**Vanet FDIA Solutions using Blockchain Based IPFS-Trust ManagementSystem with ML SVR Model.**

**Preeti GroverAnd Dr. Sanjeev Kumar Prasad**

***School of Computing Science and Engineering ,Galgotias UniversityGreater, Noida, Uttar Pradesh, NCR, India***

***preethi.grover\_phd18@galgotiasuniversity.edu.in*** ***sanjeevkps2002@gmail.com***

**ORCID ID OF THE AUTHOR :- 0000-0002-0267-0783**

**Abstract :**

A VANET is a collection of mobile nodes (vehicles) that share data through ad hoc on-demand connections. **The main aim of the paper isto provide solutions for False Data Injection Attack by Integration of Blockchain Based IPFS-TrustManagement System with ML SVR Regression Model.** Due to Network Assaults and Threats under Vanet System, the safety of the drivers is under Stake andCritical. A rogue node can send out erroneous messages, causing unavoidable scenarios. We first filter the received data from Vehicles creating false traffic jam warning messages using the Machine learning SVR Regression Model where data is created and split into train and test data. We used Machine learning supervised algorithm named as **Vehicular network Based SVR (VNBSVR)** to classify whether the vehicle is a legitimate vehicle or an attacker vehicle and result of the coefficient of Linear Regression with Decentralized Consensus BC and IPFS –Data Storage Scheme is validated using **Performance Metrics for Regression.** Algorithm Implementation results show that the FDIA attack strategy achieves a better performance than the without using ML algorithm of SVR Regression Model based attack strategy in Predicting the Vanet Security. **Users can access the system through DApp, an Ethereum-distributed application, and manage their vehicle data.**We had discussed about the results and analysis and finally had done Evaluation of the Performance Metrics toknow the accuracy of the ML SVR Model used for Vanet Security.

**Index Terms**:-OBU(On-Board Unit),TA(Trusted Authorities),FDIA(False Data Injection Attack), VSN(Vehicular Sensor Network), IPFS(Interplanetary File System),DAPP(Decentralized Applications).

**1.Introduction:**

For the coarse-resolution data-referenced relative radiometric normalization, a nonlinear radiometric transforming relation model based on support vector machine regression (SVR) is used (RRN). Support vector regression (SVR) is a type of support vector machine (SVR) that is used for regression tasks. It tries to find a function that best predicts the continuous output value for a given input value.

SVR can use both linear and non-linear kernels. A linear kernel is a simple dot product between two input vectors, while a non-linear kernel is a more complex function that can capture more intricate patterns in the data. Vanets are networks of vehicle communication and road infrastructures to extend road safety and infotainment. Vanet is used for communication between two vehicles and they are used for short-range communication infrastructure. When VANET is integrated with various other technologies including sensor networks it becomes VSN. The vehicles realize the information sharing and exchange where the driver uses an emergency alarm to deal with the dangers in time and adjust route based on Traffic Information to avoid traffic accidents and congestions. The network is termed an ad-hoc network, as the position of the vehicles changes at every instant of time. The vehicle system comprises mainly of 3 parts which are the vehicle unit, fixed-based station, and database with a software system. The average speed of vehicular nodes varies from 40 to 80 km/h. This system contains three parties:-TA(Trusted Authorities), OBU(onboard unit), and RSU(Road side unit). A car could manufacture bogus information and send it to the network on its own. For example, a car may manufacture information about fictitious road accidents and then broadcast that information to other vehicles to create a new route. Although FDIA attacks can have a significant impact by influencing changes in driver behavior. Cryptographic algorithms and protocols can be used to secure messages on VANETs. Inmost of these protocols, such as key distribution, message authentication, and digital signatures, a third party, referred to as a trust center, is involved. However, such mechanisms are not appealing alternatives in terms of both trust and cost.

Li et al introduced Trust Establishment Scheme for constraining the bad behavior of nodes and also they proposed Trustworthy Communication in Vehicular Adhoc Networks to provide reliabletraffic safety and thus increasing the efficiency. This is especially with critical applications like:Hazard Warnings etc..where the receiving Node should provide the authenticity and trust ability of the received messages. Below is the figure for depicting the vanet architecture wherein the vanet components communicate with each other across a wireless medium to control data transfer via nodes such as: Security, Latency and Data Transmission Range. Since the message is exchanged between Source vehicle to a Destination Vehicle Through roadside unit,due to which there are frequent delays in vehicular communications. It is one of the challenging job under vanet system to verify the recently received message is a legitimate or Malicious Message.If the message is the malicious message than it must be discarded either by the driver or by the poisoning of the nodes through routing protocols under Vanet system .Our analysis of the problem is done by giving the solution using the security framework based on Blockchain IPFS-Trust Management System wherein we require to correlate the dependent variable and independent variable by using the ML SVR Regression Model and verifying the condition or check regarding the attacker type=”Malicious Nodes” from IPFS-Trust Management Database, therefore we need to check the attacker behavior by including the tempering of nodes with data of abnormal or normal states and if the condition gets matched ie..than we can fire the query from the database ,as Select messageid from IPFS where the attacker type=”Malicious Nodes”.

The remaining part of this paper is organized as follows: Section 2 contains the Literature Review ,Section 3 contains the Objectives of the Research ,Section 4 contains the Research

Methodology described by us for solving the FDIA in Vanet System, Section 5 contains the Proposed Solutions ,while Section 6 contains the implementation of the solution provided by us, While Section 7 Contains the Interpretation of the output ,Section8 Contains the Limitation and scope of Future Research which is followed by Section 9 Covering the Conclusions and Recommendation emanating from this work.

