie-hellman algorithm for reliable key exchange” IOP Conference Series: Materials Science and Engineering 2017 doi:10.1088/1757-899X/263/4/042015

(**ye ECDH samiksha wale se hai**)

1. D. E. Denning, “Cryptography and Data Security”, Addison-Wesley Publishing Company, America, (**1982**).
2. G. C. Kessler, “An overview of cryptography”, [Online], Available: [http://www.garykessler.net/library/crypto.html#purpose,](http://www.garykessler.net/library/crypto.html#purpose) (**1998**).
3. P. Patil, P. Narayankar, N. D. G. and M. S. M, “A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish”, Procedia Computer Science, (**2016)**; Nagpur, India.
4. P. Prajapati, N. Patel, R. Macwan, N. Kachhiya and P. Shah, “Comparative Analysis of DES, AES, RSA Encryption Algorithms”, International Journal of Engineering and Management Research, vol. 4, no. 1, **(2014)**, pp. 132-134.
5. P. Mahajan and A. Sachdeva, “A study of Encryption algorithms AES, DES and RSA for security”, Global Journal of Computer Science and Technology, vol. 13, no. 15, **(2013)**.
6. Y. Wang and M. Hu, “Timing evaluation of the known cryptographic algorithms”, International Conference on Computational Intelligence and Security, (**2009**).
7. V. R. Pancholi and B. P. Patel, “Enhancement of Cloud Computing Security with Secure Data Storage using AES”, International Journal for Innovative Research in Science and Technology, vol. 2, no. 09, **(2016)**, pp. 18-21.
8. P. Kumar and S. B. Rana, “Development of modified AES algorithm for data security”, Optik- International Journal for Light and Electron Optics, vol. 127, no. 04, **(2016)**, pp. 2341-2345.
9. A. K. Mandal, C. Parakash and A. Tiwari, “Performance evaluation of cryptographic algorithms: DES and AES”, Electrical, Electronics and Computer Science (SCEECS), (**2012**).
10. A. A. Hasib and A. A. M. Haque, “A comparative study of the performance and security issues of AES and RSA cryptography”, Third International Conference on Convergence and Hybrid Information Technology, **(2008)**.
11. K. Rege, N. Goenka, P. Bhutada and S. Mane, “Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA”, International Journal of Computer Applications, vol. 71, no. 22, **(2013)**
12. R. R. Ahirwal and M. Ahke, “Elliptic curve diffie-hellman key exchange algorithm for securing hypertext information on wide area network”, International Journal of Computer Science and Information Technologies, vol. 4, no. 2, **(2013)**, pp. 363-368.
13. A. Pourali, M. V. Malakooti and M. H. Yektaie, “A Secure SMS Model in E-Commerce Payment using Combined AES and ECC Encryption Algorithms”, The International Conference on Computing Technology and Information Management (ICCTIM), (**2014)**.
14. B. Ji, L. Wang and Q. Yang, “New Version of AES-ECC Encryption System Based on FPGA in WSNs”, Journal of Software Engineering, vol. 9, no. 1, **(2015)**, pp. 87-95.
15. N. Jha and B. Patel, “Forward Secrecy For Google HTTPS using Elliptic Curve Diffie- Hellman Key”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 1, no. 9, **(2012)**.

**(REFERENCES FROM ARPIT AND GUNJAN which is paper 70)**

1. Jigar Chauhan , Neekhil Dedhia, Bhagyashri Kulkarni , “Enhancing Data Security by using Hybrid Cryptographic Algorithm” International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May 2013.
2. Meenakshi Shankar and Akshaya.P , . “Hybrid Cryptographic Technique Using RSA Algorithm and Scheduling Concepts”. International Journal of Network Security & Its Applications (IJNSA) Vol.6, No.6, November 2014.
3. S. Subasree and N. K. Sakthivel , . “Design of A New Security Protocol Using Hybrid Cryptography Algorithms.” IJRRAS 2 (2 ), February 2010
4. Wang Tianfu, K. Ramesh Babu, “Design of a Hybrid Cryptographic Algorithm.” International Journal of Computer Science & Communication Networks,Vol 2(2), 277-283.
5. U.S. Department Of Commerce, National Institute Of Standards And Technology: Advance Encryption Standard (AES).
6. U.S. Department Of Commerce, William M. Daley, Secretary National Institute Of Standards And Technology, Raymond G. Kammer, Director: Data Encryption Standard (DES).

