International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

Logistic System Using Artificial Intelligence for Cyber Security

D. Nagaraja[1], **Dr. M. Saravanamuthu**[2]
Department of Computer Applications, Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh, India

Article Info
Publication Issue :
Volume 8, Issue 4
July-August-2022

Page Number : 301-307

Article History
Accepted: 10 August 2022
Published: 28 August 2022

ABSTRACT

The transportation sector is significantly impacted by the Internet of Things (IoT). The goal of autonomous vehicles (AVs) is to enhance daily tasks including package delivery, traffic flow, and cargo transportation. In addition to ground vehicles, AVs can also be airborne or submerged, and they have a variety of uses. We are using Cyber Security (CS) based data transfer to autonomous vehicles to solve this issue. Here, a cloud acts as a middleman to transmit sender files to an autonomous car. For further security, we employ the CS-based Advanced Encryption Standard algorithm, which is employed to convert the sent data into cypher text. The private key that the sender generates for the specific AV can be used to decrypt the encrypted text.

Keywords : Cyber Security, Cipher text, AES, Private Key, AV.

I. INTRODUCTION

In recent years there has been an explosion of AVs. Companies are investing heavily in AVs.

While there is great potential in AVs and the improvements it can do to the transportation industry, security and privacy concerns pose new challenges that need to be addressed. The sensors are susceptible to malicious tampering (e.g., IMUs are susceptible to sound waves and GPS receptors are susceptible to spoofing signals). Vehicles should verify the veracity of sensor signals before acting upon them.

The Internet of Transportation Systems are subject to attacks (like any cyber physical system). Streaming data is being collected from such systems including autonomous and in the future driverless vehicles. As transportation systems go electric, they need energy conservation. Threats to the security of such systems could cause massive damage including accidents, loss of lives as well as being stranded on lonely highways due to attacks on energy management.

Data Science/ML techniques are being applied to analyze the data of AVs and a challenge is to apply the stream analytics/learning techniques for transportation data. For example, how can the ML techniques be applied to the massive amounts of sensor data emanating from the AVs?. The Internet of Transportation Systems will also depend heavily on Data Science/AI/ML (Machine Learning) techniques for various applications including optimum directions, driving without a human in the loop and many more. The Adversary will learn the machine learning models that we use and try and thwart our models.

Finally, while massive amounts of data are collected by the Internet of Transportation Systems, the privacy of the individuals has to be protected. We envision that much of the data sharing and analytics will be carried out using the services running in the cloud integrated with the Internet of Transportation System.

This paper explores how Artificial Intelligence, Security and the Cloud can be integrated to develop Intelligent Internet of Transportation Systems. We first discuss the integration of cyber security. Next, we discuss how a secure cloud may be utilized to carried out data analytics for the Transportation Systems. We discusses security and privacy for the data Transportation Systems. We discusses how the various components (e.g., AI, Security for Cloud) can be integrated to provide Intelligent and Secure Transportation Systems.

II. RELATED WORKS

R. Quinonez, J. Giraldo, L. Salazar, E. Bauman, A. Cardenas, Z. Lin, Securing Autonomous Vehicles with a Robust Physics-Based Anomaly Detector. 29th USENIX Security Symposium (USENIX Security 20). Boston, MA, August 2020: Autonomous Vehicles (AVs), including aerial, sea, and ground vehicles, assess their environment with a variety of sensors and actuators that allow them to perform specific tasks such as navigating a route, hovering, or avoiding collisions. So far, AVs tend to trust the information provided by their sensors to make navigation decisions without data validation or verification, and therefore, attackers can exploit these limitations by feeding erroneous sensor data with the intention of disrupting or taking control of the system. In this paper we introduce SAVIOR: an architecture for securing autonomous vehicles with robust physical invariants. We implement and validate our proposal on two popular open-source controllers for aerial and ground vehicles, and demonstrate its effectiveness.

Cyber Security Based on Artificial Intelligence for Cyber-Physical Systems: The ten papers in this special issue focus on cyber security for cyber-physical systems (CPSs). The systems have become very complex, more sophisticated, intelligent and autonomous. They offer very complex interaction between heterogeneous cyber and physical components; additionally to this complexity, they are exposed to important disturbances due to unintentional and intentional events which make the prediction of their behaviors a very difficult task. Meanwhile, cyber security for CPS is attracting the attention of research scientists in both industry and academia since the number of cyber-attacks have increased and their behaviors have become more sophisticated, commonly known as zero-day threats. The papers in this issue aim to bring together researchers from academic and industry to share their vision of AI application in the cyber security context, and present challenges and recent works and advances related to AI-based cyber security applied to CPSs.