**II. Literature Review: -**

Exiting solutions for Detection and Prevention of False Data Injection Attacks:

**II.1Detection of Data Falsification**: When the Source Vehicle and Receiver Vehicle are in different locations, then the source Vehicle sends the data using the hash function then the hashvalue is computed and send along with the data. The receiver vehicle receives the data and the hash value is computed using hash function. Both the receiver and sender hash values are

compared, if the hash value is the same then the message is forwarded to other vehicles else ifthe hash values are not the same then the message is discarded.

**II.II Security threats resolution using SDN in Vanet System :**

It uses a one-way hashing algorithm between the vehicles and RSU and a Hidden Key. Thisstrategy also addresses privacy concerns that may arise as a result of communication.

Software Defined Vehicular networking enables decoupling of control and data planes inSDVN which provides :An abstraction for Vanet application to underlying networking infrastructure. A logically centralized network intelligence and network state. The SDN Controller isfrequently the main component in charge of running the entire network in SDVN applications.The entire network halts when a single controller is assaulted. Malicious Nodes can enter the system with ease and make choices in place of the controller. SDVN mitigates or minimizes hugemanagement overhead on the controller.

**II.III Dynamic En-Route Filtering** employs the Hill Climbing Approach for Key Dissemination.

For Data Transmission in Vanet System, each node sends out its key to forwarding nodes. The transmitting nodes then reveal their keys after delivering reports, allowing the forwarding nodes to validate their reports. A hill-climbing key dissemination strategy is used to ensure that nodes located closer to data sources have greater filtering capacity. The climbing strategy makes it so that nodes near clusters carry more authentication keys than nodes near the base station. For theimportant predistribution phase and the key dissemination phase, respectively, Hill Climbing has two versions.

**II.IVProbabilistic Approach and Deterministic Approach:**

Each vehicle is anticipated to get several copies of the same message from its peers under the probabilistic approach.Based on whether or not the received message has been altered, the messages from various vehicles are utilised to determine the trust level value.

The deterministic technique, on the other hand, compares two distinct ways to estimate the distance between the two communicating

vehicles in order to determine whether the message received is authentic or not.Using the vehicle's position coordinates and the received signal intensity, we can calculate the two distances and compare them, allowing us to verify the message.In this method, we take into account that the location coordinates are periodically exchanged between vehicles or can be inferred by existing positioning software. Entity-oriented, data-oriented, and hybrid trust models are the three divisions of TMs.To preventadversaries from entering the network, entity-oriented trust models (ETMs) calculate trust values for nodes (entities).In order to manage trust, hybrid trust models (HTMs) integrate the best aspects of both DTM and ETM.DTMs (Data-oriented Confidence Models) measure the level of trust in transmitted communications (data).Therefore, entity-centric and data-centric trust models are the 2 main types of trust models employed in VANET.In order to identify malicious and dishonest nodes and ensure trustworthy data delivery, entity-centric trust models concentrate on assessing the reliability of vehicles.

**II.V Security using Randomization of Cryptographic Algorithm:** The cornerstone of cryptography is randomness (entropy), which is used to create session keys. The cryptographic system is more secure the more random the numbers are As a result, the task becomes one of creating actual unpredictability. Pseudorandom number generation is used in many modern systems.

**II.VI Using ANN FOR Validation of Nodes:** Is the node a Trusted Nodes or Untrusted Node. This model calculates the trust using a variety of roles and distance-based measures, such as Euclidean distance. Due to the dynamic changes of vehicular nodes, some scenarios may fail to capture the current study traffic based on their trust levels and the message received from the cars entities. A vehicular node then decides whether to forward or receive the messages.

**II.VII Securing Vehicular Ad-hoc Networks against Malicious Vehicles Using Clustering Algorithm**: Clustering is one solution to improve security against malicious vehicles. Using this approach, We can Block the Communication between the other malicious vehicles, and hence the wrong message is not passed ahead in the Vanet system. Malicious Vehicles easily change the identity of other vehicles.We can use Bloom Filters to record the positive and negative nodes. Each vehicle is associated with TPD(Tamper Proof Device)for Security Purposes. The position is broadcast in beacon packets on a regular basis so that every node within the wireless transmission range can compile a table of nearby nodes, including their positions. If a node is connected to another node, it is said to be connected .It chooses the next hop from the neighbor table in order to forward a packet. When a node is created, incorrect position data is disseminated through the routing process messages and VANET is harmed. A malfunction may result in incorrect position information. Attackers may falsify the positioning hardware or purposefully falsify the data to data rerouting Nodes that aren't working properly can cause a system's performance to suffer, whereas rerouting data through hostile nodes breaks basic principles to some extent. Rerouting of data through malicious nodes violates basic security goals such as confidentiality, authenticity, integrity or accountability.

**II.VIII Dynamic en-route Filtering (DEF) System**

Yu and Guan suggested a dynamic en-route filtering (DEF) system. Using the authentication key and secret keys, this system is capable of identifying a fake report throughout the transfer procedure. Key pre-distribution, key dissemination, and report forward are the three operational phases of DEF.