**Reference from cloud security paper(59 wala mera diya refrence hai)**

1. Yahia Alemami1,2, Ali M. Al-Ghonmein2 , Khaldun G. Al-Moghrabi2 , Mohamad Afendee Mohamed1 “Cloud data security and various cryptographic algorithms” International Journal of Electrical and Computer Engineering (IJECE) Vol. 13, No. 2, April 2023, pp. 1867~1879 ISSN: 2088-8708, DOI: 10.11591/ijece.v13i2.pp1867-1879
2. P. More, S. Chandugade, S. M. S. Rafiq, and P. Pise, “Hybrid encryption techniques for secure sharing of a sensitive data for banking systems over cloud,” in 2018 International Conference on Advances in Communication and Computing Technology (ICACCT), Feb. 2018, pp. 93–96, doi: 10.1109/ICACCT.2018.8529545.
3. K. R. Sajay, S. S. Babu, and Y. Vijayalakshmi, “Enhancing the security of cloud data using hybrid encryption algorithm,” Journal of Ambient Intelligence and Humanized Computing, no. 2018, Jul. 2019, doi: 10.1007/s12652-019-01403-1.
4. V. Goyal and C. Kant, “An effective hybrid encryption algorithm for ensuring cloud data security,” in Big Data Analytics. Springer, Singapore, 2018, pp. 195–210.
5. Y. K. Kumar and R. M. Shafi, “An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem,” International Journal of Electrical and Computer Engineering (IJECE), vol. 10, no. 1, pp. 530–537, Feb. 2020, doi: 10.11591/ijece.v10i1.pp530-537.
6. L. Teng, H. Li, S. Yin, and Y. Sun, “A modified advanced encryption standard for data security,” International Journal of Network Security, vol. 22, no. 1, pp. 112–117, 2019, doi: 10.6633/IJNS.202001.22(1).11.
7. H. Abroshan, “A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms,” International Journal of Advanced Computer Science and Applications, vol. 12, no. 6, pp. 31–37, 2021, doi: 10.14569/IJACSA.2021.0120604.
8. I. A. Awan, M. Shiraz, M. U. Hashmi, Q. Shaheen, R. Akhtar, and A. Ditta, “Secure framework enhancing AES algorithm in cloud computing,” Security and Communication Networks, vol. 2020, pp. 1–16, Sep. 2020, doi: 10.1155/2020/8863345.
9. M. Kumar, A. Kishor, J. Abawajy, P. Agarwal, A. Singh, and A. Y. Zomaya, “ARPS: An autonomic resource provisioning and scheduling framework for cloud platforms,” IEEE Transactions on Sustainable Computing, vol. 7, no. 2, pp. 386–399, Apr. 2022, doi: 10.1109/TSUSC.2021.3110245.
10. F. Mata, M. Kimwele, and G. Okeyo, “Enhanced secure data storage in cloud computing using hybrid cryptographic techniques (AES and blowfish),” International Journal of Science and Research (IJSR), vol. 6, no. 3, pp. 1702–1708, 2017, doi: 10.21275/ART20171804.
11. K. Dubey, S. C. Sharma, and M. Kumar, “A secure IoT applications allocation framework for integrated fog-cloud environment,” Journal of Grid Computing, vol. 20, no. 1, p. 5, Mar. 2022, doi: 10.1007/s10723-021-09591-x.

