Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume7-Issue1, January 2024
Paper: 57

Electric Vehicles Using Block Chain Based on Machine Learning Algorithm

A.S.Malini AP/CSE
Department of Computer Science and Engineering
P.S.R.R College of Engineering
malini@psrr.edu.in

M.Malathi
Computer Science and Engineering
P.S.R.R College of Engineering
Anna University
mm26032001@gmail.com

B.Guru Lakshmi
Computer science and Engineering
P.S.R.R College of Engineering
Anna University
abi353126@gmail.com

R.Sakthi Priya
Computer Science and Engineering
P.S.R.R College of Engineering
Anna University
priyacse3042002@gmail.com

ABSTRACT **Cybersecurity is neglected, any network system loses its effectiveness, trustability, and adaptability. With the huge integration of the Information, Communication and Technology capabilities, the Connected Electric Vehicle(CEV) as a transportation form in metropolises is getting more and also effective and suitable to reply to citizen and environmental prospects which better the quality of citizens life. It targets the cybersecurity issues for CEVs in parking lots where a peer- to- peer(P2P) energy sale system predicated on blockchain, and smart contract scheme is launched. A False Data Injection Attack on the electricity price and power signal is proposed and a Machine literacy/ SVM class protocol is used to determine and prize the right values. Simulation results are conducted to prove the effectiveness of this proposed model.**

Keywords ***Blockchain, connected electric vehicles, false data injection attack, machine learning, support vector machine,smart contract.***

I.INTRODUCTION

Eliptic Cryptography arc, an indispensable form to Rivest Shamir Adleman, is a important cryptography approach. It generates security between crucial braces for public key encryption by using the mathematics of elliptic angles. RSA algorithm does entity analogous with high arithmetic rather of elliptic curvatures, but ECC has gradationally been growing in fashionability lately due to its lower crucial size and capability to maintain security. This trend will presumably continue as the demand on bias to remain secure increases due to the size of keys growing, drawing on scarce mobile coffers. This is why it's so important to understand elliptic wind cryptography. In discrepancy to RSA algorithm, ECC bases its approach to public key cryptography systems on how elliptic angles are structured algebraically over finite fields. thus, ECC creates keys that are more delicate, mathematically, to crack. For this reason, ECC is considered to be the coming generation perpetration of public key cryptography and further safe. It also makes sense to borrow ECC to maintain high situations of both performance and security. That's because ECC is decreasingly in wider use as websites strive for lesser online security in client data and lesser mobile optimization coincidently. further spots using ECC to secure data means a lesser need for this kind of quick companion to elliptic wind crypto. An elliptic wind for current ECC purposes is a over a finite field which is made up of the points satisfying the equation

$$y^2=x^3 + ax + b$$

In this elliptic wind cryptography illustration, any point on the wind can be imaged over thex-axis and the wind will stay the same. Anynon-vertical line will cross the wind in three places With the enhancement of pall services, data possessors are getting motivated in outsourcing their data into the pall garçon to achieve better access and storehouse installation at a low cost. Cracking the data before outsourcing into the pall is considered as a general approach for guarding data sequestration. Indeed though encryption protects the data against unauthorized access, but at the same time, it also activates vexation for the authorized druggies in penetrating the translated data at large. As a result, important exploration is being carried out so as to snappily recoup the information from the huge pool of data using some keyword-grounded hunt ways. It has come a challenge for the experimenters to give an effectivemulti-keyword hunt model. sequestration-conserving conjunctive keyword hunt system over translated pall data cares the update operations stoutly. The indicator structure is constructed on the base ofMulti-Attribute Tree and an effective hunt procedure which is known as hunt MAT algorithm is introduced. In order to enhance the effectiveness of the textbook

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume7-Issue1, August 2023
Paper: 57

searching the indicator structure grounded on the Hierarchical Agglomerative Clustering tree indicator(HAC- tree) is proposed. To cipher the indicator of HAC tree and query vector, this system uses the secure inner product algorithm. In this,Non-candidate Pruning DFS Algorithm is used to search the corresponding file in the tree which prunes thesub-tree which doesn't contain any hunt result to increase the relevancy of the searched keyword to the shadow column, the match matching along with inner product similarity is introduced. Rear data structure to permit druggies to negotiate dynamic operations on document collection is proposed, which perform either fitting or deleting.