**Below is the Fig 1: Depicting the Existing Authentication Schemes in Vanet System.**



**Fig.1 Categories of Authentication in Vanet System(<https://doi.org/10.1155/2019/2423915>)**

**III.Research Methodology:**

Vehicles can connect with each other over the Global System for Mobile Communications (GSM) or the 5G Long Term Evolution (LTE) network, however with some limitations. Each car on the road may work together to create a significantly better driving experience when data are processedand information is shared with the others. **Data that we received through radio channels or smart antennas using beam forming array techniques is put into Blockchain Based IPFS for Trust Management in Vanet And**

**We have written an algorithm for our methodology for prevention of False Data InjectionAttack, steps are mentioned below:**

Algorithm -Vehicular network Based SVR(VNBSVR) Steps are discussed as Below:

1.Load input data

2.Split data into training and testing parts

3.Check for IPFS Offchain storage in testing data

4.Train ML model in a distributed manner

5.Select SVR classifier for attack detection

1. Fit classifier to training data
2. Predict attack alarm
3. If attack is detected, predict abnormal data
4. Admin takes action or control in choosing for false data Alarm or True Attacks
5. Log details in IPFS
6. Add smart contract for existing Transactional Logic
7. If attack is not detected, predict normal data
8. Use smart contract for executing Transactional Logic
9. Use Blockchain Network with POW Scheme for Data Aggregation by adding the transaction in it
10. Select SVR classifier for predicting classification of nodes
11. Fit classifier to input data
12. Predict classification of nodes

**III.IData Collection from all Sources:**

There are types of Data Repositories, from an Analyst Perspective like: Spreadsheets and data marts ("spreadmarts"),Data Warehouses, Analytic Sandbox(Data assets gathered from multiple sources and technologies for analysis Enables flexible, high-performance analysis in a nonproduction environment; can leverage in-databas),Structured,Semi-Structured and Un- Structured Data Types are there with Big Data Characteristics , Size and attributes of data: Including internal and external data sources, everything from summary-level aggregated data, structured data, raw data feeds, and unstructured text data from call logs or web logs etc..

An adversary hacks particular nodes and injects bogus data into the network in a false data injection attack. Through the infected nodes, false sensing reports can also be injected. An adversary can take control of a sensor node by compromising a few sensor nodes and gaining access to all important aspects .Below is the methodology we are depicting in Fig3 which is **based on SVR Regression Algorithm for**

**Trust Evaluation after classifying the dataset and using the scatter plots for analyzing the relationship between the attacker types which can be : Insider attacker,Outsider attacker, Malicious Attacker, Rational Attacker,Active Attacker or Passive Attacker and Messageid. We tried to correlate the two variables namely malicious attacker and message id and if there is a match than we can suspend that node .**

To find out the expected Trust Value of the nodes and to derive the rules for Trust Calculation we need to self-train the vehicular nodes and for all this we need to use SVR Regression Model. Majorly Attacks are categorize in different types like:(i) Passive attack: Using a wireless channel, an attacker can eavesdrop on node-to-node conversation and gather useful data. Passive attack is highly challenging to identify because it merely steals data without interfering with the protocol's usual operation. (ii) Active assault (such as the Sybil assault and the Black Hole Attack): A hostile node actively obstructs network protocols and violates the security policy by injecting fake information and modifying the data packets, which might have a direct impact on the security and availability of the network.

**III.IIData Preparation:**

**Data pre-processing**-The range of nodes for monitoring the communication variables stated above is decided during this phase. Since the nodes (vehicles) in the network move quickly, it is important to keep track of and update the data on the nodes that have left the network. Information about the node's presence and connectivity throughout the network is gathered using the spatial reusability-aware single-path routing protocol (SASR). When messagecopies are transferred using the DTN algorithm, network overhead is increased due to the vehicular network's instability. To improve data delivery, machine learning can be used to distinguish between malicious intermediate nodes. In order for the trained classifier to forecast the state of a message, the set of features that represent misbehavior communication mustbe gathered. The model demonstrated a high accuracy and detection rate of 99.06% along with an accuracy of 99.74%.We had used the dataset-2-supervisedlearning.csv file and Dataset( "C:\Users\PREETI\Downloads\JSONlog-7-49-A1.json.xls")and then did data cleaning, The trainedimputer was used to convert the training set by replacing the missing values with learned medians because most machine learning algorithms cannot deal with missing features. The outcome is a NumPy array holding the altered features.

The dataset uses continuous data, hence SVR is used in the coding in Python rather than SVR. A regression prediction algorithm based on SVR theory is support vector regression (SVR). Classification issues are addressed by SVR, which is a key application of support vector machines algorithm. In the above Fig.5(Decentralized Consensus BC and IPFS **–**Data Storage Scheme,where we are classifying the attack type and message id which can be stored in a IPFS server more securely with the use of BC and Data Aggregation Method. Once an attack has been identified, the transaction data is more securely stored on the server using data aggregation and the blockchain. As soon as an attack is discovered, the transaction data is securely stored on the server using a smart contract-based blockchain system. The transaction handling stage divides transactions into Normal and Abnormal types, after which the smart contract executes business logic, adding the Blockchain transaction to the Network Cloud.

Physical sensors, sensor data transfer lines, and data processing algorithms can all be compromised in order to introduce false data injection attacks (FDIA) into the system. Physical sensors must be physically accessed in order to be compromised, making it a difficult task. In contrast, it is simpler for an attacker to compromise the sensor data transfer lines and data processing applications.

A successful FDIA could affect the predictive maintenance model physically or financially by causing the engine sensors to send incorrect values to the central engine control.Therefore ,we correlate the IPFS with Trust Management System using Blockchain system and used

SVR for Classification of Malicious Nodes and Legitimate Nodes in the Vanet System. We can make use of introducing decentralized consensus blockchain and Interplanetary file system (IPFS) based data aggregation for effective classification and data storage. The training data and model files used in machine learning training are ideally suitable for protection because IPFS has no storage capacity restrictions and offers high - throughput content-addressed storage.When data needs to be extracted, IPFS reads the blocks of data simultaneously from every node. As a result, IPFS can satisfy the training process's performance criteria for reading and writing.The widespread distribution of IPFS nodes allows for adequate backups.Because hackers cannot attack every node at once, IPFS is able to store and share a lot of secure data and files.The InterPlanetary File System (IPFS) can be viewed as a peer-to-peer distributed file system without privileged nodes that stores IPFS objects locally on each node.These objects, which stand in for files and other data structures, are subsequently transferred between nodes via connections.

