RESEARCH ARTICLE | JUNE 05 2024

A survey report on cloud based cryptography and steganography procedures

Mohammed Ali ✉; P. Praveen; Sampath Kumar; Sallauddin Mohmmad; M. Sruthi

AIP Conf. Proc. 2971, 020040 (2024)
https://doi.org/10.1063/5.0196050

View Online
Export Citation

A Survey Report on Cloud based Cryptography and Steganography procedures

Mohammed Ali[1, a)], P Praveen[1], Sampath Kumar[1], Sallauddin Mohmmad[1] and M. Sruthi[2]

[1]School of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana, India.
[2] Sumathi Reddy Institute of Technology for Women, Warangal, Telangana, India.

[a)] Corresponding author: niharali@gmail.com

Abstract. This is an era of successful implementation of cryptography and Steganographic technique in cloud environment where people share their data to each other over the internet using different protocols like Http/Https, web sockets, FTP, SMTP etc. For the security aspects of data cryptography plays an important role. And due to increase in usages of the internet the cyber-attacks have also increased over the past few years. Thus, this problem gives rise to steganography techniques that is some advanced secret sharing techniques are evolved to hide data in other files after applying cryptography to the confidential/secret data. This paper speaks about the different existing cryptography and steganography techniques in cloud environments.

INTRODUCTION

In this modern era there are several communication techniques which are used to send messages between receiver and transmitter. Due to the increase in online implementation of transferring data between sender and receiver, the threat of losing confidential data through unauthorized access also increases.

This gives rise the requirement to have some protocols for secret data transmission between sender and recipient over the web. Thus, some data encryption and data hiding techniques are introduced over the time to secure confidential data from unauthorized access. [2] The transmitted data can be directly sent to the cloud for computation, for storage purposes in databases or it can be sent to another person for direct communication [14,34]. In all these cases the data has to cross many network nodes like gateways, switches, routers, servers etc. This makes the communication channel insecure. So it is required to have some protocols which can be used to make data inaccessible to any kind of unauthorized access at intermediate nodes [29]. Some techniques to secure data are described below.

CRYPTOGRAPHY

The art of manipulating data in human unreadable form is called Cryptography (i.e. data encryption). In most of the cases cryptography is the widely used technique to transmit data all over the internet [4,13,35].

International Conference on Research in Sciences, Engineering, and Technology
AIP Conf. Proc. 2971, 020040-1–020040-8; https://doi.org/10.1063/5.0196050
Published by AIP Publishing. 978-0-7354-4866-7/$30.00

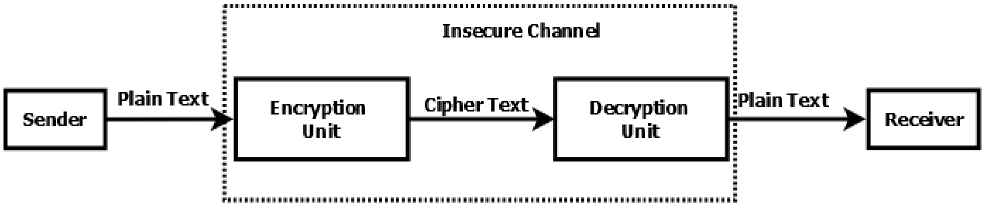

FIGURE 1. Block Diagram of Cryptography

The cipher text is a result of encryption performed on plain text. As shown in figure 1. the cipher text is sent to the recipient through an insecure channel. Thus, the data sent to the receiver is not safe i.e. one can access that data at intermediate nodes and if he/she has the decryption key then the data could be accessed easily. [13,36] This means we cannot guarantee that the data transferred over the communication channel is secure and safe from unauthorized access if we just apply cryptography on it.

STEGANOGRAPHY

A method of concealing one type of data into another one, to make the original data unrecognizable for humans is known as Steganography (i.e. data hiding) [3,37] as shown in figure 2.

