iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.51570

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

A Novel Approach to Provide Security for Autonomous Vehicles

Sudhakar Avareddy[1], P Vijayalakshmi[2], Uday Kiran H P[3], Venu Gopal Reddy M[4]
[1, 2, 3, 4]*Ballari Institute of Technology & Management*

Abstract: ***Autonomous Vehicles (AVs) have been developing as the time passes in the events and it reduces the workload of mankind and reducing the errors done in the traffic(accidents). AVs are not bounded to roadways but also take part in other possible transportation modes. The issues of the extant process have less privacy due to involvement of sensor components and inappropriate of data transfer which will be subjected to more cyber-attacks. To prevent these issues, a methodology is proposed and the cryptography algorithms is implemented for transferring the data for drones, UAV's. Here cloud acts as negotiator between user and drones and UAV's, user shares the files from sender to drones(UAV's) with enhanced security. The AES algorithm is incorporated to inscribe the data from plain text into unidentified encoded form of text. The concealed text can be deciphered by entering the hash key.***

Keywords; AES (Advanced Encryption standards), UAVs (unmanned aerial vehicles)

I. INTRODUCTION

Autonomous vehicles (Drones, UAV's) are the mode of transportation where there is less or no interaction with humans which make the transportation easier and reduces the cost expenses of the labor. Drones have been developing as the time passes in the events and it reduces the workload of mankind and reducing the errors done in the traffic (accidents). The usage of drones has been increasing day by day. For manual vehicles most of the actions are monitored by human which will be enclosed by the automated technologies. Drones use deep learning and machine learning algorithms and technologies to achieve the goal of drones. In the existing method the data is stored in the hardware components to store, access, and retrieve the data which will be transferred to Drones. But this system has some limitations in the field of security such as inappropriate data transfer and easy to alter the data.

In Existing method there are some disadvantages such as less security, Cyber-attacks as well as Inappropriate data transfer. So, to overcome this we are implementing Artificial Intelligence (AI), Cyber Security (CS) and the Cloud. The cloud is like a middleman between sender and receiver. Sender sends the data to the cloud and preserves it. The data will be received by the receiver from the cloud. Here cloud will be more secured. The importance of implementing the Artificial Intelligence is to automatically store, access and retrieve data from the cloud. To provide security during transfer of the data we are using cryptography-based algorithm that is Advanced Encryption Standards (AES).

Autonomous Vehicles (AVs) have been developing as the time passes in the events and it reduces the workload of mankind and reduces the errors done in the traffic(accidents). AVs are not bound to roadways but also take part in other possible transportation modes.

The issues of the extant process have less privacy due to involvement of sensor components and inappropriate data transfer which will be subjected to more cyber-attacks. To prevent these issues, a methodology is proposed, and the cryptography algorithms is implemented for transferring the data for drones, UAV's. Here cloud acts as negotiator between user and drones and UAV's, user shares the files from sender to drones (UAV's) with enhanced security. The AES algorithm is incorporated to inscribe the data from plain text into unidentified encoded form of text. The concealed text can be deciphered by entering the hash key**.**

II. LITERATURE SURVEY

In paper [1], the author introduced how Transportation Systems Internet features related to Autonomous vehicles and security and privacy issues for such systems and how to integrate Artificial intelligence and security in autonomous vehicles and cloud- based internet was discussed.

In article [2], the author Introduced how Internet of transportation store the data in the cloud using the intel extension SGX, which maintains privacy by using Trusted Environment such as SGX within end-to-end information hiding mechanism. Analyze the framework by safely running condition-based programs on SGX using simulated and real data from IoT devices. SGX is designed to be safe but has pattern leak issues.

©IJRASET: All Rights are Reserved

In article[3], the author Introduced how Artificial intelligence is seen on the shores of the automotive industry. This is an important tool in any vehicle industry. Vehicles with very little human input must be installed on mobile platforms.

In article[4], the author Introduced how the importance of the data which is recorded from the sensors and these sensors produce huge load of data due to this huge amount of data we cannot store them in the hardware components due to the risk of losing the drives so author brought up an idea saving this information in the cloud. In this author is simply creating a fuss about the cyber security. To grasp various kinds of traces and advance ML technologies to find and avoid strikes.