Although the most well-liked hashing algorithms can be used, SHA256 is the default. A content ID (CID), a hash that specifically identifies each file or directory, is present. Even a single byte in the content can change and cause this CID to change. When content changes, we must use the new CID; otherwise, we are referring to an earlier version of the file. Dealing only with hashes is not particularly user-friendly. As a result, IPFS includes the InterPlanetary Name System (IPNS).Vehicle data is obtained and saved in the user's contract via data encryption, string separation, IPFS upload, and data compression. Real-time car data is generated by an OBD-II scanner and is subsequently transferred and copied to the DApp.If the DApp is not running or the user is not logged in, the data are in the backlog.While the DApp is running and the user checks in, the most recent stat from the queues is sent. By entering the user's Ethereum address, private key, FileList contractual name, and file name into the DApp, the user can begin accessing the FileList contract in the user's UserData contract.In order to access the FileList contract, identity verification is carried out via by checking the mapping data to see if they have access to the FileList. A crucial step in the data sharing process is creating a contract for the exchange of FileLists.Users are given the information requester's public key and Ethereum address.The user provides the DApp with their contact information, the data that the data requester needs to share with the data recipient, and the name of the new FileList contract.The DApp builds a new sharing FileList contract in the user information contract using the input data.The user's data contract and insurance provider are where the freshly created information is saved. It effectively runs and processes car data with large data sizes and stores the hash value of linked vehicles in a blockchain that makes use of a digital signature mechanism.

**IV.Results and Analysis**: It contains the Implementation of the Algorithm using Python Programming Language. The Below Screenshot is taken from Python Code where we are finding the correlation between the MessageId and AttackerType under ML-SVR Regression Model.

\



**Fig2: Screenshot Depicting Support Vector Regression Correlation for attacker types and message-id.(Output by Coding in Python)**



**Fig3: Screenshot of the Scatter Plot for SVR Results(Obtained output by coding in python)**

In Above Figures such as :Fig:2 that is used for Depicting Support Vector Regression Correlation for attacker types and message-id , Fig:3 for Visualizing the SVR results .We can measure the performance and ensure the reliability and creditability of the data which we had classified the nodes under the Vanet system are malicious nodes or are they legitimate nodes using the Machine LearningSVR Algorithm.

A popular method for calculating the coefficients of linear regression equations that represent the connection between one Or rmore independent quantitative variables and a dependent variable, Also had used ordinal least squaresregression (OLS) (simple or multiple linear regression).Below is the OLS Result Summary for our model .

The method of Ordinary Least Squares(OLS) Regression Model is most widely used due to its efficiency. This model gives best approximate of true egression line. The principle of OLS is to minimize the square of errors ( ∑ei2 ). The most commonly used procedure

used for regression analysis is called ordinary least squares (OLS).

Ordinary Least Squares regression (OLS) is a not unusual approach for estimating coefficientsof linear regression equations which describe the connection among one or extra unbiased quantitative variables and a established variable (easy or a couple of linear regression).

**Fig:4- Screenshots for OLSRegressionResults Summary.(Obtained Output byPython Coding)**

**V. Analysis of the Output :**

**V.I Result Parameters from Our Model:** The below diagram depicts the Statistical Measurement of the Result Parameters from the

model we had made using the Algorithm: Vehicular network Based SVR (VNBSVR).Result parameters are: Mean Absolute Error, Mean Squared Error, R2 Score, Adjusted R2 etc.

**Fig:5- Depicts the Statistical Measurement of the Result Parameters and Trust Evaluation is done using Evaluation Metrics.**

**After applying linear regression on the particular dataset and after that, we will study each evaluation metric and check it on our Linear Regression model, Below are some of mentioned one:**

* **Mean Absolute Error(MAE)**
* **Mean Squared Error(MSE)**
* **R Squared (R2)**

**VI. Open Issues and Future Research Directions:**

Our research is discussing about the Vanet Security System using Machine Learning Algorithms similar to SVR (Support Vector Machine) Supervised Learning and employed MAPE for testingthe classification performance by utilising the summarised table and the number of right and incorrect predictions are with count values and broken down by each class for SVR Classification. like-Linear SVR, SVR or SGD Classifier. But still, there are some limitations of our model as we could have done the data analysis by using the IBM SPSS Tool or By using the Artificial Intelligence CNN MODEL( Convolutional neural networks ) tools for deep learning, and are especially suited for analyzing image data. We have done coding for ML using Python and in future, the coding for data analysis for measuring the trust model can be done using R Language, tableau or may be done using Big Data Analytics Tools like Apache Spark, tableau public, etc..Future Scope of the research lies with using the ML unsupervised Learning Algorithms for data processing and using classification algorithms along with clustering algorithms for Prediction and selecting and training the model using ANN and then performing validation and testing for checking the output obtained matches with the predicted values or not? Since we had not used ANN for validation but it can be used with LSTM Algorithm.Even we canalso use the Spark Technology for Data Analysis for Predicting the security level in Vanet System and can use SparkSQL with Blockchain Based IPFS-Trust Management System instead of Machine Learning SVR Model for Data Analysis .