M. Masood, L. Khan, and B. Thuraisingham, Data Mining Applications in Malware Detection, CRC Press 2011:Data mining is the process of posing queries to large quantities of data and extracting information, often previously unknown, using mathematical, statistical, and machine learning techniques. Data mining has many applications in a number of areas, including marketing and sales, web and e-commerce, medicine, law, manufacturing, and, more recently, national and cyber security. For example, using data mining, one can uncover hidden dependencies between terrorist groups, as well as possibly predict terrorist events based on past experience. Furthermore, one can apply data mining techniques for targeted markets to improve e-commerce. Data mining can be applied to multimedia, including video analysis and image classification. Finally, data mining can be used in security applications, such as suspicious event detection and malicious software detection. Our previous book focused on data mining tools for applications in intrusion detection, image classification, and web surfing. In this book, we focus entirely on the data mining tools we have developed for cyber security applications.

Bayesian network based analysis of cyber security impact on safety:Cyber security gains further importance regarding life cycle risk analysis of technical systems, e.g. Cyber Physical Systems (CPS) or Systems of Systems (SoS) in the context of increasing dependency on networked systems and processes in domains like industry 4.0 or smart home. At the same time, the operation of networked systems in environments critical to safety poses the challenge of analyzing a growing number of potential interactions between safety and security aspects. In industrial environments, the assessment of functional safety is a standard procedure, e.g. using IEC 61508 and domain-specific derivatives, while cyber security in safety relevant domains has only been introduced in the last few years. The assessment of cyber security is a rapidly developing discipline, but until now there have been only few approaches to merge the standardized procedures in safety and security. This paper presents an approach based on Bayesian Networks (BN) that enables to consider the impact of cyber security threats on functional safety considerations. By means of a simplified x-by-wire system, safety and security relations as well as structures are derived and an integrated safety and security BN is established. It is shown that parameter learning in BN can be used to adapt chosen target parameters to a required integrated safety and security level. Thus, it is possible to enhance the system configuration considering new cyber security threats.

B. M. Thuraisingham, SecAI: Integrating Cyber Security and Artificial Intelligence with Applications in Internet of Transportation and Infrastructures, Clemson University Center for Connected Multimodal Mobility, Annual Conference, October 2019:Intelligent Transportation Systems (ITS) are emerging field characterized by complex data model, dynamics and strict time requirements. Ensuring cyber security in ITS is a complex task on which the safety and efficiency of transportation depends. The imposition of standards for a comprehensive architecture, as well as specific security standards, is one of the key steps in the evolution of ITS. The article examines the general outlines of the ITS architecture and security issues. The main focus of security approaches is: configuration and initialization of the devices during manufacturing at perception layer; anonymous authentication of nodes in VANET at network layer; defense of fog-based structures at support layer and description and standardization of the complex model of data and metadata and defense of systems, based on AI at application layer. The article oversees some conventional methods as network segmentation and cryptography that should be adapted in order to be applied in ITS cybersecurity. The focus is on innovative approaches that have recently been trying to find their place in ITS security strategies. These approaches includes blockchain, bloom filter, fog computing, artificial intelligence, game theory and ontologies. In conclusion, a correlation is made between the commented methods, the problems they solve and the architectural layers in which they are applied.

III. Methodology

Proposed system:

In proposed system we are implementing Cyber Security (CS) based data transfer to Autonomous vehicle to overcome the existing problems. Here a cloud is the mediator that which transfers sender files to autonomous vehicle with more security we are using CS based algorithm (Advanced Encryption Standard) which is used to hide the transferred data into cipher text. The cipher text can be decrypted by the private key generated by sender to the particular AV.