In article[5], the author Introduced how the labelled objects from different kinds of related branches that may assist in predicting these unlabeled objects within a mentioned branch became an important problem. Authors have stated their objective of finding class names of information objects within the targeted stream by using the help of classifiers which are prepared by the initial stream. Authors have a proposal of framework for multi stream classification that uses projected information from a most frequently used features space filled in both the initial and destined domains. The framework is important to defenders of undertaking systems to find strikes during the changes of platforms threats such as Advanced Persistent Threats (APTs).

In article[6], the author Introduced how the Autonomous vehicles trust their sensors to navigate the direction of the vehicles without verification or validation that can be abused by the hackers to sabotage the systems and can inject corrupted data into the autonomous vehicle system. Authors proposes an architecture called as SAVIOR for securing unmanned vehicles with robust physical invariants. Authors mentioned that this architecture (SAVIOR) can only detect and cannot take any action regarding it.

In article[7], the author Introduced how Combined connected vehicles and autonomous vehicles to advance with faster and secured traffic in sustainable cities and he said that there is rise in the depend on technology that is based on sensors and thus reduces the dependency on the drivers. There is growth in connectivity and leads to the vulnerability of cyber-attack on the sensors.

In article[8], the author Introduced how the advancement of the cloud computing in recent years. Here Authors presents an encryption and decryption method while uploading, the file must be double encrypted, so he mentioned two encryption algorithms that is RSA and AES algorithms.

In article[9], the author Introduced how an inversion encryption technique for protecting private keys stored on removable storage. It requires no additional hardware, making it practical and economical to implement, and helps maintain the integrity and confidentiality of private keys.

In article[10], the author This paper examines the RSA algorithm and suggests changes to improve its security level and execution time. Three experiments were conducted to analyze the encryption and decryption processes, and programming techniques were used to speed up these processes. The results display the run-time of encoding was increased by 14% and decoding by 22% in the third experiment.

In article[11], the author Introduced about the major cyber security problems faced by the world, to resolve this problem he introduced how an image file and text file can be encrypted and decrypted using cyber security-based encryption algorithms which provide a private key to decrypt the data. Authors mentioned some of the powerful encryption algorithms such as RSA, AES and these algorithms are implemented using MATLAB (Matrix Laboratory) software.

III. PROPOSED METHODOLOGY

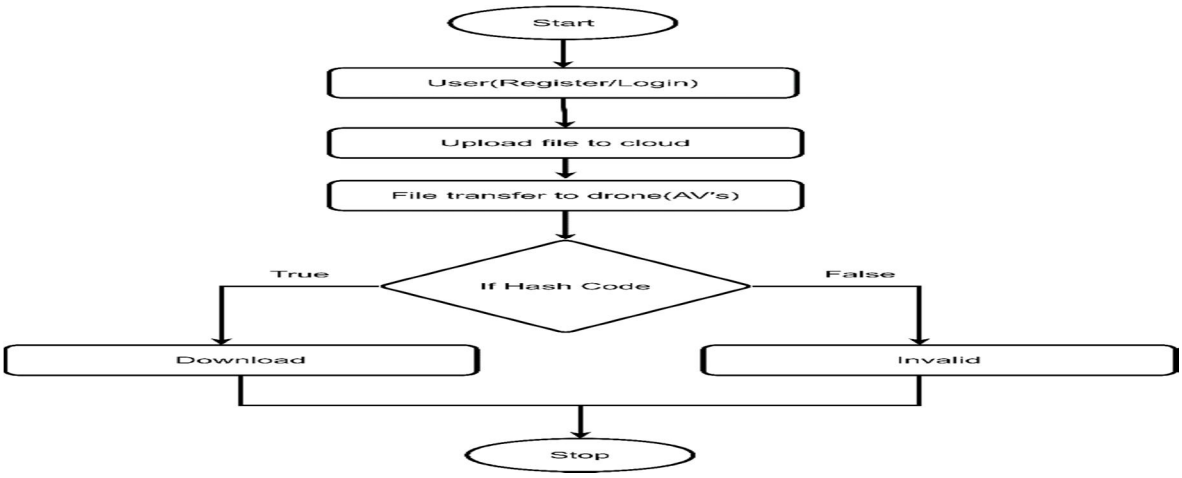


Figure 1: flowchart for Providing security for autonomous vehicles.