**VII.Conclusions :**

In this paper, we had provided the solutions by predicting and preventing False Data Injection Attack by Integration of Blockchain Based IPFS-TrustManagement System with ML SVR Regression Model for that we fetched the smart wireless antennas sensors and done preprocessing of the data by dividing into training and testing part. Than putting the preprocessed data into IPFS for Offchain storage and using ml for training the data in a distributed manner and collectively using the SVR classifier for attack detection and than on basis of the attack detection we can predict the normal data or abnormal data which is than again choosen or selected as malicious node data and legitimate node data and if we get thefalse alarm attack on the malicious node than we create the smart contract for executing the transactional logic and we had used the Blockchain network with pow scheme with data aggregation to add transactions in it.If there is true attacks, than we log the details and maintained for prevention of the attack and start analyzing the dataset again from start and thereafter doing all these steps we finally stop further. Using the SVR Classifier,We had predicted the relationship between the variables Attacker Types and Message-id and by using data visualization tool ie. scatter plot and ml algorithm for classification of dataset we had classified malicious nodes and legitimate node using SVR Algorithm. We further analyzed the dataset using MAPE for performance evaluation. We further analyzed the dataset using MAPE for performance evaluation.

**Acknowledgement:** This is the original work of Ms.Preeti Grover under the guidance ofDr. Sanjeev Kumar Prasad(Guide) for the Completion of the research paperwork.

**Declaration of Competing Interest:**

1. Conflicts of Interest/ Competing Interests:The authors declare no conflict of interest.
2. *Funding/ Grants/ Financial Support:* No, I did not receive.
3. *Ethical Approval and Consent to Participate:* No, the article does not require ethical approval and consent to participate with evidence.

**DATA AVAILABILITY STATEMENT :**The datasets analyzed during the current study are available in the [VeReMi] repository, [VeReMi dataset | VeReMi-dataset.github.io](https://veremi-dataset.github.io/) .

**References:**

[1].M. Furdek et al., "An overview of security challenges in communication networks," 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM), 2016, pp. 43-50, doi: 10.1109/RNDM.2016.7608266.

1. Praveen Kumar P, Syam Kumar P, Alphonse P.J.A.,Attribute based encryption in cloudcomputing: A survey, gap analysis, and future directions,Journal of Network and Computer Applications,Volume 108,2018,Pages 37-52,ISSN 1084-8045,https://doi.org/10.1016/j.jnca.2018.02.009.

[3]M. Nehe and S. A. Jain, "A Survey on Data Security using Blockchain: Merits, Demerits and Applications," 2019 International Conference on Recent Advances in Energy-efficient Computingand Communication (ICRAECC), Nagercoil, India, 2019, pp. 1-5, doi:

10.1109/ICRAECC43874.2019.8995064.:

[4]L. Xu, C. Jiang, J. Wang, J. Yuan and Y. Ren, "Information Security in Big Data: Privacy and Data Mining," in IEEE Access, vol. 2,

pp. 1149-1176, 2014, doi: 10.1109/ACCESS.2014.2362522.

[5]Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," in IEEE Access, vol. 6, pp. 35365-35381, 2018, doi: 10.1109/ACCESS.2018.2836950.

[6]L. He, Z. Yan and M. Atiquzzaman, "LTE/LTE-A Network Security Data Collection and Analysis for Security Measurement: A

Survey," in IEEE Access, vol. 6, pp. 4220-4242, 2018, doi: 10.1109/ACCESS.2018.2792534.

[7]Paul J. Taylor, TooskaDargahi, Ali Dehghantanha, Reza M. Parizi, Kim-Kwang RaymondChoo,A systematic literature review of

blockchain cyber security, Digital Communications and Networks,Volume 6, Issue 2,2020,Pages 147-156,ISSN

2352-

8648,https://doi.org/10.1016/j.dcan.2019.01.005.

[8]Y. R. Bachupally, X. Yuan and K. Roy, "Network security analysis using Big Data technology," SoutheastCon 2016, Norfolk, VA,

2016, pp. 1-4, doi:10.1109/SECON.2016.7506686.

[9]Z. Jin and Z. Jian, "Research on Application of Internet of Things Information Security UsingBlockchain Technology," 2020 IEEE

International Conference on Power, Intelligent Computing and Systems (ICPICS), Shenyang, China, 2020, pp.

402-404, doi:10.1109/ICPICS50287.2020.9202375.

[10]H. R. Andrian, N. B. Kurniawan and Suhardi, "Blockchain Technology and Implementation

* A Systematic Literature Review," 2018 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung - Padang, Indonesia, 2018, pp. 370-374, doi: 10.1109/ICITSI.2018.8695939.:https://ieeexplore.ieee.org/document/8695939

[11]S. V. Kartalopoulos, "Differentiating Data Security and Network Security," 2008 IEEE International Conference on Communications, Beijing, 2008, pp. 1469-1473, doi: 10.1109/ICC.2008.284.

[12]Sarker, I.H., Kayes, A.S.M., Badsha, S. et al. Cybersecurity data science: an overview from machine learning perspective. J Big Data 7, 41 (2020). [https://doi.org/10.1186/s40537-020- 00318-5](https://doi.org/10.1186/s40537-020-00318-5)

[13]L. Yue, H. Junqin, Q. Shengzhi and W. Ruijin, "Big Data Model of Security Sharing Based on Blockchain," 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM), Chengdu, 2017, pp. 117-121, doi: 10.1109/BIGCOM.2017.31. [14]A. Farion, O. Dluhopolskyi, S. Banakh, N. Moskaliuk, M. Farion and Y. Ivashuk, "Usingblockchain Technology for Boost Cyber Security," 2019 9th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 2019, pp. 452-455, doi: 10.1109/ACITT.2019.8780019.