The advanced protocol support many keyword quests similar as conjunctive keyword hunt and disjunctive keyword hunt. In the disjunctive keyword hunt, it apprehends in a plain way that it sends the worths of the keyword to the server in the query. In the conjunctive keyword hunt, the addition of all keywords values is used as the fresh keywords values involved in the computation. By using these two quests this system achieves effective hunt and matched cipher textbook themulti-keyword tree- grounded hunt scheme is proposed to give security to the sensitive information of the data possessors. The document collection in the pall terrain is achieved through the hierarchical clustering system. To induce an translated indicator as well as query vectors, the vector space model is used and to achieve effective hunt, DFS algorithm is used. The secure proposed algorithm is used to cipher the query vectors. The clustering of documents is performed using intersecting k- means clustering.

Environment- apprehensive hunt is introduced to make semantic hunt smart. The proposed system first introduces the Semantic emulsion Keyword Hunt(SCKS) as a knowledge representation tool. Two schemes are proposed grounded on CG. This system converts original CG into their corresponding direct form with smaller variations and it matches them to numerical vectors. Ranked multi keyword hunt over translated data in the pall is introduced on the base of two trouble models. To resolve the problem in the sequestration- conserving smart semantic hunt grounded on CGs, the proposed scheme uses PRSCG and PRSCG-TF schemes. The emulsion conception semantic similarity evaluation system is projected to quantify the similarity between the emulsion generalities. This system integrates both secure K nearest neighbour scheme and CCSS with position Sensitive Hashing Function, therefore proposing the Semantic emulsion Keyword Hunt(SCKS).

The thing of secure this scheme is to steadily fete the K-Nearest points in the translated databank to a handed translated query. This proposed system not only achieves semantic-grounded hunt but at the same time also performs amulti-keyword hunt and ranks the searchedresult.One of the most common type ofcyber-attacks that was firstly introduced in the power systems is the False Data Injection Attack(FDIA). This type of attack is suitable to compromise the most vital concern of the data integrity by infectingdevices.It can produce untruthful values of the state estimation(SE), use malware to infect waiters of power suppliers, falsify the real volume of energy truly handed, and virulently forget the network countries by vacating bumps. therefore, the FDIA can give a huge deceiving of the energy distribution, performing in ruinous power deficit, redundant energy transmission costs, knockouts, and overloads. substantially, FDIA can target the electricity price and the power line cargo. For the first script, this attack manipulates the price data entered from a mileage or any other electricity service provider. As a result, each consumer will admit different electricity prices which make anwillful demand side operation medium by intruding the metering data transmission. This false metering can beget for illustration a dysfunction of the cargo balancing procedure or scheduling protocol. The damage is in terms of insecurity of the grid network or in terms of dropped stoner satisfaction situations. The alternate case is grounded on the malfunction of a system operation caused by edging in false data into the dimension system. therefore, a hacker can manipulate the consumer and or the mileage cargo which can affect in significant and expensive damage to the power grid. This damage can go to Smart Grid(SG) structure and a implicit SG failure by overfilling the bias and power lines Which can bring billion of bones
for certain communities in addition to victims which are losing their life in certain scenario.To overcome this problem, the attack discovery is the most essential step in minimizing the damages. Several approaches are proposed since 2010 to descry FDIAs. Some of them were grounded on SE type similar as the conventional bad data discovery, the SE partitioning, and the discovery grounded on dynamic Systems Engineering. Other approaches are grounded on protection, among them there are the optimal Phasor Measurement Unit(PMU) placement, and the selection of optimal measures.

.