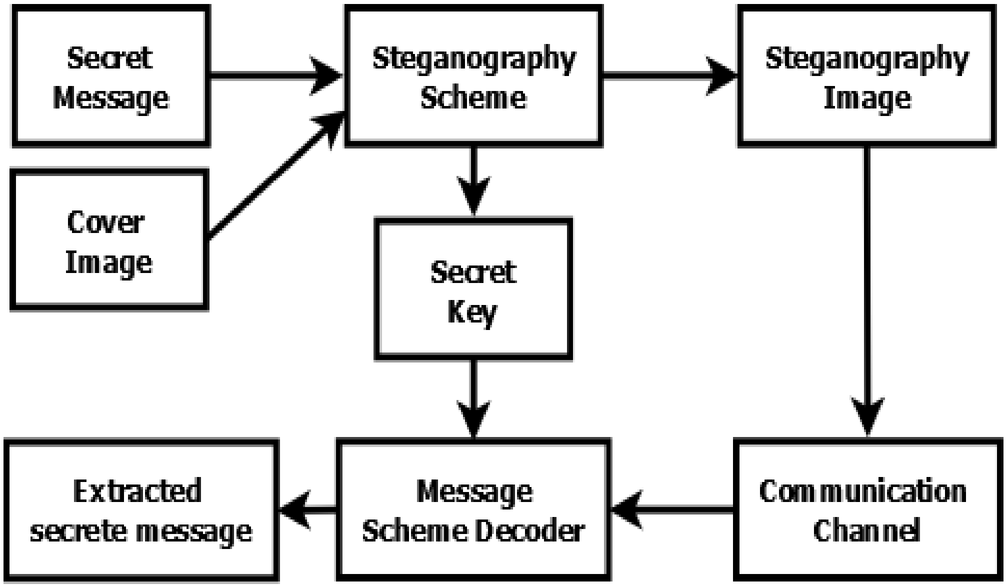

FIGURE 2. Steganography Block Diagram [15]Cryptography

The cover image is the output of some consecutive operations on a carrier called stego image as shown in Fig-1. The plain text message is concealed into the stego image using a key called stego key. The cover image is now sent to the receiver through a channel which is insecure [3]. In this case the date is hidden into the image. Means if someone got access to this stego image at any intermediate node then he/she is not able to recognize the original hidden message. Thus, steganography is the safer method to communicate and to send confidential data over the web [34,38].

The overview of the research is ordered in the following manner: Section-1 is Introduction, Section-2 is highlighting the literature review of cryptography and steganography in cloud. In literature review we talked about different existing techniques which are used in both cryptography and steganography. In section-3 related work which is already done is elaborated in tabular form. The last section i.e. section-4 speaks about the conclusion of existing research in a decent way [32,33,39].

LITERATURE REVIEW

CLOUD

All the hardware technologies, distributed computing systems and dynamic platforms give rise to a cyberinfrastructure which is known as cloud. The cloud provides online access to services like software, online data storage and file management systems etc. [1] [2]. There are 3 layers in the cloud which are described below and in figure 3.

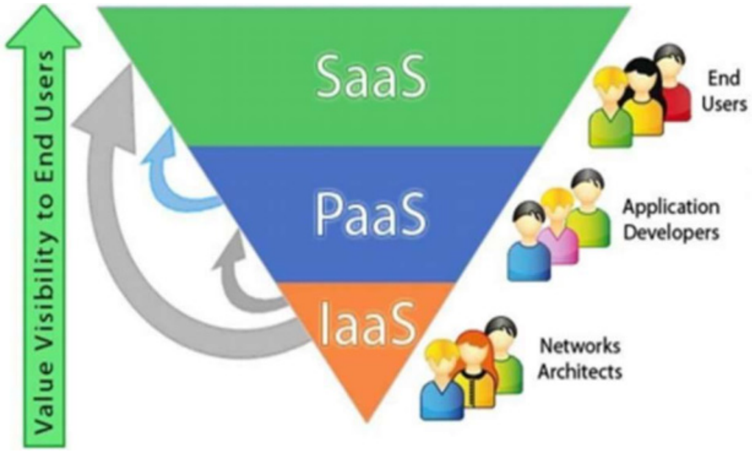

FIGURE 3. Cloud Computing Structure [2]

1) Infrastructure as a Service: This is also referred to as IAAS. In this type of cloud layer, the hardware resources such as file storing databases and physical or virtual machines for file handling on rent. For example, Google Chrome, Amazon EC2 etc. are the examples of IAAS cloud [30,31,42].