Swarnkar M., Bhadoria R.S., Sharma N. (2021) Security, Privacy, Trust Management and Performance Optimization of Blockchain Technology. In: Namasudra S., Deka G.C. (eds) Applications of Blockchain in Healthcare. Studies in Big Data, vol 83.Springer, Singapore.https://doi.org/10.1007/978-981-15-9547-9\_3

G. SUBATHRA and ANTONIDOSS, "Secure Blockchain-based Storage with Meta-Key – DataSharing Mechanism," 2020 Fourth International Conference on Inventive Systems and

Control (ICISC), Coimbatore, India, 2020, pp. 138-142, doi: 10.1109/ICISC47916.2020.9171064.

Dasgupta, D., Shrein, J.M. & Gupta, K.D. A survey of blockchain from securityperspective.J BANK FINANC TECHNOL 3, 1–17 (2019).https://doi.org/10.1007/s42786-018- 00002-6.

A. Farion, O. Dluhopolskyi, S. Banakh, N. Moskaliuk, M. Farion and Y. Ivashuk, "Using blockchain Technology for Boost Cyber Security," 2019 9th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 2019, pp. 452-455, doi: 10.1109/ACITT.2019.8780019.

V. Monev, "Defining and Applying Information Security Goals for Blockchain Technology," 2020 International Conference on Information Technologies (InfoTech), Varna, Bulgaria, 2020, pp. 1-4, doi: 10.1109/InfoTech49733.2020.9211073.

L. Liu and B. Xu, "Research on information security technology based on blockchain," 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), Chengdu, 2018, pp. 380-384, doi: 10.1109/ICCCBDA.2018.8386546.

Johnstone M., Peacock M. (2020) Seven Pitfalls of Using Data Science in Cybersecurity. In: Sikos L., Choo KK. (eds) Data Science in Cybersecurity and Cyberthreat Intelligence. Intelligent Systems Reference Library, vol 177. Springer, Cham.https://doi.org/10.1007/978-3-030-38788- 4\_6.

[22]G. Liang, S. R. Weller, F. Luo, J. Zhao and Z. Y. Dong, "Distributed Blockchain-Based Data Protection Framework for

Modern Power Systems Against Cyber Attacks," in IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 3162-3173, May 2019, doi:

10.1109/TSG.2018.2819663.

[23]M. Steichen, B. Fiz, R. Norvill, W. Shbair and R. State, "Blockchain-Based, Decentralized Access Control for IPFS," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1499- 1506, doi:

10.1109/Cybermatics\_2018.2018.00253.

 [24]K. Wang, J. Dong, Y. Wang and H. Yin, "Securing Data With Blockchain and AI," in IEEEAccess, vol. 7, pp. 77981-77989, 2019, doi: 10.1109/ACCESS.2019.2921555.

[25]SebahattinDemirkan, IremDemirkan& Andrew McKee (2020): Blockchain technology in thefuture of business cyber security and

accounting, Journal of Management Analytics, DOI: 10.1080/23270012.2020.1731721.

[26]S. X. Wu and W. Banzhaf, “The use of computational intelligence in intrusion detection systems: a review,” Applied Soft Computing

Journal, vol. 10, no. 1, pp. 1–35, 2010.View at: Publisher Site | Google Scholar.

E. Bonabeau, M. Dorigo, and G. Theraulaz, Swarm Intelligence: From Natural to ArtificialIntelligence, Oxford University Press, Oxford, UK, 1999.

T. Mahmood and U. Afzal, "Security Analytics: Big Data Analytics for cybersecurity: A review of trends, techniques and tools," 2013

2nd National Conference on Information Assurance (NCIA), Rawalpindi, 2013, pp. 129-134, doi: 10.1109/NCIA.2013.6725337. [29]S. Curry, E. Kirda, E. Schwartz, W. H. Stewart, and A. Yoran, “Big Data Fuels Intelligence-Driven Security”, RSA Security Brief, January, 2013.

N. Srivastava and U. Chandra Jaiswal, "Big Data Analytics Technique in Cyber Security: A Review," 2019 3rd International Conference

on Computing Methodologies and Communication (ICCMC), Erode, India, 2019, pp. 579-585, doi: 10.1109/ICCMC.2019.8819634. Pandey, Shailja. (2011). MODERN NETWORK SECURITY: ISSUES AND CHALLENGES.International Journal of Engineering Science and Technology.

[32]P. Sinha, A. k. Rai and B. Bhushan, "Information Security threats and attacks with conceivable counteraction," 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur,Kerala, India, 2019, pp. 1208-1213, doi: 10.1109/ICICICT46008.2019.8993384.

[33]C. Aravindan., T. Frederick, V. Hemamalini. and M. V. J. Cathirine, "An Extensive Research onCyber Threats using Learning Algorithm," 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Vellore, India, 2020, pp. 1-8, doi: 10.1109/ic-ETITE47903.2020.337.

R. John, J. P. Cherian and J. J. Kizhakkethottam, "A survey of techniques to prevent sybil attacks," 2015 International Conference on Soft-Computing and Networks Security (ICSNS), Coimbatore, 2015, pp. 1-6, doi: 10.1109/ICSNS.2015.7292385.

“Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users”International Journal of Comp.

Angin, Pelin&Bhargava, Bharat &Ranchal, Rohit. (2019). Big Data Analytics for CyberSecurity.Security and Communication Networks.

2019. 1-2. 10.1155/2019/4109836.