II.EXISITNG SYSTEM

The use of Cloud Service Provider(CSP) reduces hunt time and increases hunt effectiveness by exercising a Boolean hunt in the proxy server.Main server supports multiple druggies at a time with the help of Deep learning grounded Neural Network, which provides an accurate result.Trusted Authority is employed to give secure document reclamation for authorized stoner. Trusted Agent manages binary security processes as crucial operation and Security Device Issuing.Secure top k ranking is achieved using Euclidean distance computation and delicacy of document reclamation is developed.In being system, This is because ML/ DL grounded styles can capture benign and anomalous in Internet Of effects surroundings. IoT bias and network business can be captured and delved to learn normal patterns. Any deviation from these normal learned patterns can be used to descry anomalous geste likewise, Machine Learning and Deep Learning grounded styles have been tested to prognosticate new or zero- day attacks.

The delicacy is 50% and special IOT tackle needed the accuracy.It can display the battery position and charging, discharging level.It doesn’t effective for large volume of data’s Training model vaticination on Time is High It's grounded on Low delicacy content of FDIA is attracting several industrials and cyber

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume7-Issue1, August 2023
Paper: 57

security experimenters in different fields and especially in SG as a centralized armature. In the literature, a variety of strategies are suggested to reduce FDIA. The FDIA discovery and exploration workshop can be divided into four major sub-categories. The SE kind is highlighted in the first one. The protection- grounded defence is the goal of the alternative. The third one takes into account statistical models, and the final bone is based on utilising ML capabilities.

For the first order, in the reference, the statistical test of the Largest regularized Residual(LNR) is presented to single, and multiple, interacting issues but non-conforming bad data. It's shown that this model isn't effective for bad influence points. For the alternate order, the authors propose a PMU placement fashion to insure that an L1 state estimator has the necessary quantum of adaptability against poor measures. still, PMUs are precious, and installing enough of them to insure detector readings is impracticable. It's more precious, particularly with the integration of new ubiquitous seeing technology into large- scale of network systems similar as Smart Grids. For the third order, numerous statistical models were proposed, for illustration the Bayesian test sensor in reference where authors developed a Bayesian test to relating relay malfeasance(false data injection) at the packet position in loss one way wireless relay networks, nonetheless, another study shows that the Bayesian fashion fails to descry an attack when vicious data has the same distribution pattern as literal data or when an adversary replaces current cadence readings with previous readings with the same distribution. Although these approaches stated above are making enhancement in detecting FDI assaults, but they're getting decreasingly limited as FDIAs get more complex and sophisticated schemes suitable to surpass the SG protection layers. In the last order, grounded on examination of the current exploration workshop, it set up out that numerous studies were conducted in the content of FDIA using ML like where different ML models like the intermittent Neural Network(RNN) and Artificial Neural Network(ANN) to descry FDIA in bad bumps or in power system state estimators and there are numerous other studies prove that ML is an effective tool to descry FDIA in power system.

III PROPOSED SYSTEM

cloud services have increased the number of data possessors it has been store their translated data in the pall, while an equal or lesser number of data druggies grounded in data retrieval.AES Algorithm using the Encrypted and deciphered the dataset Translated train will be Stored in Cloud Garçon and stoner grounded on Keyword Searching for Algorithm.User grounded Enter the keyword that also Translated Query After that Searching Encrypted pall Garçon Eventually, Retrieval process is done to cost the translated train, which is Related to the Query data.User grounded enter the Particular crucial stoner decrypts train the better performance better performance in terms of recall, ranking sequestration, perfection, searching time.

Time taken to done the Encryption and decryption is veritably low, when compared with the other techniques.Easy to recoup the data from the cloud.Data loss is low, in the receiver side during the decryption process.It's effective for large number of datasets. It's further effective of performance analysis. Performance was veritably high. It give accurate vaticination results. It avoid sparsity problems. The proposed model is introduced to overcome all the disadvantages that arises in the being system. This system will increase the delicacy of the bracket results by classifying the data grounded on the software quality vaticination dataset and others XGboost Random timber and decision Tree algorithms.It enhances the performance of the overall bracket results.