The proposed methodology for providing security is carried out by the following stages.

1) Step1: User Register/Login

Initially user should register in the application, if already user has registered then user can login to their account, which gives the privilege to exploit the features of the application.

2) Step2: Upload file to cloud

In this step the user can give input. In this module private key will be generated from the input and this input is encryptedinto the hash code using AES (Advanced Encryption Standards) Algorithm, Later file is uploaded to cloud so that we need not to upload the file every time in the applicationand input can be received by the drone through cloud.

3) Step3: Transfer of file from cloud to Drone (AV's)

Furtherthe file will be transferred to the Drone (AV's). Drone canaccess the file by deciphering the text using a private hash code which will be sent to the drone through mail. Here wecan check the status of the input file.

4) Step4: Verification

In the final step we need to verify the hash key value. By entering the correct hash code which is sent through mail, the drone will access the information which is presented in input file. If there is a case of wrong Hash key value pair,then drone will fail in accessing and processing the file andreturns Invalid.

IV. RESULTS AND DISCUSSIONS

The proposed methodology is implemented and tested for correctness and completeness by considering several case studies. The results obtained for various inputs are found satisfactory.

1) User Registration Form

In this window a new user can register by filling his/her details to gain access in this application.

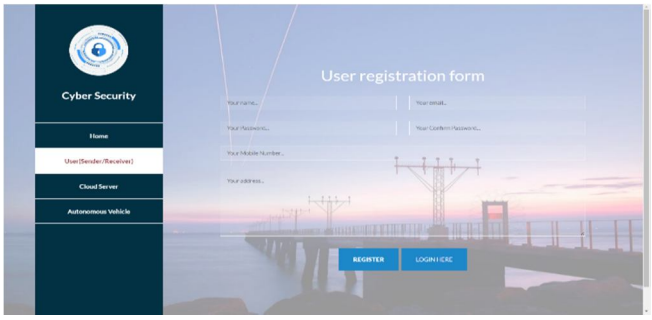


Fig 2 User registration form for new users

2) Login Page

The authenticated user can login to their account by entering their credentials.

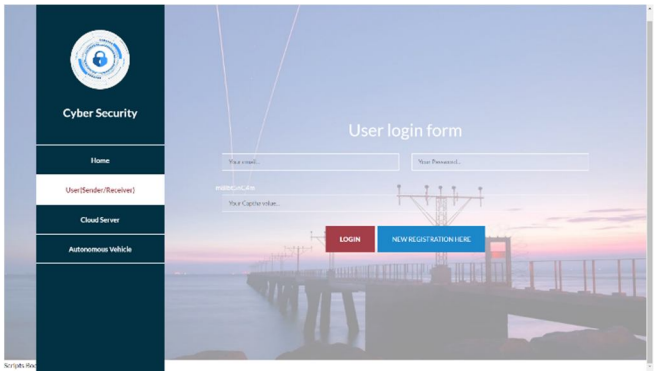


Fig 3 Login page for registered users

3) Upload transferring files

This is the page where users can transfer the text file to drone by filling some necessary details.

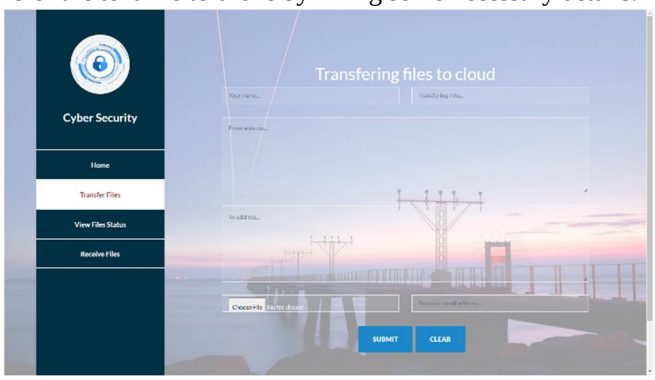


Fig 4 Transfer of file from user to drone

4) Transferring File Status Tracking

This is the page where the user can locate the status of the file so that he/she can ensure that text file is reached without any disruptions.



