REVIEW OF VARIOUS ALGORITHMS FOR DATA ENCRYPTION USED IN HYBRID TECHNIQUE TO IMPLEMENTATION IN DATABASE

Satinder, Research Scholar, Deptt. of Computer Science & Engineering , School of Engineering & Technology, Om Sterling Global University, Hisar, Haryana, India satindercse192@osgu.ac.in,
Dr. Parveen Sehgal, Professor, Deptt. of Computer Science & Engineering , School of Engineering & Technology, Om Sterling Global University, Hisar, Haryana, India

ABSTRACT

In this present scenario 99 percentpeople of the world are mostly interested in communicating with each other through digital platforms. But out of those, some people are not encrypted their data which causesa high chance of losing data or hacking. Now a day's security of information has become a very important aspect in every field of life. Cryptography is one of the techniques which is used by people for hiding information and keeping them confidential from the attack of intruder. Presently based on hybridization, hybrid encryption technique is studied. This study is related to the information from 2000 to 2021 and all the concepts of hybrid cryptography are analysed in data storage environment. For this purpose,nearly 100 papers have been researched and out of them 36 papers are reviewed and taken into consideration after filtration. In this paper, our main purpose is to provide information related to previous reviews and their major focus on the study about user of various algorithms of hybrid technique. The hybrid approach is very useful in comparison to others in terms of keeping data in more redundant form. By using this method, users can protect their data and help to keep them confidential and secret and provides privacy and integrity from hackers.

Keyword: Hybrid Encryption, Database, Symmetric and Asymmetric

INTRODUCTION

In the current era of technology, every work these days is being done by computer. Today, we are living in the digital world where everything from using social networking sites for chatting purpose to use of net banking to conduct online transactions, every minute work is being done online with the help of computers. Though we are transitioning from an offline to an online world in every way, using online services comes with security and privacy risks because all of the data is stored in databases. So, to avoid the data misuse protection of user data is of utmost important.

Authorization and authentication are two crucial procedures that are used to protect data from the front end (i.e., user side) that is being accessed by the user. Authorization denotes whether or not a person has the right to access the data, while authentication denotes user identification, which is typically accomplished with the aid of a username and password.

Saving the encrypted data in the database is another significant means or way to protect the data. Encryption is that process with the help of which plain text can be transformed into unreadable form by using algorithms (also known as cipher text) except the person who has special knowledge about the key. The result or output which we get from this process is known as cipher text and the process used to make the information in readable form is called decryption. In other words, encryption is that process which transforms the data/information in the form which is not understandable by unauthorized person and only authorized person can access the data in its original form by the decryption of data. The key challenges that data encryption must overcome are the robustness of encryption techniques, the fulfilment of security criteria, and processing speed. The main issue arises when sending encrypted data and keys across unsecured remote channels or media. An effective solution for data protection provides management visibility and also able to ensure the security about end-to-end encryption, integrity, reliability and confidentiality through integrated security as application level. It is also helpful in finding the best technological security solution for the data exchange process.

Why Encryption Is Important?

A crucial component of data security and privacy is encryption. Every day, a lot of private information, including financial data and Social Security numbers, are transmitted online. Making sure that information is secure is crucial.

For data access, almost all websites and apps rely on user passwords and password verification tools. There isn't much people can do to encrypt their passwords aside from learning how to build a secure password. Customers can use password managers to the fullest extent possible, but in order to safeguard sensitive information, they must employ high-quality encryption.

Apart from other tools and procedures like two-factor authentication, businesses and government agencies that have access to customer and employee data must at the very least use AES encryption. The latter would guarantee that data accessibility is restricted to authorised users alone. Organisations must take all necessary precautions to protect customer information online. "Digital security is becoming increasingly important to protect us as we bank, shop, and communicate," according to the Software Alliance. And encryption is at the heart of that security.

Data Encryption

The process of converting data from a readable format into an encoded format is known as encryption. Data that has been encrypted cannot be read or used until it has been decrypted. As a result, encryption is the cornerstone of data security. A computer system's or database's information may be protected against theft by using encryption, which also ensures that only people with the proper authorization can access it.

Data encryption is used by both small and large businesses to safeguard user information when it is sent between a browser and a server. Data encryption software, encryption algorithms, and cyphers are used to create an encryption system that, in theory, can only be cracked with very powerful computers.

The two most popular encryption techniques are symmetric encryption and asymmetric encryption.