Verma, Pushpak. (2016). Network Security in Big Data: Tools and Techniques.10.1007/978-81-322-2755-7\_26. <http://www.ibm.com/software/security/>

“Big security for big data”, Business White Paper, HP, December 2012 [https://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html](http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html)

[40]P. Helebrandt, M. Bellus, M. Ries, I. Kotuliak and V. Khilenko, "Blockchain Adoption for Monitoring and Management of Enterprise Networks," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, 2018, pp. 1221-1225, doi: 10.1109/IEMCON.2018.8614960.

[41]Alam, Furqan&Katib, Iyad&Alzahrani, Ahmed. (2013). New Networking Era: Software Defined Networking. International Journal of Advanced Research in Computer Science and Software Engineering. 4.

[42]D. Homan, I. Shiel and C. Thorpe, "A New Network Model for Cyber Threat Intelligence Sharing using Blockchain Technology,"

2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, 2019, pp. 1-6, doi:

10.1109/NTMS.2019.8763853.

[[43]Greenspan,G.,2015b.MultiChainPrivateBlockchain,WhitePaper,http://www.multichain.com](http://www.multichain.com/)

/ download/MultiChain-White-Paper.pdf.

[44]L. Mohan, S. Jain, P. Suyal and A. Kumar, "Data mining Classification Techniques for Intrusion Detection System," 2020 12th

International Conference on Computational Intelligenceand Communication Networks (CICN), Bhimtal, India, 2020, pp. 351-355, doi:

10.1109/CICN49253.2020.9242642.

Blockchains for Network Security: Principles, Technologies and Applications. N.p., Institutionof Engineering and Technology, 2020. M. Singh, G. S. Aujla, A. Singh, N. Kumar and S. Garg, "Deep-Learning-Based Blockchain Framework for Secure Software-Defined Industrial Networks," in IEEE Transactions on Industrial Informatics, vol. 17, no. 1, pp. 606-616, Jan. 2021, doi:

10.1109/TII.2020.2968946.

[47]A. Bose, G. S. Aujla, M. Singh, N. Kumar and H. Cao, "Blockchain as a Service for Software Defined Networks: A Denial of Service Attack Perspective," 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Fukuoka, Japan, 2019, pp. 901-

C. Zhang, X. Shen, X. Pei and Y. Yao, "Applying Big Data Analytics Into Network Security: Challenges, Techniques and Outlooks,"

2016 IEEE International Conference on Smart Cloud(SmartCloud), New York, NY, USA, 2016, pp. 325-329, doi:

10.1109/SmartCloud.2016.62.

[48]Y. Mengke, Z. Xiaoguang, Z. Jianqiu and X. Jianjian, "Challenges and solutions of information security issues in the age of big data," in China Communications, vol. 13, no. 3, pp. 193-202, March 2016, doi: 10.1109/CC.2016.7445514.

[49]Gang Chen, Sai Wu, Yuan Wang,The Evolvement of Big Data Systems: From the Perspective of an Information Security Application,Big Data Research,Volume 2, Issue 2,2015,Pages 65- 73,ISSN 2214-5796,https://doi.org/10.1016/j.bdr.2015.01.002. [50]TALABIS, M., MARTIN, J. L., MCPHERSON, R., & MIYAMOTO, I. (2015). Information security

analytics: finding security insights, patterns, and anomalies in big data. Waltham, MA, Syngress.

[51]Naz M, Al-zahrani FA, Khalid R, Javaid N, Qamar AM, Afzal MK, Shafiq M. A Secure Data Sharing Platform Using Blockchain and Interplanetary File System. Sustainability. 2019; 11(24):7054. https://doi.org/10.3390/su11247054.

[52]S. Wang, Y. Zhang and Y. Zhang, "A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems," in IEEE Access, vol. 6, pp. 38437-38450, 2018, doi: 10.1109/ACCESS.2018.2851611.

[53]S. Jianjun, L. Ming and M. Jingang, "Research and application of data sharing platform integrating Ethereum and IPFs Technology," 2020 19th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES), Xuzhou, China, 2020, pp. 279-282, doi: 10.1109/DCABES50732.2020.00079.

[54]Naz, Muqaddas; Al-zahrani, Fahad A.; Khalid, Rabiya; Javaid, Nadeem; Qamar, Ali M.; Afzal, Muhammad K.; Shafiq, Muhammad.

2019. "A Secure Data Sharing Platform Using Blockchain and Interplanetary File System" Sustainability 11, no. 24: 7054.

https://doi.org/10.3390/su11247054.

[55]Fukumitsu, M.; Hasegawa, S.; Iwazaki, J.; Sakai, M.; Takahashi, D. A proposal of a secure P2P-type storage scheme by using the secret sharing and the blockchain. In Proceedings of the 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), Taipei, Taiwan, 27–29 March 2017; pp. 803–810.

[56]V. Hoang, E. Lehtihet and Y. Ghamri-Doudane, "Privacy-Preserving Blockchain-Based Data Sharing Platform for Decentralized Storage Systems," 2020 IFIP Networking Conference (Networking), Paris, France, 2020, pp. 280-288. [58]Reshiwaran A/L Jegatheswaran et al 2020 J. Phys.: Conf. Ser. 1712 012020

[57]A. R. Onik, N. F. Haq and W. Mustahin, "Cross-breed type Bayesian network based intrusion detection system (CBNIDS)," 2015 18th International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 2015, pp. 407-412, doi:

10.1109/ICCITechn.2015.7488105.

[58]MdReazulKabir, AbdurRahmanOnik and TanvirSamad. A Network Intrusion Detection Framework based on Bayesian Network using Wrapper Approach. International Journal of Computer Applications 166(4):13-17, May 2017.