Fig 5 tracking the status of file

5) Received Files Information

This is the page where the files which are received by the Drone can be accessed here.

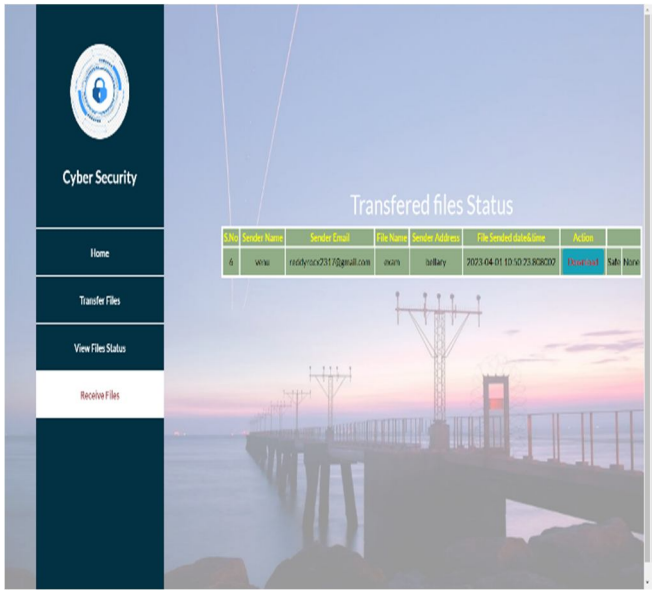


Fig 6 receiving files information

6) Download File Using Private Key

This is the page where the received file can be downloaded by entering the valid private key.

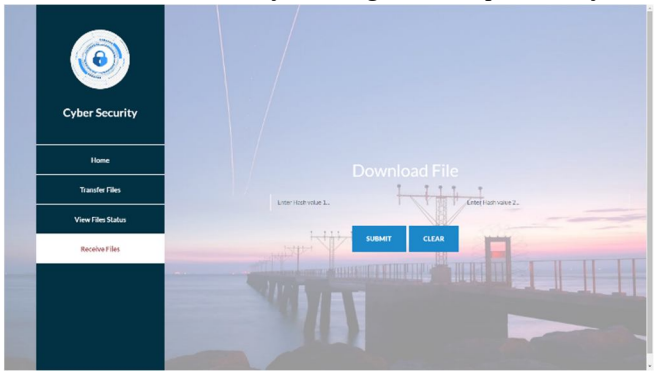


Fig 7 Decoding text using private key

7) Downloading File

This is the page where we can read and download the file after entering the valid private key.

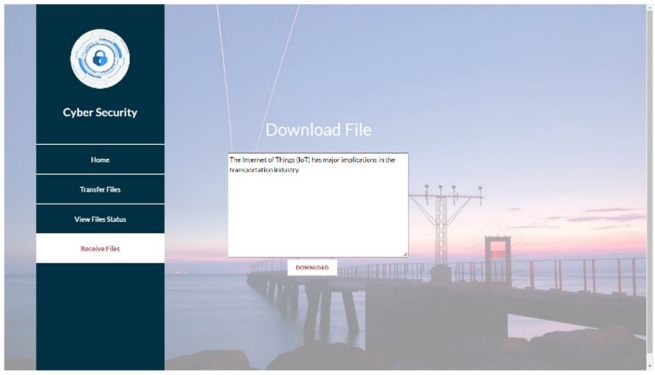


Fig 8 Deciphered text file downloaded

8) Sending Files From Cloud

In this page we can send the files to Drone.