2) Platform as a Service: PAAS is a type of cloud layer which includes all the virtual computing machines like online programming execution, databases and web servers. The PAAS is the base infrastructure platform for IAAS. Some examples of PAAS cloud models are Heroku, Google app engine etc. [32,35,40,41].

3) Software as a Service: SAAS is the easiest model for the end users. Users do not have to worry about the installation of the software and its setup on the cloud. The service providers will do that for you. The users just have to pay for its service and can use the service directly. Microsoft office, Adobe Photoshop, Google apps etc. are some examples of Software as a service model [33,36,43,44].

CRYPTOGRAPHY TECHNIQUES

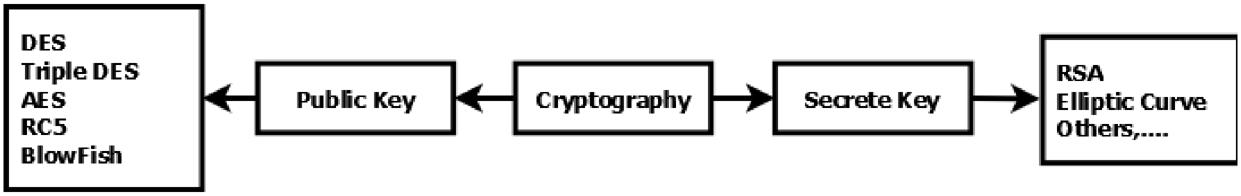

FIGURE 4. Classification of Cryptography [4]

There are mainly 2 ways as show in figure 4 to implement cryptography. These two techniques are described below.

1) Secret Key Cryptography: In this type of cryptography, a same key is used for both data encryption and decryption. Both the receiver and transmitter have the key which is used in the data processing unit to encrypt and decrypt data. DES, AES, Triple DES are some examples of this type of cryptography techniques [4,8,45].

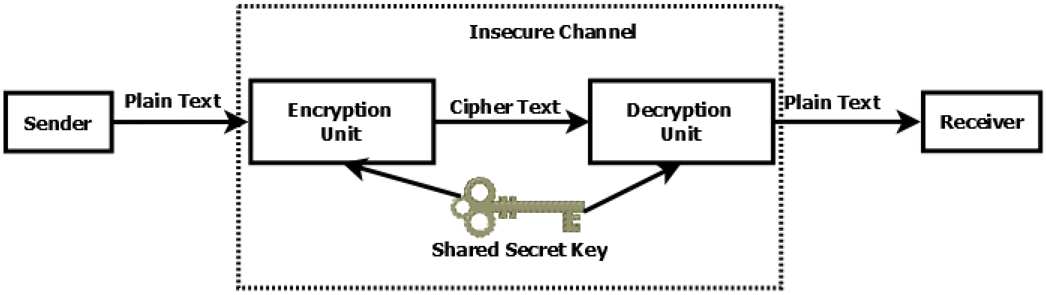

FIGURE 5. Secret Key Cryptography [4].

1.1 Data Encryption Standard (DES): This algorithm was introduced in 1977 by IBM. A 64-bit stream block is taken at a time & the cipher text bits are generated by applying XOR operation on the bits after manipulating the position of bits inside the block [8,16,46]. The 3DES uses a 192-bit size key where TDES uses 3 keys to generate cipher text bits. Due to large bit manipulation count,

these methods are more time consuming than DES [4] [8].

1.2 Advanced Encryption Standard (AES): The AES was introduced in 1997 by the National Institute of Standards and Technology (NIST). In this method a minimum 128-bits block is used. Certain operations like substitution of bits, changing the rows and mixing the columns are performed to generate output bits [4] [8].

1.3 Blowfish Algorithm: Blowfish is the most efficient technique among all existing techniques. A variable key length between 32 to 448 bits is used. Basically 2 steps are involved in this algorithm. [8,16,47]

- Data Encryption: A function is repeated 16 times with key dependent permutation and substitution. [4]
- Sub key Generation: It includes conversion of the key ranging 448 bits to 4168 bits. [4]

2) Public Key Cryptography: When 2 different keys are used i.e. one key for data encryption and the other one is for data decryption. This type of cryptography is known as public key cryptography.

RSA is an example of public key cryptography [34].