- **Symmetric encryption keys**, also known as private or secret key encryption, are ideally suited for solitary users and closed systems because the same keys are used for both encoding and decoding.
- **Asymmetric encryption keys**: In this case, two distinct keys—public and private—are employed. These are mathematically related to one another. Large numbers that have been paired together but are not identical make up the keys. The owner keeps the private key a secret, while distributing or making the public key available to the general public or only authorised recipients.

Hybrid Encryption

Hybrid encryption is a type of encryption that combines two or more encryption techniques. The advantages of each kind of encryption are combined, integrating both symmetric and asymmetric properties. As a result, it guarantees both speed and security. The best way to protect data is via hybrid encryption, provided that both the public and private keys are completely secure. The effectiveness of symmetric encryption and the simplicity of asymmetric encryption are combined in a hybrid encryption technique. Combining encryption methods offers several advantages. While symmetric encryption can speed up both types of encryption, asymmetric encryption can lengthen the encryption process. Increased overall security for the data transmission process results from combining encryption.

Some examples of encryption algorithms

For the purpose of transforming data into ciphertext, encryption methods are used. Although the encrypted data will appear random, an algorithm uses the encryption key to change the data in a predictable way so that it can still be decrypted and returned to plaintext.

Different encryption algorithms are created to serve various purposes.

- **DES encryption**
- **Triple DES encryption**
- **AES encryption**
- **RSA encryption**
- **Twofish encryption**

REVIEW OF LITERATURE

This literature review summarizes the research that has been published in the area of cryptography encryption models and techniques as it relates to secured information transmission. It analyzes various encryption models which are playing a vital role to achieve high level of security of information. It has been observed that so many encryption models and techniques have been developed which are using for protecting information over open channels. These are extremely complex to evaluate, hence offer a high level of security. As complexity increases the efficiency and performance decreases. By reviewing scholarly and non – scholarly works, the primary aim of this study is to make a case that continuing research into the enhancement of the speed and performance of cryptography encryption models and designing and implementing a Hybrid encryption technique which is much better than others in terms of execution speed and performance.

We've already indicated that the goal of this work is to present an overview of the several hybrid cryptography algorithms that are utilized, as well as studies that have used hybrid cryptography to store data. Using the right keywords, the entire search paper is explored. After locating close to 100 papers connected to the survey, topic filtering was carried out, producing a collection of 36 papers that were used in this review paper.

#	Authors	Year of publication	Base Encryption algorithms used/ Algorithms used in Hybrid Cryptosystem	Worked on Technology	Advantages /Result/ Conclusion
1	Mohammed et. al.	2000	Elgamal signatures, RSA blinding	Database Encryption	Proposed scheme is used to generate blinded as well as normal Elgamal digital signatures with advantage of being efficient, faster, and simpler than RSA and offers privacy enhancement.
2	Chang, C., and Chan, C.	2003	RSA (Rivest, Shamir, Adleman) master key	Database Encryption	Author introduced two new data base encryption system. (i) A field-oriented encryption system and (ii) A record-oriented encryption system with a user Master Key.
3	Hirani, S.A.	2003	Symmetric Algorithm	Common Encryption Comparison	AES is faster and more efficient than other encryption algorithms.
4	Nadeem A. and Javed M.	2005	DES, 3DES, AES, and Blowfish	Encryption Comparison	Author doing comparison in different algorithms by encrypting input files of various text and size. i)Blowfish ii)AES iii)3DES
5	Arshad, N.H., et al.	2008	Enhanced affine block cipher algorithm	Database Encryption	Change the mode off encryption and decryption, and suggest for hybrid fashion.
6	Kaur, K., et al.	2009	3KDES	Numeric to Numeric Encryption	A proper access control mechanism should be enforced for securing the data. This process is Easy to use and less computation
7	Yong-Xia, Z.	2010	DES and AES	Database Encryption	Author discuss some advantages and disadvantages of these algorithms and Suggest to improve security using hybrid algorithm.

8	Ren, W. and Miao, Z.	2010	DES, RSA	Blue Tooth Communication	Hybrid algorithm is produced using DES and RSA. Author uses 64-bit DES session key to provide high security at real time.
9	Elminaam, D.S., et al.	2010	AES, DES, 3DES, RC2, Blowfish, and RC6	Comparison	Blowfish had more efficient compared to other algorithms.
10	Kuppuswamy, P. and Chandrasekar, C.	2011	New Linear Block Ciper (NLBC)	Database Encryption	Author introduce a New Linear block cipher that worked on modular 37 whereas existing algorithm are based on modular 26.