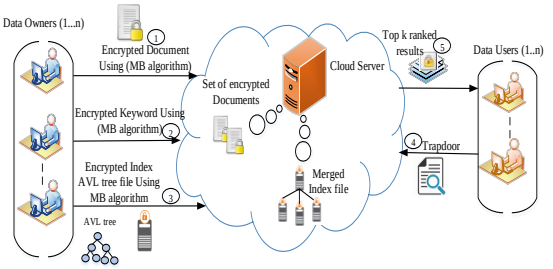

Fig.System architecture

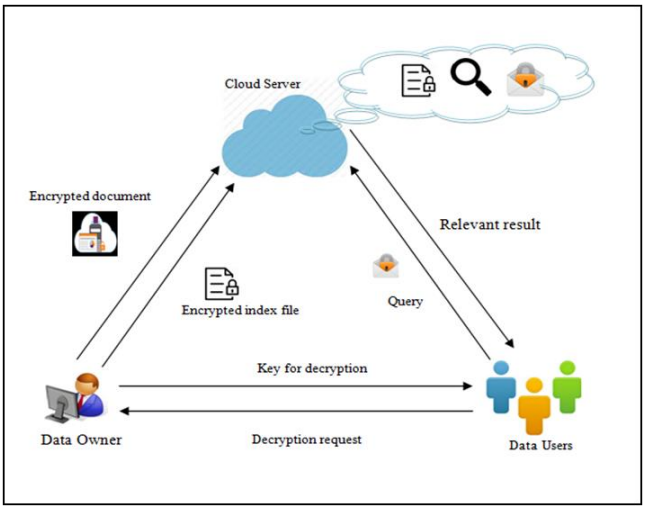

Fig.Block Diagram

The advanced model is introduced to conquer all the drawbacks that arises in the existing system. This system will increase the delicacy of the type outcomes by classifying the data based on the software quality predicting data set and others Navie Bayes Algorithm, arbitrary timber and decision tree algorithms.It enhances the performance of the overall bracket results.Block chain is used to give block of connected vehicles.The user as well as the admin can pierce the information by the exchange of secret key.The delicacy is increased by 98 by the use of CNN algorithm.It display where the fault occurs analogous as failure of

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume7-Issue1, August 2023
Paper: 57

break, motor speed reduced, battery get drained and some other faults do in our electric vehicles.It provides clarity in transaction by the operation of Block Chain Technology.

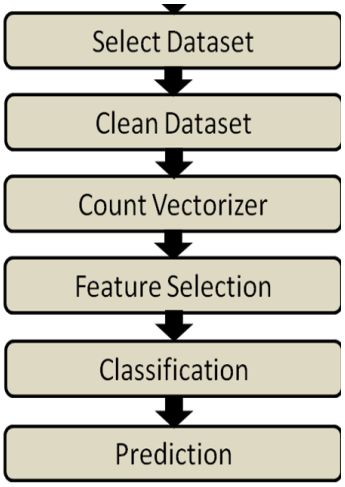

Fig.Flow Chart

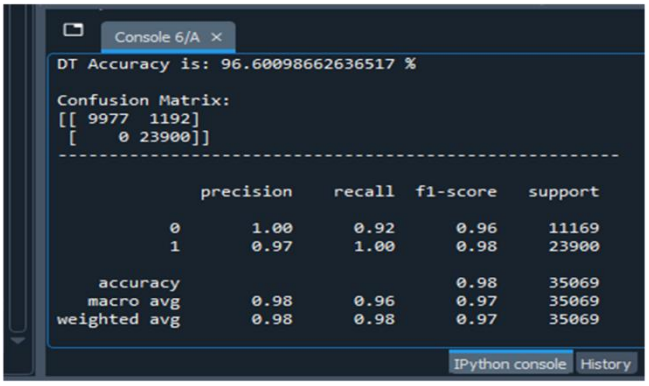

Fig Confusion matrix

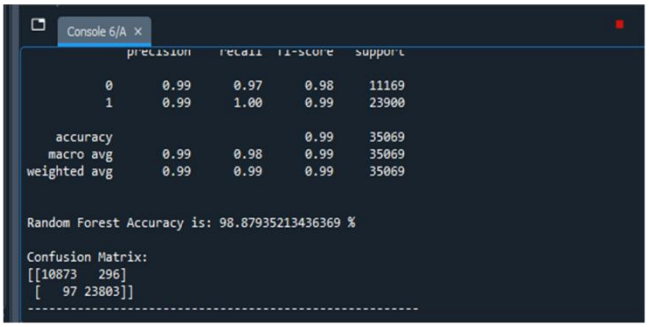

Fig Random Forest Accuracy

Accuracy Delicacy of classifier refers to the capability of classifier. It predicts the class marker correctly and the delicacy of the predictor refers to how well a given predictor can guess the value of called peculiarity for a new data.