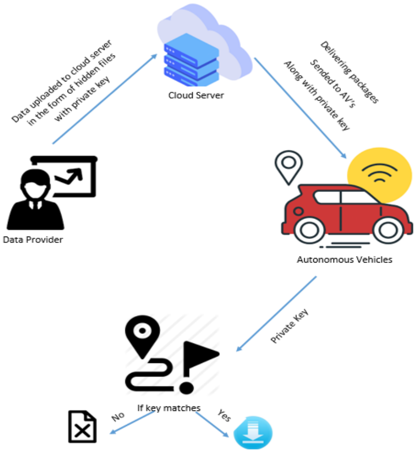

Data uploaded to cloud server in the form of hidden files with private key
Cloud Server
Delivering packages Sended to AV's Along with private key
Data Provider
Autonomous Vehicles
Private Key
If key matches
No
Yes

Figure 1 : Fake reviews dataset block diagram

Advantages:

- More Security
- Accurate data transfer
- Less cyber attacks

IV. Implementation

1. AES Algorithm

The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data? The data to be encrypted. This array we call the state array.

You take the following aes steps of encryption for a 128-bit block:

Derive the set of round keys from the cipher key.

Initialize the state array with the block data (plaintext).

Add the initial round key to the starting state array.

Perform nine rounds of state manipulation.

Perform the tenth and final round of state manipulation.

Copy the final state array out as the encrypted data (ciphertext).

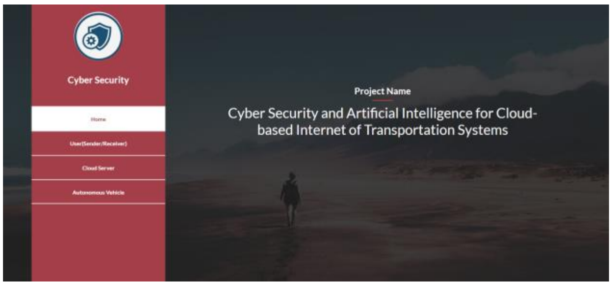
The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others.

The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so we first convert the 128 bits into 16 bytes. We say "convert," but, in reality, it is almost certainly stored this way already. Operations in RSN/AES are performed on a two-dimensional byte array of four rows and four columns. At the start of the encryption, the 16 bytes of data.

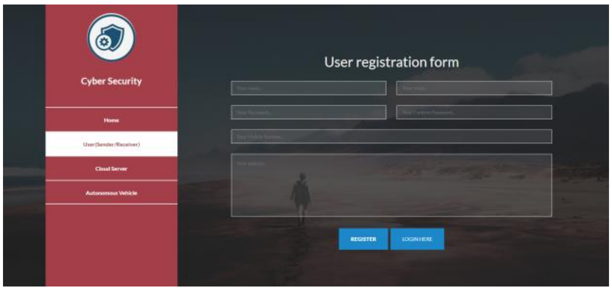
V. Results and Discussion

The following images will visually depict the process of our project.

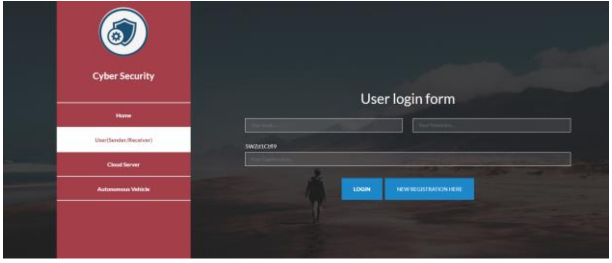
Home page: In this home page we can see the logo designing of our website and here we are detecting the fake reviews from the review entered by the user.


Cyber Security
Home
User(Sender/Receiver)
Cloud Server
Autonomous Vehicle
Project Name
Cyber Security and Artificial Intelligence for Cloud-based Internet of Transportation Systems

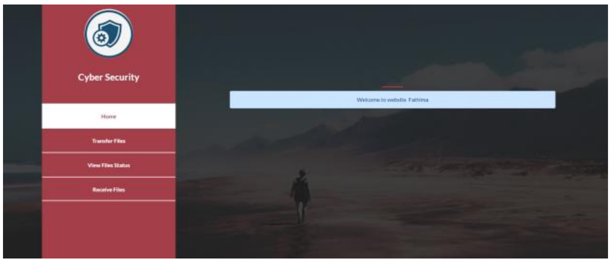
User registration: In this page the user can register into account.



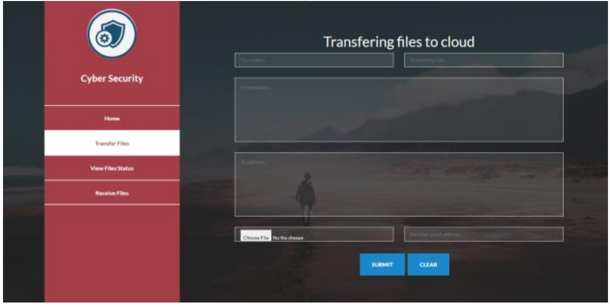
User registration form: After user gets registered this page will be created as like user registration details.