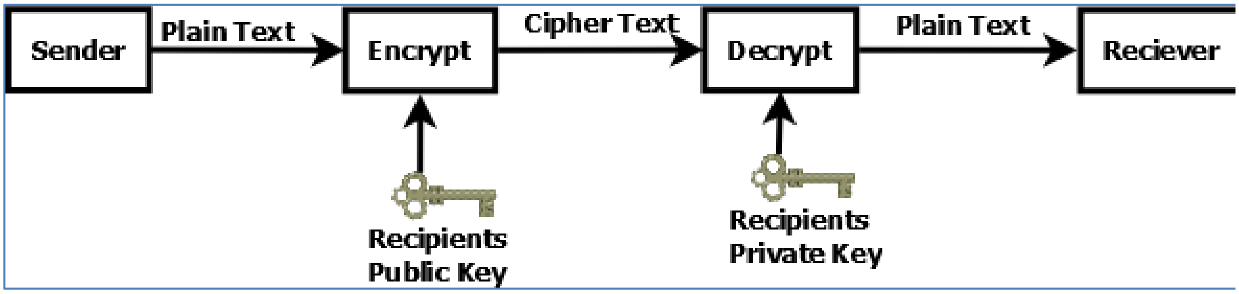

FIGURE 6. Public Key Cryptography [37]

RSA

The RSA algorithm was invented by Rivest Shamir, Adelman [4]. This method uses 2 different keys i.e. a public key and a private key. Encryption is performed by using the public key on the other hand, data decryption is done by using a private key [4] [8].

3) Comparison of Different Cryptography Algorithms:

TABLE 1. Comparison of Cryptographic Algorithms [4]

Algorithm	Inventor	Key Size	Block Size
		(bytes)	(bytes)
DES	IBM	56	64
3DES	IBM	168	64
AES	Joan Daemen& Vincent Rijmen (1998)	256	128
BlowFish	Bruce Schneier (1993)	448	64

Steganography Techniques

The steganography or the data hiding provides an extra security layer to confidential data. The output file seems to be normal for human eyes and other computational operations. On the other hand, if it is processed with the proper decryption key, then only we can extract the hidden message inside the file. There are a ton of ways to conceal data inside a file. Some of these are described below. [11] [6]

1) Binary File Technique: We can add Watermark or a trademark on a file to hide data inside the watermark. The cover media is a binary file in this case. This technique is simple to implement. The only drawback of this technique is that it makes the viewers think about the file because the watermarks may be visible to human eyes. [3] [6].

2) Text Technique: A text document is used to cover the original message in this technique. We can manipulate some characters of the document file to represent the hidden message characters. To keep the process efficient matrix block selection can be used, in which we can select the characters by making a matrix inside the text file [6] [12].

3) Image hiding: An image is used as cover media in this case. We can use LSB method i.e. the least significant bits are used to store original message bits in the image [6]. On the other hand, pixel mapping technique is also possible to hide data by manipulating pixel's RGB values [5] [12].

RELATED WORK

Several techniques have evolved in the past few years to secure data over the cloud. Some of these techniques are described in the following table 2:

CONCLUSION

From the above explanation of recent techniques, it is concluded that several techniques are evolved w.r.t time and each technique has its own strong zone of implementations. A technique without any involvement of a third party service can be considered as a safer and robust technique. The techniques which use HTML or CSS tags and labels are capable of having large capacity to hide data with least effect on original file size.

On the other hand, this is not an efficient way to hide data inside an HTML webpage because one has to hide data manually inside the HTML document, this makes the process less efficient as it is time consuming as well.

TABLE 2. Comparison of Cryptographic Algorithms [4]

Sl. No.	Citation	Research Findings
1	[1-5]	“A session key is generated to hide data using PMM (Pixel Mapping Method). Each session has a different key. The session key is sent with the image after encryption. So first we have to decrypt the key to decrypt the rest of data.”
2	[6-10]	“Different techniques are used by the authors to hide data inside a webpage.
3	[11-15]	Changing the CSS style tags like, the use of extra space, upper and lower case alphabets will not affect the output on the webpage but it can be considered as a ‘0’ or ‘1’ value. Thus, by calculating these binary values, a bit stream of hidden data can be made.”
4	[16-20]	“The image is divided into several blocks. Each block has pixels having the same MSB values. According to the MSB other values of bits are changed. This method is only applicable for billboard type displays.”
5	[20-25]	“The authors use HTML space codes to hide data inside a webpage. Several space codes like ‘&nbsp’, ‘&emsp’ etc. can be used inside a webpage in different manner regardless of output behavior. These codes are mapped with a symmetric key binary data table and thus this table can be used to encrypt and decrypt data.”
6	[26-30]	“The system uses a public key scheme to hide data. The public key and a private key are generated when a user does registration on the public cloud. The public key is used as an encryption key where the private key is used for data decryption when there will be data migration over the cloud.”
7	[30-37]	“The authors introduced a new technique to implement steganography in a HTML/XML document. They use techniques like white spaces in tags, appearing order of elements/attributes, use of empty tags etc. only in even number of rows in the document.”