$$\mathbf{Ac}=\frac{TP+TN}{TP+TN+FP+FN}$$

Precision Precision is defined as the number of true cons divided by the number of true cons plus the number of false cons.

$$\mathbf{Precision}=\frac{TP}{TP+FP}$$

Recall is the number of correct results divided by the number of results that should have been returned. In binary type, recall is called perceptivity. It can be viewed as the probability that a applicable document is retrieved by the query.

ROC angles are constantly used to show in a graphical way the connection trade-off between clinical perceptivity and particularity for every possible cut- off for a test or a combination of tests. In addition the area under the ROC wind gives an idea about the benefit of using the test in question.

A **confusion matrix** is a table that is often used to describe the performance of a classification model (or "classifier") on a set of test data for which the true values are known.The confusion matrix itself is relatively simple to understand,but the related terminology is confusing.

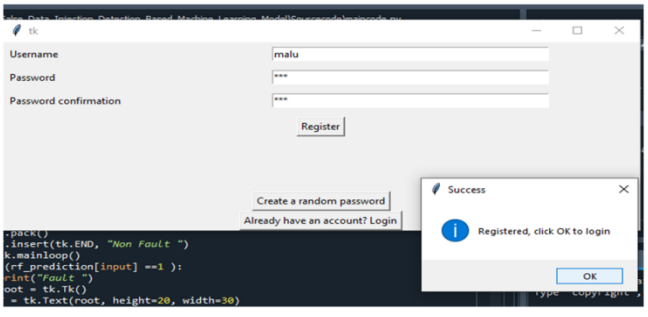

Fig Screenshot of Registration

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume7-Issue1, August 2023
Paper: 57