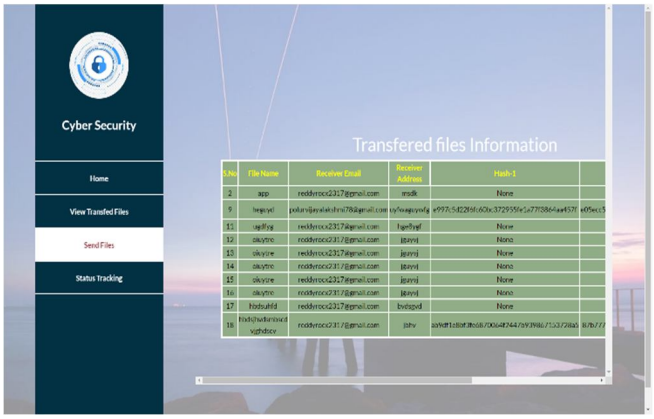


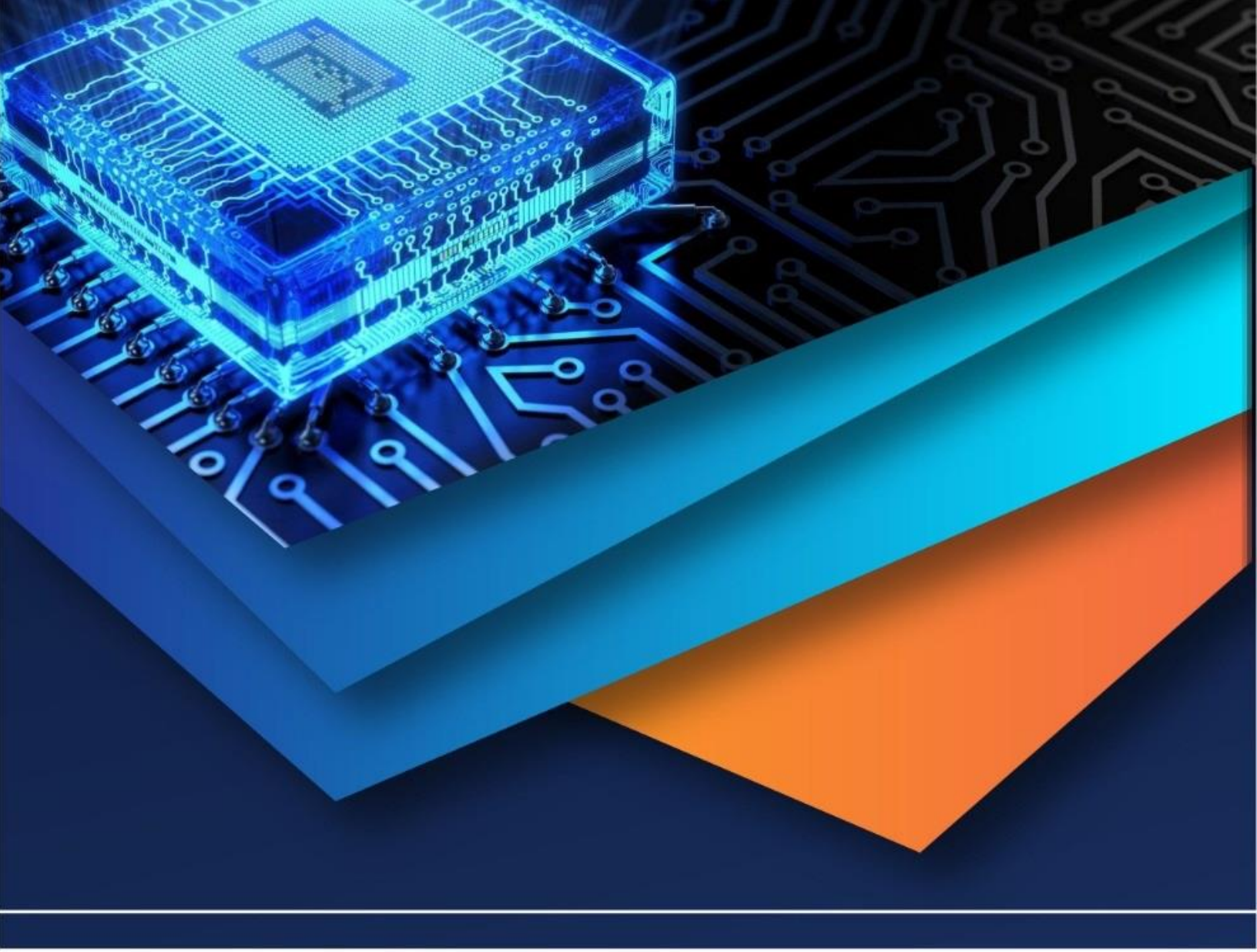
Fig 9 Sending files to Cloud

V. CONCLUSION

Ensuring the security of drone (UAV's), it is important to make sure the safe and reliable operation of the drone. There is a risk of facing the potential threats like denial of service, hacking, implementation of malware etc. To improve the security encryption algorithm (AES) have been used to inscribe the data so that the important information is concealed making it more secure and according to the need of file it can be decrypted using the hash key. This results in transfer of data without any interruptions and improve the confidentiality of the file.