11	Gutub, A.A. and Khan, F.A.	2012	DES(56 bit key)
			AES(128 bit key)
			RSA
				Designing Hybrid Crypto System	Key encryption with RSA, data encryption with DES & AES. Faster in execution and provides security

12	Pratap, C.M.	2012	DES, 3DES, AES, and Blowfish	Encryption Comparison	Author doing comparison in different algorithms and found that blowfish is more suitable than AES in terms of throughput, processing time and power consumption.
13	R. Patel, J. et al.	2013	AES and DES	Hybrid Encryption	Author presented an improved Hybrid AES-DES algorithm with adding irrational number in DES and integrating the AES algo into DES structure to improve security.
14	Nentawe Y.G.	2013	RSA (Rivest, Shamir, Adleman)	Network Environment Encryption	Design of data encryption/decryption in a network using RSA algorithm with specific message block size technique.

15	Vladescu, M. and Mattescu, G.	2013	Digital Signature and RSA	Small and Medium Enterprises Database	Author analyse these three ciphers techniques i.e. symmetric, asymmetric and hash function to develop a hybrid approach for Small and medium Enterprises that wants to offer a complex solution with the following characteristics: Unified system – all the crypto techniques are combined to solve each other's threats and weaknesses Structured system – encapsulating different types of ciphers to maximize the efficiency
16	Shmueli, E. et al.	2014	Traditional Architectures	Database Encryption	Author suggested a novel architecture for database encryption, which is based on placing the encryption module inside the Database Management Software (DBMS), just above the database cache, and using a dedicated technique to encrypt each database cell value together with its coordinates.
17	Saini, G. and Sharma, N.	2014	DSA and AES with Steganography	Cloud Database Encryption	Authors combine three algorithm DSA, DES and Steganography to provide security of data in cloud computing.
18	Patel, G.R. and Panchal, N.K.	2014	RSA and Diffie Hellman algorithm	Hybrid Encryption Using bitwise X-OR operation	The new proposed model provides more security compared to normal RSA algorithm.
19	Kuppuswamy, P. and Al-Khalidi, S.Q.	2014	Block cipher and Symmetric key	Hybrid Encryption	Developed a hybrid encryption algorithm using Block cipher and symmetric key which provides a more secure and convenient technique

					for secure data transmission for all kind application.
20	Singh, N. and Kaur, P.D.	2015	AES and RSA	Cloud Environment	A hybrid technique is proposed using two different techniques to provide the security to data on the higher level. This technique is beneficial in simple data transfer and storing the data on cloud. Some experimental analysis has been done on the basis of performance, execution time, response time and the CPU performance in VM telemetry view
21	Onyesolu, M.O. and Ogwara, N.O.	2017	3DES and AES	Using Symmetric Encryption for Hybrid	Provide more security from vulnerable attacks
22	Rani, S. and Kaur, H.	2017	AES and Elgamal	Network Security	decrease encryption and decryption time and increase throughput.
23	Deore, P. and Chaudhari, T.	2017	Symmetric and Asymmetric Algo	Database Encryption	Hybrid encryption technique uses symmetric encryption to encrypt data and then uses asymmetric encryption to encrypt secret key. This technique provides two level of protection to the database.
24	Babitha M. P. & Babu K. R. R.,	2017	AES-128	Cloud Computing Envronmentt	The algorithm AES-128 is used to improve the security and confidentiality of data. In this method, data is encrypted using 128 bit AES and then uploaded to the cloud.

25	Soman, V.K. and Natrajan, V.	2017	ECDSA, SHA256 and AES	Cloud Database / Server	Combination of ECDSA, SHA256 and AES is used for sending and receiving data message on the cloud. Authors using the SHA256 hashing algorithm along with the AES data encryption algorithms for the verification process and confidentiality and integrity to maintain data in the cloud.
26	Thangapandiyan, M., et al.	2018	Modified Elliptic Curve Cryptography (MECC)	Cloud Security	Separate key for all admin/User
27	Onyesolu, M.O. and Nnabugwu, N.C.	2018	RSA, AES and SHA512	Database Encryption Security	Author introduces the concept of a hybrid encryption approach with the combination of RSA and AES encryption models as well as SHA512, more secure and difficult to break.
28	Kamboj, L. et al.	2018	AES, RC6, Blowfish and BRA	Cloud Environment	Secure file storage in cloud environment. File is sliced into 8 equal parts and encrypted using these
29	Chinnasamy, P., and Deepalakshmi, P.	2018	RSA, AES and Blowfish	Cloud Storage for health data	An enhanced RSA algorithm is used to encrypt the blowfish keys. This hybrid method offered the benefits like fast encryption, large prime numbers for key generation and efficient key management.
30	Batra, M. et al.	2018	RC4, DES,AES	Cloud Storage Data (Hybrid Technique)	This hybrid algorithm will help users and cloud service provider to transmit their data without being stolen or affected.