[59]B. Dong and X. Wang, "Comparison deep learning method to traditional methods using fornetwork intrusion detection," 2016 8th

IEEE International Conference on CommunicationSoftware and Networks (ICCSN), 2016, pp. 581-585, doi:

10.1109/ICCSN.2016.7586590. [62]AnimeshPatcha, Jung-Min Park,An overview of anomaly detection techniques: Existing solutions and

latest technological trends,ComputerNetworks,Volume 51,

Issue12,2007,Pages34483470,ISSN13891286,https://doi.org/10.1016/j.comnet.2007.02.001.

[60]Selvaraj, Sharanya & Selvaraj, Karthikeyan. (2017). Classifying malicious nodes in VANETsusing Support Vector Machines with Modified Fading Memory. 12. 171-176.

[61]Narasimman, Karthik & Dhulipala, V.R.Sarma. (2011). Trust calculation in wireless sensornetworks. 10.1109/ICECTECH.2011.

[62]M. S. Iftikhar, N. Javaid, O. Samuel, M. Shoaib and M. Imran, "An Incentive Scheme for VANETs based on Traffic Event Validation using Blockchain," 2020 International Wireless Communications and Mobile Computing (IWCMC), 2020, pp. 2133-2137, doi:

10.1109/IWCMC48107.2020.9148556.

[63]Fadzil, Mohd & Hooi, Yew & Qureshi, Muhammad Aasim & Chung, Tran & Akbar, Rehan & Safdar, Sohail & Rehman, Abdul. (2021).

[64]Context and Machine Learning Based Trust Management Framework for Internet of Vehicles. Cmc -Tech Science Press-. 68. 4125-4142. 10.32604/CMC.2021.017620. [68]https://datagy.io/mape-[python/https://www.askpython.com/python/examples/mape-](http://www.askpython.com/python/examples/mape-)mean-absolute-percentage-error.

[65]S. Abe. 2010. Support Vector Machines for pattern classification. Advances in Pattern Recognition, 2nd ed., Springer. pp. 2089-2093. [70]H. Yang, H. Luo, F.Ye, S. Lu, L. Zhang. 2004.Security in mobile ad hoc networks: challenges and

solutions. IEEE Wireless Communications.

[66]VANSec: Attack-Resistant VANET Security Algorithm in Terms of Trust Computation Error and Normalized Routing Overhead. Sheeraz Ahmed ,Mujeeb Ur Rehman,Atif Ishtiaq,Sarmadullah Khan ,Armughan Ali, and Shabana Begum,Iqra National University, Peshawar, Pakistan,Career Dynamics Research Centre, Peshawar, Pakistan,School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK,COMSATS Institute of Information Technology, Attock, Pakistan,Islamia College University, Peshawar, Pakistan.

[67]https://ebooks.iospress.nl/pdf/doi/10.3233/APC210117, VANET: Trust Evaluation Using Artificial Neural Network.

[68]Rathee G, Ahmad F, Kerrache CA, Azad MA. A Trust Framework to Detect Malicious Nodes in Cognitive Radio Networks. Electronics. 2019; 8(11):1299. [https://doi.org/10.3390/electronics8111299.](https://doi.org/10.3390/electronics8111299)

[69]A Comprehensive Survey on VANET Security Services in Traffic Management System,Hindawi,Wireless Communications and

Mobile Computing.Volume 2019,Article ID 243915,23 Pages,https://doi.org/2019/2423915.

[70]A Privacy-Preserving Attack-Resistant Trust Model for Internet of Vehicles Ad Hoc Networks,https://doi.org/10.1155/2020/8831611, 10.1155/2020/8831611,Scientific Programming, Hindawi.

[71]Liu G, Fan N, Wu CQ, Zou X. On a Blockchain-Based Security Scheme for Defense against Malicious Nodes in Vehicular Ad-Hoc Networks. Sensors. 2022; 22(14):5361. [https://doi.org/10.3390/s22145361.](https://doi.org/10.3390/s22145361)

[72]Alghofaili Y, Rassam MA. A Trust Management Model for IoT Devices and Services Based on the Multi-Criteria Decision-Making Approach and Deep Long Short-Term Memory Technique. Sensors. 2022; 22(2):634. https://doi.org/10.3390/s22020634.

[73] W. Li and W. Meng, "BCTrustFrame: Enhancing Trust Management via Blockchain and IPFS in 6G Era," in IEEE Network, vol. 36, no. 4, pp. 120-125, July/August 2022, doi: 10.1109/MNET.013.2100768.

[74] https://www.researchgate.net/publication/367291135\_Vanet\_FDIA\_Solutions\_using\_Blockchain\_Based\_IPFS-Trust\_Management\_System\_with\_ML\_SVR\_Model. DOI:10.21203/rs.3.rs-2483611/v1

Mobile Computing.Volume 2019,Article ID 243915,23 Pages,https://doi.org/2019/2423915.

1. A Privacy-Preserving Attack-Resistant Trust Model for Internet of Vehicles Ad Hoc Networks,https://doi.org/10.1155/2020/8831611, 10.1155/2020/8831611,Scientific Programming, Hindawi.
	1. Liu G, Fan N, Wu CQ, Zou X. On a Blockchain-Based Security Scheme for Defense against Malicious Nodes in Vehicular Ad-Hoc Networks. Sensors. 2022; 22(14):5361. [https://doi.org/10.3390/s22145361.](https://doi.org/10.3390/s22145361)
2. Alghofaili Y, Rassam MA. A Trust Management Model for IoT Devices and Services Based on the Multi-Criteria Decision-Making Approach and Deep Long Short-Term Memory Technique. Sensors. 2022; 22(2):634. https://doi.org/10.3390/s22020634.