REFERENCES

1. Mohamed A. Mahfouz, d M. A. Ismail, Fuzzy Relatives of the CLARANS Algorithm With Application to Text Clustering, International Journal of Electrical and Computer Engineering, 370-377, (2009).
2. Pushpa.R. Suri, Mahak, Image Segmentation With Modified K-Means Clustering Method, International Journal of Recent Technology and Engineering, 176- 179, (2012).
3. Mohammed Ali Shaik, T. Sampath Kumar, P. Praveen, and R. Vijayaprakash, Research on Multi-Agent Experiment in Clustering, International Journal of RecentTechnology and Engineering (IJRTE), 8, 1S4, 1126-1129, (2019).
4. Praveen. P and Ch. JayanthBabu. “Big Data Clustering: Applying Conventional Data Mining Techniques in Big Data Environment.”. Innovations in Computer Science and Engineering, Lecture Notes in Networks and Systems 74, Springer Singapore (2019).
5. Mohammed Ali Shaik, Dhanraj Verma, , Agent-MB-DivClues: Multi Agent Mean based Divisive Clustering, Ilkogretim Online - Elementary Education, 20(5), 5597-5603, (2021)
6. T. Sampath Kumar, B. Manula, A Comprehensive Study on Single Sign on Technique, International Journal of Advanced Science and Technology (IJAST) 127, 430-435, (2019).
7. N. Paivinen, “Clustering with a Minimum Spanning Tree of Scale- free-like Structure”, in Pattern Recognition Letters, (Elsevier, 2005) , 26(7), 921-930.
8. Mohammed Ali Shaik and Dhanraj Verma, “Enhanced ANN training model to smooth and time series forecast”, in IOP Conf. Ser.: (Mater. Sci. Eng 2020). 981022038.
9. T. Sampath Kumar, B. Manula,"Competent multi-level encryption methods for implementing cloud security", in IOP Conf. Series: (Materials Science and Engineering, 2020) 022039 IOP Publishing.
10. P Pramod Kumar and K Sagar, “A Relative Survey on Handover Techniques in Mobility Management”, in IOP Conf. Ser.: (Mater. Sci 2019), Pp. 12023-12027.