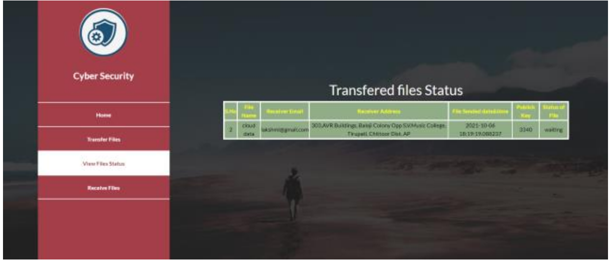
User home page: After user gets login User will get this User home page where the user can switch into account and user can use it.



Upload transferring files: In this page the user can upload those transferring files here.



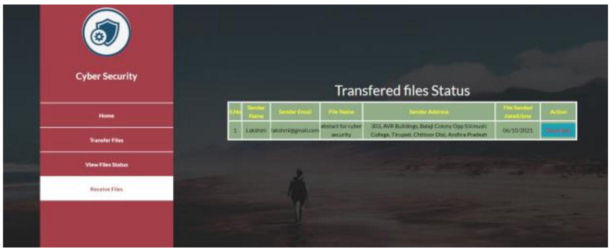
Transferring files status tracking: Here the user can track the status of transferring files.



Transfered files Status

S.No	File Name	Receiver Email	Receiver Address	File Sended date&time	Publick Key	Status of File
2	cloud data	lakshmi@gmail.com	303,AVR Buildings, Balaji Colony Opp SV.Music College, Tirupati, Chittoor Dist.,AP	2021-10-06 18:19:19.088237	3340	waiting

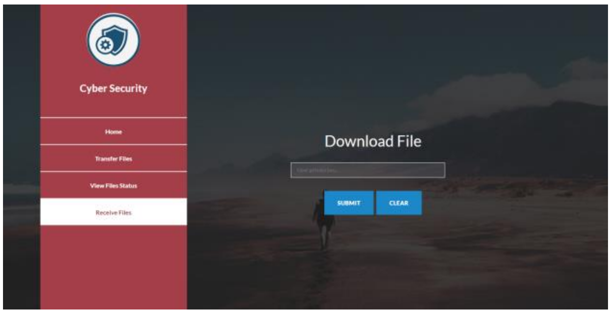
Received files information: This page contains the information of received files.

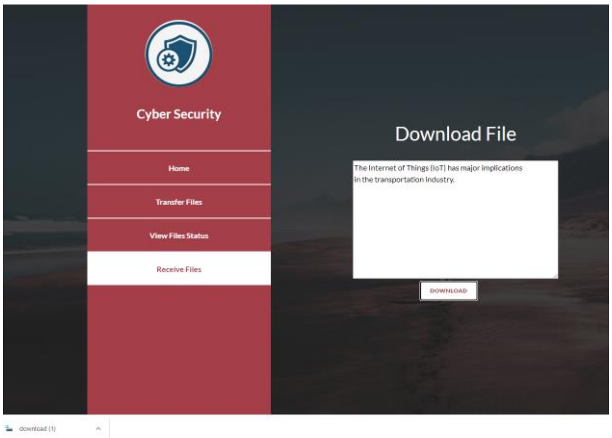


Transfered files Status

S.No	Sender Name	Sender Email	File Name	Sender Address	File Sended date&time	Action
1	Lakshmi	lakshmi@gmail.com	abstact for cyber security	303, AVR Buildings, Balaji Colony Opp S.V.music College, Tirupati, Chittoor Dist, Andhra Pradesh	06/10/2021	[illegible]

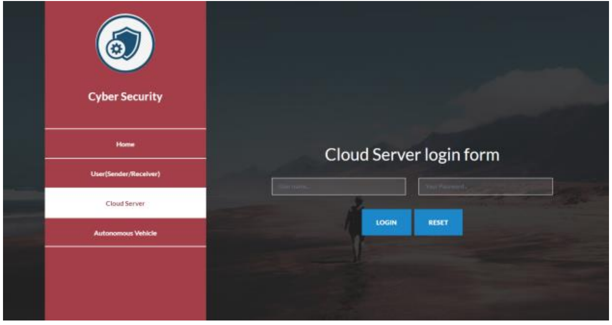
Downloading file: In this page user can download the files.