**Ye mera diya refrence hai**

1. Arpit Agrawal, Gunjan Patankar , “Design of Hybrid Cryptography Algorithm for Secure Communication”. International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 01 | Jan-2016
2. Saba Rehman , Nida Talat Bajwa , Munam Ali Shah , Ahmad O. Aseeri and Adeel Anjum  **“**Hybrid AES-ECC Model for the Security of Data over Cloud Storage**”** Electronics**2021**, 10, 2673.Online available at <https://doi.org/10.3390/electronics10212673>
3. Samiksha Sharma\* and Vinay Chopra **“**Data Encryption using Advanced Encryption Standard with Key Generation by Elliptic Curve Diffie-Hellman**”** International Journal of Security and Its Application(IJSIA) ISSN: 1738-9976 ,Vol. 11, No. 3 (2017), pp.17-28, available online at <http://dx.doi.org/10.14257/ijsia.2017.11.3.02>

**Cloud com 1,2,3,9,10,11,12,13,15,16,17,18,19**

1. M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud computing: Opportunities and challenges,” Information Sciences, vol. 305, pp. 357–383, Jun. 2015, doi: 10.1016/j.ins.2015.01.025.
2. M. N. O. Sadiku, S. M. Musa, and O. D. Momoh, “Cloud computing: Opportunities and challenges,” IEEE Potentials, vol. 33, no. 1, pp. 34–36, Jan. 2014, doi: 10.1109/MPOT.2013.2279684.
3. A. A. Soofi, M. I. Khan, and Fazal-e-Amin, “A review on data security in cloud computing,” International Journal of Computer Applications, vol. 94, no. 5, pp. 12–20, May 2014, doi: 10.5120/16338-5625.
4. S. Singh, Y.-S. Jeong, and J. H. Park, “A survey on cloud computing security: Issues, threats, and solutions,” Journal of Network and Computer Applications, vol. 75, pp. 200–222, Nov. 2016, doi: 10.1016/j.jnca.2016.09.002.
5. B. S. P. Mishra, H. Das, S. Dehuri, and A. K. Jagadev, Cloud computing for optimization: Foundations, applications, and challenges, vol. 39. Cham: Springer International Publishing, 2018.
6. K. G. Al-moghrabi, A. M. Al-ghonmein, and M. Z. Alksasbeh, “Towards a cloud computing success model for hospital information system In Jordan,” International Journal of Advanced Trends in Computer Science and Engineering, vol. 10, no. 2, pp. 1121–1127, Apr. 2021, doi: 10.30534/ijatcse/2021/891022021.
7. Z. N. Rashid, S. R. M. Zebari, K. H. Sharif, and K. Jacksi, “Distributed cloud computing and distributed parallel computing: A review,” in 2018 International Conference on Advanced Science and Engineering (ICOASE), Oct. 2018, no. June, pp. 167–172, doi: 10.1109/ICOASE.2018.8548937.
8. M. Almubaddel and A. M. Elmogy, “Cloud computing antecedents, challenges, and directions,” in Proceedings of the International Conference on Internet of things and Cloud Computing, Mar. 2016, pp. 1–5, doi: 10.1145/2896387.2896401.
9. S. A. Bello *et al.*, “Cloud computing in construction industry: Use cases, benefits and challenges,” Automation in Construction, vol. 122, Feb. 2021, doi: 10.1016/j.autcon.2020.103441.
10. N. Subramanian and A. Jeyaraj, “Recent security challenges in cloud computing,” Computers & Electrical Engineering, vol. 71, pp. 28–42, Oct. 2018, doi: 10.1016/j.compeleceng.2018.06.006.
11. M. Mohammed Sadeeq, N. M. Abdulkareem, S. R. M. Zeebaree, D. Mikaeel Ahmed, A. Saifullah Sami, and R. R. Zebari, “IoT and cloud computing issues, challenges and opportunities: A review,” Qubahan Academic Journal, vol. 1, no. 2, pp. 1–7, Mar. 2021, doi: 10.48161/qaj.v1n2a36.
12. A. T. Atieh, “The next generation cloud technologies: A review on distributed cloud, fog and edge computing and their

opportunities and challenges,” Research Berg Review of Science and Technology, vol. 1, no. 1, pp. 1–15, 2021.

1. S. S. Khan and R. Tuteja, “Security in cloud computing using cryptographic algorithms,” International Journal of Innovative Research in Computer and Communication Engineering, vol. 03, no. 01, pp. 148–154, Feb. 2015, doi: 10.15680/ijircce.2015.0301035.