11. Mohammed Ali Shaik, Dhanraj Verma, P Praveen, K Ranganath and Bonthala Prabhanjan Yadav, , RNN based prediction of spatiotemporal data mining, in IOP Conf. Ser.: (Materials Science and Engineering, 2020) 981 022027.
12. Murtagh F. The Haar, Wavelet transform of a dendrogram, Journal of Classification 24:3–32, (2007).
13. Mohammed Ali Shaik, Time Series Forecasting using Vector quantization, International Journal of Advanced Science and Technology (IJAST), 29(4), 169-175, (2020).
14. P. Praveen, B. Rama and T. Sampath Kumar, "An efficient clustering algorithm of minimum Spanning Tree," in Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB, Chennai, 2017), Pp. 131-135.
15. Mohammed Ali Shaik, A Survey on Text Classification methods through Machine Learning Methods, International Journal of Control and Automation (IJCA), 12(6), 390-396, (2019).
16. T. Sampath Kumar, and B. Manjula, Perusing on Cloud Computing and its Security Issues, International Journal of Engineering and Advanced Technology (IJEAT), 9(2), 123-129, (2019).
17. N. Bhatia and V. Ashev, Survey of nearest-neighbor techniques, International Journal of Computer Science and Information Security, 8(2), 302–305, (2010).
18. P.Praveen, B.Rama, An Efficient Smart Search Using R Tree on Spatial Data, Journal of Advanced Research in Dynamical and Control Systems, 4, 1943-1948 (2019).
19. Praveen P., Shaik M.A., Kumar T.S., Choudhury T. (2021) Smart Farming: Securing Farmers Using Block Chain Technology and IOT. In: Choudhury T., Khanna A., Toe T.T., Khurana M., GiaNhu N. (eds) Blockchain Applications in IoT Ecosystem. EAI/Springer Innovations in Communication and Computing. Springer.
20. T.Sampath Kumar, B.Manjula, Asymmetric AES Algorithm for Cloud Security, International Journal of Future Generation Communication and Networking 12(5), 301- 305, (2019).
21. R. Ravi Kumar, M. Babu Reddy and P. Praveen, "A review of feature subset selection on unsupervised learning," in Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB, Chennai, 2017), pp.163-167.
22. Mohammed Ali Shaik, Geetha Manoharan, B Prashanth, NuneAkhil, Anumandla Akash and Thudi Raja Shekhar Reddy, "Prediction of Crop Yield using Machine Learning", in International Conference on Research in Sciences, Engineering & Technology, (AIP Conf. Proc. 2418, 2022), Pp.020072-1–020072-8, doi.org/10.1063/5.0081726.
23. S.Vijayarani, S.Nithya. An Efficient Clustering Algorithm for Outlier Detection, International Journal of Computer Applications. 22-27, (2011).
24. Mohammed Ali Shaik and Dhanraj Verma, "Predicting Present Day Mobile Phone Sales using Time Series based Hybrid Prediction Model", International Conference on Research in Sciences, Engineering & Technology, in (AIP Conf. Proc. 2418, 2022), Pp. 020073-1–020073-9.
25. XV. Zhang, D. Chao, and J. Wang, Composite Quantization for Approximate Nearest Neighbor Search, in ICML, 1234-1239, (2014).
26. Yerrolla Chanti, Seena Naik Korra, Bura Vijay Kumar, A Harshavardhan, D Kothandaraman, New Technique using an IoT Robot to Oversight the Smart Domestic Surroundings, Studia Rosenthaliana (Journal for the Study of Research), issue. 0039-3347, 2019.
27. Ravi Kumar, R., Mohmmad, S., Shabana, Kothandaraman, D., Ramesh, D, "Static Hand Gesture Recognition for ASL Using MATLAB Platform, Computer Communication", Networking and IoT. Lecture Notes in Networks and Systems, Springer, Singapore, 459, (2023).
28. Y Chanti, Mahesh Akarapu, B Swathi, B Vijaykumar, D Kothandaraman, Using the NI PXI platform for Li Fi-enabled intelligent transportation systems, AIP Conference Proceedings, vol. 2418, issue. 1, 2022, pp.020071
29. Mohammed Ali Shaik and Dhanraj Verma, "Prediction of Heart Disease using Swarm Intelligence based Machine Learning Algorithms", in International Conference on Research in Sciences, Engineering & Technology, (AIP Conf. Proc. 2418, 2022), Pp.020025-1–020025-9, doi.org/10.1063/5.0081719.
30. Y. Chen, T. Guan, and C. Wang, Approximate nearest neighbor search by residual vector quantization, Sensors, 10(12), 11259– 11273, (2010).
31. M. A. Shaik, S. k. Koppula, M. Rafiuddin and B. S. Preethi, (2022), "COVID-19 Detector Using Deep Learning", in International Conference on Applied Artificial Intelligence and Computing (ICAAIC, 2022), pp. 443-449.