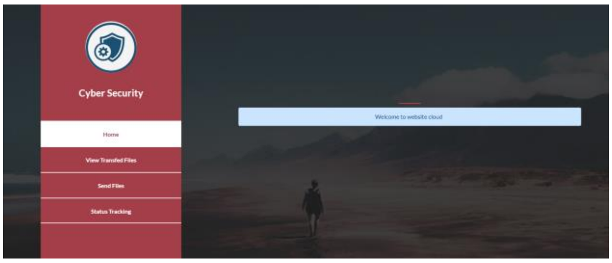


The Internet of Things (IoT) has major implications in the transportation industry.

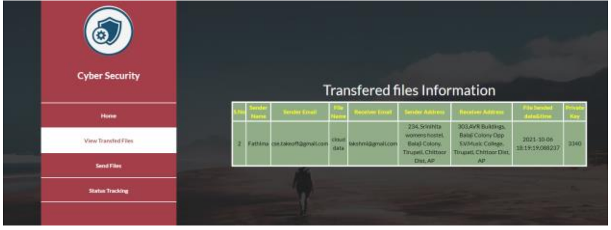
Cloud server login page: Here the cloud server can login into account.



Cloud server home page: This is the home page of cloud server.



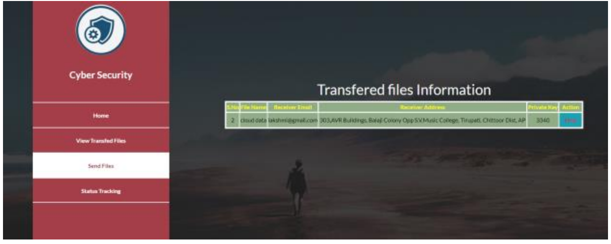
View transferring files: Here the cloud server can view the transferring files.



Transfered files Information

S.No	Sender Name	Sender Email	File Name	Receiver Email	Sender Address	Receiver Address	File Sended date&time	Private Key
2	Fathima	cse.takeoff@gmail.com	cloud data	lakshmi@gmail.com	234, Srinivasa womens hostel, Balaji Colony, Tirupati, Chittoor Dist, AP	303,AVR Buildings, Balaji Colony Opp S.V.Music College, Tirupati, Chittoor Dist, AP	2021-10-06 18:19:19.088237	3340

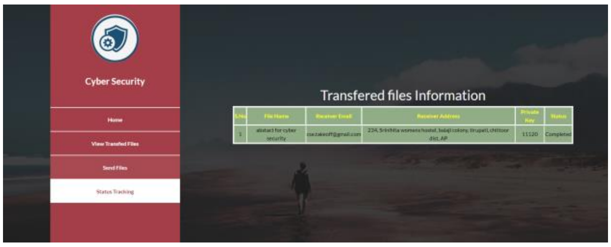
Send files: In this page the files will be send.



Transfered files Information

S.No	File Name	Receiver Email	Receiver Address	Private Key	Action
2	cloud data	lakshmi@gmail.com	303,AVR Buildings, Balaji Colony Opp S.V.Music College, Tirupati, Chittoor Dist, AP	3340	[illegible]

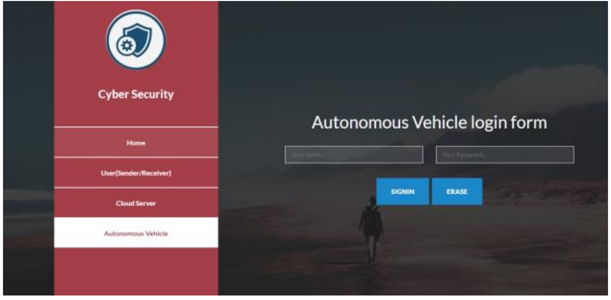
Status tracking: Here the cloud server can track the status of files.