31	Prakash, V. et al.	2019	Well-trusted fusion of RECTANGLE SPECK & LED	Hybrid Cryptograph y for IOT	A New Model of Light Weight Hybrid Cryptography for Internet of Things was introduced. Author created a hybrid using L.E.D. cipher which works closely like AES and author tried to change its weaknesses and hybrid it with other required algorithm in order to make according to our need for coming future.
32	Kumar, L.and Badal, N.	2019	AES, FHE	Cloud Security	Authors reviewed various hybrid cryptographic models and suggested to use AES and FHE which can overcome security issues like data confidentiality, privacy and integrity.
33	Fenghua, Z., et al.	2019	P-AES	Cloud Database	In this P-AES algorithm is proposed for increasing the efficiency of encryption and decryption efficiency and is more suitable for processing long data.
34	Poduval, V. et al.	2020	3-DES and Image steganography	Store on Cloud	The use of 3-DES algorithm has been done for the encryption purpose for getting suitable results and achieving higher security for the transmitted data.
35	Viswanath, G.R. and Krishna, P.V.	2020	AES and Fiestel Network Block Wise	Cloud Environment	The proposed framework uses the data uploading, slicing, indexing, encryption, distribution, decryption, retrieval and merging process to secure the big data stored in the multi cloud.

36	Mallepalli, P. K. and Tumma, S. R.	2021	Diffie-Hellman Key and Elliptic curve crypto	Big Data Security	author proposed a Lightweight Hybrid Scheme (LHS) which is based on Diffie-Hellman key exchange and Elliptic Curve Cryptography. LHS is capable of achieving power efficiency, reduction in computational overhead besides rendering equivalent security to asymmetric encryption techniques like RSA.

(Table 1:- All paper summaries form related to previous work/research)

By reviewing a lot of research work, somemajor problems are evaluated as stated below:

➢ Most of the encryption systems are vulnerable to attacks after some period of time, so there is a requirement of stronger encryption algorithms and models that provide a very high level of security.

➢ Since existing encryption systems are mainly concerned with complicated mathematical procedures. As complexity of algorithms increases, the execution speed decreases i.e. performance becomes low. So, there is a huge scope of introducing some new ideas and concepts with hybrid encryption systems so that performance of the system would be enhanced.

➢ Most of the hybrid technology works on cloud environment but on offline database they don't work properly.

CONCLUSION

In the foreseeable future, hybrid cryptography has a lot of potential as it results in increased efficiency, speed and throughputs by the combinations of various techniques and algorithms. Using hybrid cryptography has given rise to several opportunities and has further enabled researchers to address the difficult constraints of algorithms in their original efforts.Hybrid technique provides a great chance for improvement as it is easy to work on it.

The strategies and algorithms recommended in this work can be used to secure insecure media, and they are all very helpful. This document compiles research on hybrid cryptography methods from the previous 20 years, which will be useful for future studies in related fields. It is also useful to select a variety of topics relating to cryptography algorithms. Due to its Integer Factorization Problem, this study suggests that RSA should be used as much as possible in the various hybridization algorithms. The most popular and secure option for removing the various cryptographic methods' limitations is Diffie-Hellman. There is no question that a variety of cryptographic methods are provided here, but none of them are exhaustive or complete.

REFERENCES

[1] E. Mohammed, A. E. Emarah, and Kh. El-Shennawy, (2000) "A Blind Signature Scheme Based OnElGamal Signature", *Radio Science Conference*. 17th NRSC '2000. Seventeenth National, Page(s): C25/1 - C25/6.

[2] Chang, C., and Chan, C. (2003), "A database record encryption scheme using the RSA public key cryptosystem and its master keys," *International Conference on Computer Networks and Mobile Computing*. pp. 345-348, doi: 10.1109/ICCNMC.2003.1243067.