REFERENCES

[1] Bhavani Thuraisingham, Computer Science Dept, The University of Texas at Dallas RichardsonUSA, bxt043000 @utdallas. edu,do i:10.1109/CSCloudEdgeCom 49738.2020.0001.
[2] Md Shahiul Islam, Latifur Khan, Mustafa Safa Ozdayi, Murat Kantarcioglu, Department of Computer Science the University of Texas at Dallas Richardson, TX 75080, U.S.A. md.shihabul.islam@utdallas.edu.
[3] Wang, Z.;Wei, H.; Wang, J.; Zeng, X.; Chang, Y. Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey. Sustainability2022,4, 2409.https://doi.org/10.3390/su141912409
[4] Nikata B. Shingote1 Prof. Monika D. Rokade2 1,2Sharadchandra Pawar College of Engineering, otur, Maharashtra, India. IJSRD - International Journal for Scientific Research & Development| Vol. 9, Issue 2, 2021 |ISSN (online): 2321-0613.
[5] Li, Y. -F, H. Tao, Y. Gao, L. Khan, et al. 2019."Multistream classification for cyber threat data withheterogeneous feature space." Proceedings of the WorldWide Web Conference (WWW '19): 2992-2998, doi: 10.1145/3308558.3313572 .Raul Quinonez, University of Texas at Dallas; Jairo Giraldo, University of Utah; LuisSalazar, University of California,Santa Cruz; Erick Bauman, University ofTexas at Dallas; Alvaro Cardenas, University of California, Santa Cruz; Zhiqiang Lin, Ohio State University August 12– 14, 2020 978-1-939133-17-5.
[6] K. Jaspin, S. Selvan, S. Sahana and G. Thanmai,"Efficient and Secure File Transfer in Cloud ThroughDouble Encryption Using AES and RSA Algorithm," 2021International Conference on Emerging Smart Computingand Informatics (ESCI), 2021, pp. 791-796, doi: 10.1109/ESCI50559.2021.9397005.
[7] Matthew N. O.Sadiku | Sarhan M. Musa | Abayomi Ajayi-Majebi "Artificial Intelligence in Autonomous Vehicles" Published in International Journal of Trend in Scientific Research and Development(ijtsrd), ISSN: 24566470, Volume-5 |Issue-2, February 2021, pp.715-720, URL :www.ijtsrd.com/papers/ijtsrd38514.pdf.
[8] M. G. Z. Fernando, A. M. Sison and R. P. Medina,"Securing Private Key using New Transposition Cipher Technique," 2019 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE), 2019,pp. 490493, doi: 10.1109/ECICE47484.2019.8942798.
[9] F. H. M. S. Al-Kadei, H. A. Mardan and N. A.Minas, "Speed Up Image Encryption by Using RSAAlgorithm," 2020 6th International Conference on Advanced Computing and Communication Systems(ICACCS), Coimbatore, India, 2020, pp. 1302-1307, doi: 10.1109/ICACCS48705.2020.9074430.
[10] V. S. Aparna, A. Rajan, I. Jairaj, B. Nandita, P. Madhusoodanan and A. A. S. Remya, "Implementation of AES Algorithm on Text and Image using MATLAB," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2019, pp. 1279-1283, doi: 10.1109/ICOEI.2019.
[11] V. S. Aparna, A. Rajan, I. Jairaj, B. Nandita, P. Madhusoodanan and A. A. S. Remya, "Implementation of AES Algorithm on Text and Image using MATLAB," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2019, pp. 1279-1283, doi: 10.1109/ICOEI.2019.8862703.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)