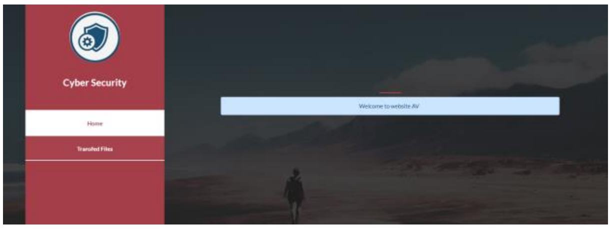
Transfered files Information

S.No	File Name	Receiver Email	Receiver Address	Private Key	Status
1	abstact for cyber security	cse.takeoff@gmail.com	234, Srinithla womens hostel, balaji colony, tirupati, chittoor dist, AP	11120	Completed

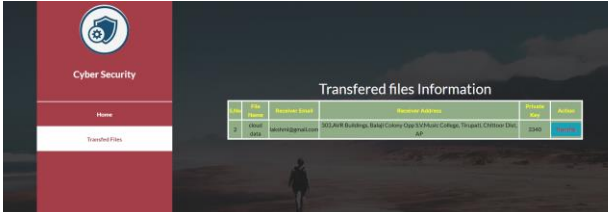
Autonomous vehicle login page: In this page the autonomous vehicle can gets login.



Av home page: This is home page of autonomous vehicle.



Sent transferring file to user: In this page the transferring file can send to user.



Transfered files Information

S.No	File Name	Receiver Email	Receiver Address	Private Key	Action
2	cloud data	lakshmi@gmail.com	303,AVR Buildings, Balaji Colony Opp S.V.Music College, Tirupati, Chittoor Dist, AP	2340	[illegible]

VI. Conclusion

Here we implemented Cyber Security (CS) based data transfer to Autonomous vehicle system. Cloud is used has mediator to transfers files from sender to autonomous vehicle with more security using CS based algorithm (Advanced Encryption Standard) for converting data into cipher text. The cipher text is decrypted by the private key generated by sender to the particular AV.

VII. REFERENCES

[1]. R. Quinonez, J. Giraldo, L. Salazar, E. Bauman, A. Cardenas, Z. Lin, Securing Autonomous Vehicles with a Robust Physics-Based Anomaly Detector. 29th USENIX Security Symposium (USENIX Security 20). Boston, MA, August 2020.

[2]. M. Masood, L. Khan, and B. Thuraisingham, Data Mining Applications in Malware Detection, CRC Press 2011.

[3]. Y. Zhou, M. Kantarcioglu, B. M. Thuraisingham, B. Xi, Adversarial support vector machine learning. ACM KDD 2012: 1059-1067

[4]. B. M. Thuraisingham, SecAI: Integrating Cyber Security and Artificial Intelligence with Applications in Internet of Transportation and Infrastructures, Clemson University Center for Connected Multimodal Mobility, Annual Conference, October 2019.

[5]. B. M. Thuraisingham, P Pallabi, M. Masud, L. Khan, Big Data Analytics with Applications in Insider Threat Detection, CRC Press, 2017.

[6]. K. W. Hamlen, V. Mohan, M. M. Masud, L. Khan, B. M. Thuraisingham: Exploiting an antivirus interface. Comput. Stand. Interfaces 31(6): 1182- 1189 (2009)

[7]. L. Liu, M. Kantarcioglu, B. M. Thuraisingham: The applicability of the perturbation based privacy preserving data mining for real-world data. Data Knowl. Eng. 65(1): 5-21 (2008)

[8]. B. M. Thuraisingham, M. Kantarcioglu, E. Bertino, J. Z. Bakdash, M. Fernández, Towards a Privacy-Aware Quantified Self Data Management Framework. SACMAT, pp 173-184, 2018 [9] K. W. Hamlen, M. Kantarcioglu, L. Khan, B. M. Thuraisingham, Security Issues for Cloud Computing. IJISP 4(2): 36-48 (2010)

[9]. Y. Li, Y. Gao, G. Ayoade, H. Tao, L. Khan, B. M. Thuraisingham, Multistream Classification for

Cyber Threat Data with Heterogeneous Feature Space. WWW, pp 2992-2998, 2019

[10]. H. Qiu, Q. Zheng, G. Memmi, J. Lu, M. Qiu, B. M. Thuraisingham, "Deep Residual Learning based Enhanced JPEG Compression in the Internet of Things", accepted by IEEE Transactions on Industrial Informatics, 2020

[11]. G. Ayoade, V. Karande, L. Khan, K. W. Hamlen, Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment. IRI, pp 15-22, 2018.

Cite this article as :

D. Nagaraja, Dr. M. Saravanamuthu, "Logistic System Using Artificial Intelligence for Cyber Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 4, pp. 301-307, July-August 2022.
Journal URL : https://ijsrcseit.com/CSEIT228450