[3] S. Hirani, Energy Consumption of Encryption Schemes in Wireless Devices Thesis, University of Pittsburgh, Apr. 9, 2003, Retrieved October 1,2008 http://portal.acm.org/citation.cfm?id=383768.

[4] Nadeem, A., andJaved, M. (2005), "A performance comparison of data encryption algorithms",*International Conference on Information and Communication Technologies*, pp. 84-89, doi: 10.1109/ICICT.2005.1598556.

[5] Arshad, N.H., Shah, S.N., Mohamed, A.H., andMamat, A.M. (2008), "Database encryption using enhanced affine block cipher algorithm."*In Proceedings of the 10th WSEAS International Conference on Mathematical Methods and Computational Techniques in Electrical Engineering,*ISSN. 1790-5117, pp. 71-76.

[6] Kaur,K.,Dhindsa, K. S., and Singh G. (2009),"Numeric to Numeric Encryption of Databases: Using 3Kdec Algorithm." *IEEE International Advance Computing Conference*, pp. 1501-1505, doi: 10.1109/IADCC.2009.4809240.

[7] Yong-Xia, Z. (2010),"The Technology of Database Encryption.", *In 2nd International Conference on Multimedia and Information Technology*, vol. 2, pp. 268-270, doi: 10.1109/MMIT.2010.185.

[8] Ren, W. and Miao, Z. (2010), "A hybrid encryption algorithm based on DES and RSA in bluetooth communication". *InProceedings of the 2nd International Conference on Modeling, Simulation and Visualization Methods*, China, pp. 221-225, doi: 10.1109/WMSVM.2010.48.

[9] Elminaam, D.S., Abdual-Kader, H.M. andHadhoud, M.M. (2010), "Evaluating The Performance of Symmetric Encryption Algorithms",*International Journal of Network Security*, Vol.10, No.3, pp.216-222.

[10] Kuppuswamy, P., and Chandrasekar, C. (2011). "Enrichment of security through cryptographic public key algorithm based on block cipher", Indian Journal of Computer Science and Engineering, Vol. 2, No. 3, pp. 347-355.

[11] Gutub, A.A., and Khan, F.A. (2012), "Hybrid Crypto Hardware Utilizing Symmetric-Key and Public-Key Cryptosystems," *International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, pp. 116-121, doi: 10.1109/ACSAT.2012.44.

[12] Pratap,C.M. (2012), "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish" *Journal of Global Research in Computer Science*, vol. 3, no. 8, pp. 67-70.

[13] R.Patel, J., Bansode, R.S., and Kaul, V. (2013), "Hybrid Security Algorithms for Data Transmission using AES-DES", *International Journal of Applied Information Systems (IJAIS)*,vol. 2, no.2, pp. 15-21.

[14] Nentawe Y. G. (2013), "Data encryption and decryption using RSA algorithm in a network environment", International Journal of Computer Science and Network Security, vol. 13 No.7, pp. 9-13.

[15] Vladescu, M., andMateescu, G. (2013). "A Hybrid Approach of System Security for Small and Medium Enterprises", *Proceedings of the Federated Conference on Computer Science and Information Systems*, pp. 656-662.

[16] Shmueli, E., Vaisenberg, R., Gudes, E., andElovici, Y. (2014),"Implementing a database encryption solution, design and implementation issues", *Computers & Security*, Volume 44, ISSN 0167-4048,pp. 33-50.

[17] Saini, G. and Sharma, N. (2014), "Triple Security of Data in Cloud Computing.", *International Journal of Computer Science & Information Technologies*, Vol. 5(4), ISSN:0975-9646 pp. 5825-5827.

[18] Patel, G.R., and Panchal, N.K. (2014),"Hybrid Encryption Algorithm", *International Journal of Engineering Development and Research (www.ijedr.org)*, Vol. 2, Issue 2, ISSN: 2321-9939, pp.

2064-2070.

[19] Kuppuswamy, P., and Al-Khalidi, S.Q. (2014). “Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm”.*International Journal of Information and Computer Security*, Vol 6, Issue 4, pp 372–382, doi: 10.1504/IJICS.2014.068103.

[20] Singh, N. and Kaur, P.D. (2015), “A Hybrid Approach for Encrypting Data on Cloud to prevent DoS Attacks”. *International Journal of Database Theory and Application,* vol. 8, no. 3, ISSN: 2005-4270, pp. 145–154.