32. Mohammed Ali Shaik, MD.Riyaz Ahmed, M. Sai Ram and G. Ranadheer Reddy, "Imposing Security in the Video Surveillance", in International Conference on Research in Sciences, Engineering & Technology, (AIP Conf. Proc. 2418, 2022), Pp. 020012-1 to 020012-8
33. Yu-Chen Song, J.O'Grady, G.M.P.O'Hare, Wei Wang, "A Clustering Algorithm incorporating Density and Direction", IEEE Computer Society, (CIMCA 2008).
34. Mohammed Ali Shaik, Praveen Pappula, T Sampath Kumar, Predicting Hypothyroid Disease using Ensemble Models through Machine Learning Approach", European Journal of Molecular & Clinical Medicine, 9 (7), 6738-6745, (2022).
35. Mendu, M., Krishna, B., Sandeep, C.H., Mahesh, G., Pallavi, J. Development of real time data analytics based web applications using NoSQL databases 2022 AIP Conference Proceedings 2418 020038, doi.org/10.1063/5.0082146
36. Akarapu M., Martha S., Donthamala K.R., Prashanth B., Sunil G., Mahender K. Checking for Identity-Based Remote Data Integrity Cloud Storage with Perfect Data Privacy 2020 IOP Conference Series: Materials Science and Engineering 981 2 22034 10.1088/1757-899X/981/2/022034.
37. Bojja P., Divya V., Naidu M.G.M., Ashok G., Kumaraswamy E. The prediction of No2and O3concentrations in ambient air using soft computing techniques for hyderabad model 2022 AIP Conference Proceedings 2418 30016 10.1063/5.0091515.
38. Bojja P., Kiran C., Thilak B., Bhargav A., Mahender K. Development of medical assistance systems by cloud computing networks with Covid-19 datasets 2022 AIP Conference Proceedings 2418 30006 10.1063/5.0091514.
39. Magesh Kumar S., Auxilia Osvin Nancy V., Balasundaram A., Korra S.N., Kothandaraman D., Sudarshan E. Innovative Task Scheduling Algorithm in Cloud Computing 2020 IOP Conference Series: Materials Science and Engineering 981 2 22023 10.1088/1757-899X/981/2/022023.
40. Prasad C.H.S.S., Yadav B.P., Mohmmad S., Gopal M., Mahender K. Study of threats associated with cloud infrastructure systems 2020 IOP Conference Series: Materials Science and Engineering 981 2 22055 10.1088/1757-899X/981/2/022055.
41. Yadav B.P., Prasad C.S.S., Padmaja C., Korra S.N., Sudarshan E. A Coherent and Privacy-Protecting Biometric Authentication Strategy in Cloud Computing 2020 IOP Conference Series: Materials Science and Engineering 981 2 22043 10.1088/1757-899X/981/2/022043.
42. Rajasri Reddy I., Reddy C.V.K., Rao Y.V.D., Chandra Shekar A. Comparison of Tests for Isomorphism in Planetary Gear Trains 2020 IOP Conference Series: Materials Science and Engineering 981 4 42023 10.1088/1757-899X/981/4/042023.
43. Sammaiah P., Rushmamanisha K., Praveenadevi N., Rajasri Reddy I. The Influence of Process Parameters on the Surface Roughness of the 3d Printed Part in FDM Process 2020 IOP Conference Series: Materials Science and Engineering 981 4 42021 10.1088/1757-899X/981/4/042021.
44. Vasanthi P., Senthil Selvan S., Murthi P., Rajasri Reddy I., Poongodi K. Impact of Partial Replacement of Cement by Coconut Shell Ash and Coarse Aggregate by Coconut Shell on Mechanical Properties of Concrete 2020 IOP Conference Series: Materials Science and Engineering 981 3 32080 10.1088/1757-899X/981/3/032080.
45. Bhushan T., Chandrashekhar A., Venkat Prasat S., Rajasri Reddy I. Effect of Substrate Surface Roughness on Adhesion of Titanium Nitride Coatings Deposited by Physical Vapour Deposition Technique 2020 IOP Conference Series: Materials Science and Engineering 981 4 42022 10.1088/1757-899X/981/4/042022.
46. Dule C.S., Rajasekharaiah K.M., Dr., Prashanth B. Analyze the Legislative Frameworkrelating to Surveillance and Right to Privacy: Issues and Challenges 2020 IOP Conference Series: Materials Science and Engineering 981 2 22063 10.1088/1757-899X/981/2/022063.
47. Rajasekharaiah K.M., Dr., Dule C.S., Sudarshan E. Cyber Security Challenges and its Emerging Trends on Latest Technologies 2020 IOP Conference Series: Materials Science and Engineering 981 2 22062 10.1088/1757-899X/981/2/022062.
48. Venkatramulu S., Kandukuri A., Rao V.C.S., Srinivas C., Pratapagiri S., Sudharshan E. IP spoofing controlling with design science research methodology 2022 AIP Conference Proceedings 2418 30075 10.1063/5.0082212.