[21] Singh, P. and Kaur, K., "Database security using encryption,"*International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE)*, Greater Noida, India, pp. 353-358, doi: 10.1109/ABLAZE.2015.7155019.

[22] Onyesolu, M.O. and Ogwara, N.O. (2017), "On Information Security using a Hybrid Cryptographic Model", *International Research Journal of Computer Science (IRJCS)*, Vol. 4, Issue 11,ISSN: 2393-9842, pp 15-23.

[23] Rani, S. and Kaur, H. (2017), “Implementation and Comparison of Hybrid Encryption Model for Secure Network using AES and Elgamal”, *International Journal of Advanced Research in Computer Science*, Vol.8, no.3,pp 254-258.

[24] Deore, P. and Chaudhari, T. (2017), “Hybrid Encryption for Database Security”, *International Research Journal of Engineering and Technology (IRJET)*, Vol. 04, no. 11, pp 1264-1266.

[25] Babitha M. P. & Babu K. R. R., (2017) “Secure cloud storage using AES encryption”, *IEEE International Conference on Automatic Control & Dynamic Optimization Techniques*. pp. 859-864, doi: 10.1109/ICACDOT.2016.7877709.

[26] Soman, V.K., and Natarajan, V. (2017). "An enhanced hybrid data security algorithm for cloud", *International Conference on Networks & Advances in Computational Technologies (NetACT)*, pp. 416-419. doi: 10.1109/NETACT.2017.8076807.

[27] Thangapandiyan, M., Anand, P., and Sankaran, K. (2018),"Enhanced cloud security implementation using modified ECC algorithm." *IEEE Proceeding International Conference on Communication and Signal Processing (ICCSP)*, pp. 1019-1022, doi: 10.1109/ICCSP.2018.8524212.

[28] Onyesolu, M.O. andNnabugwu, N.C. (2018),” Design and Implementation of a Hybrid Database Encryption Model”,*International Journal of Innovative Research in Science, Engineering and Technology*, vol. 7, issue 3,pp.2066-2074, doi:10.15680/IJIRSET.2018.0703015.

[29] Kamboj, L., Bala, B., and Luthra, P. (2018) “Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm,” *International Journal of Advanced Research in Computer Science*, vol. 9, no. 2, pp. 773-776, doi: 10.26483/ijarcs.v9i2.5916.

[30] Chinnasamy, P., andDeepalakshmi, P. (2018). "Design of Secure Storage for Health-care Cloud using Hybrid Cryptography",*Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, pp. 1717-1720, doi: 10.1109/ICICCT.2018.8473107.

[31] Batra, M., Dixit, P., Rawat, L., and Khalkar, R. (2018), “Secure File Storage In Cloud Computing Using Hybrid Encryption Algorithm,” *International Journal of Computer Engineering and Applications*, vol. 19, no. 6, pp. 30-36.

[32] Prakash, V, Singh, A.V. and Khatri, S.K. (2019), "A New Model of Light Weight Hybrid cryptography for Internet of Things." In 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 282-285.

[33] Kumar, L., and Badal, N. (2019), “A Review on Hybrid Encryption in Cloud Computing”,*Proceeding 4th International Conference Internet of Things Smart Innovation Usages, (IoT-SIU)*, pp. 1-6, doi: 10.1109/IoT-SIU.2019.8777503.

[34] Fenghua, Z., Yaming, C., Meng, W., and Wu, Q. (2019), “Hybrid Encryption Algorithms for Medical Data Storage Security in Cloud Database,” *International Journal of Database Management*

Systems, vol. 11, no. 01, pp. 57–73, doi: 10.5121/ijdms.2019.11104.

[35] Poduval, V., Koul, A., Rebello, D., Bhat, K. and Wahul, R.M.,(2020), "Cloud based Secure Storage of Files using Hybrid Cryptography and Image Steganography", *International Journal of Recent Technology and Engineering (IJRTE)*, Vol. 8,no. 6, ISSN: 2277-3878, pp. 665-667.

[36] Viswanath, G.R., and Krishna, P.V. (2020). "Hybrid encryption framework for securing big data storage in multi-cloud environment ",*Evolutionary Intelligence*, S.I. 14, pp. 691-698, doi: https://doi.org/10.1007/s12065-020-00404-w

[37] Mallepalli, P. K., and Tumma, S. R. (2021). A lightweight hybrid scheme for security of big data. Materials Today: Proceedings, ISSN 2214-7853, pp. 1-6, doi:10.1016/j.matpr.2021.03.151