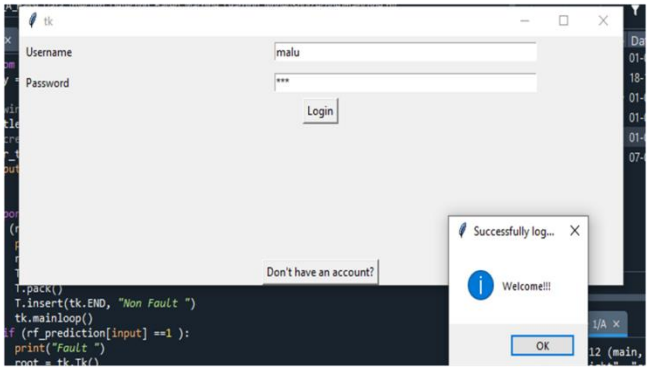

Fig ScreenShot of Login

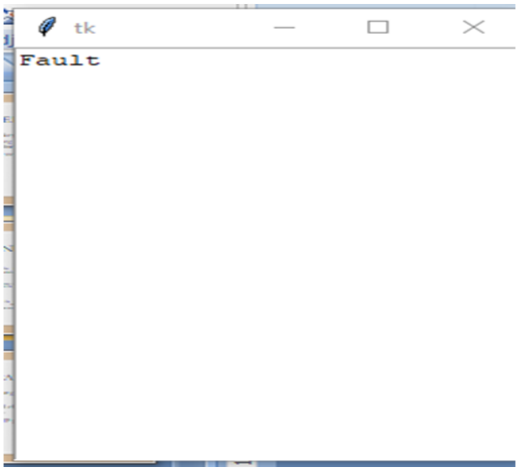

Fig Result

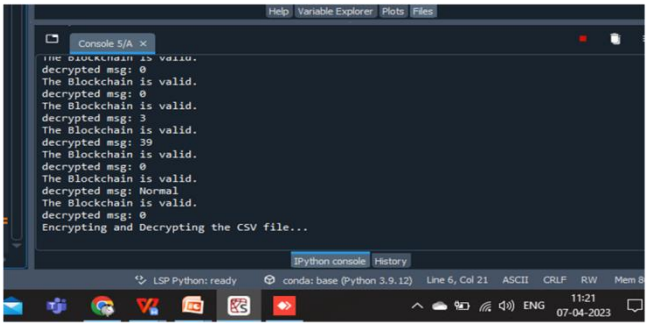

Fig Validating Blocks

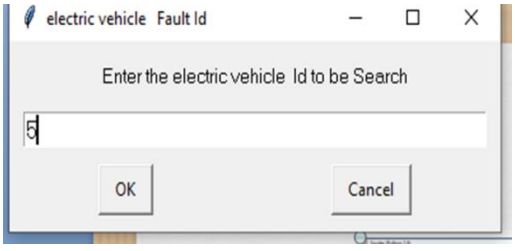

Fig Screenshot of Id to be searched

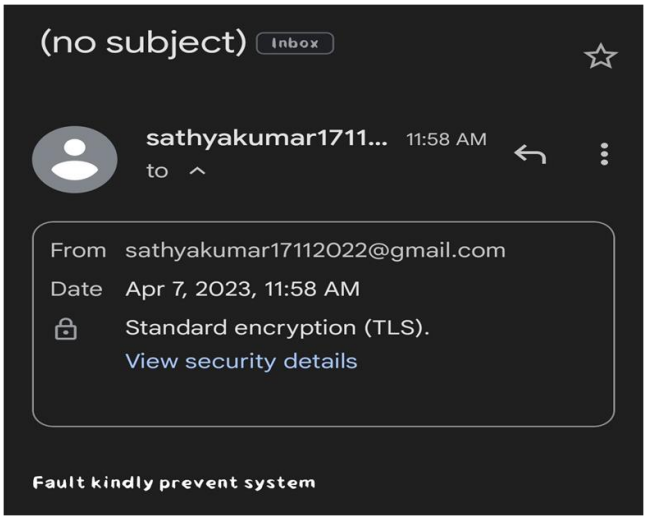

Fig ScreenShot of Notification received through mail

IV.FUTURE WORK

It's grounded on unborn hybrid algorithm for ECC and AES Algorithm You may increase the effectiveness of the Algorithm.we Can unborn perpetration on testing Software for IOT Security The input data was collected from dataset depository. KDDCup99 data selection method for a dataset The data may contain a great deal of irrelevant and missing information. Data cleansing is completed to handle this portion. Running of missing data, noisy data, etc. is involved. Pass across the tuples. Only when we have a sufficiently large dataset and an a tuple has numerous missing values does this strategy make sense.There are colorful ways to do this task. You can choose to fill the missing values manually, by trait mean or the most probable value.That categorical data is defined as variables with a

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume7-Issue1, August 2023
Paper: 57

finite set of marker values. That most machine literacy algorithms take numerical input and affair variables. That an integer and one hot encoding is used to convert categorical data to integer data.Scikit- learn's Count Vectorizer is used to convert a collection of manual documents to a vector of term/ commemorative counts. It also enables the pre-processing of textbook data previous to generating the vector representation. This functionality makes it a largely flexible point representation module for text.Data splitting is the act of partitioning available data into two portions, generally for cross-validator purposes. Separating data into training and testing sets is an important part of assessing data mining models. generally, when you separate a data set into a training set and testing set, utmost of the data is used for training, and a lower portion of the data is used for testing. To train any machine literacy model irrespective what type of dataset is being used you have to resolve the dataset into training data and testing data.In machine literacy, bracket refers to a prophetic modelling problem where a class marker is forecast for a given illustration of input data. Classification is the task of reading a separate class marker. Retrogression is the task of reading a non stop quantity.In machine literacy, bracket is a supervised literacy conception which principally categorizes a set of data into classes. Before bracket, we should have resolve the data into test and train. utmost of data's are used for training and lower portion of the data's are used for testing. Training data is used for estimate the model and testing data is used for predictive the model. After data splitting, we've to apply the bracket algorithm. In our process, we've to use, support vector machine(SVM) Predictive analytics algorithms try to achieve the smallest error possible by either using " boosting " or " bagging ".

.

V.CONCLUSION

Hybrid ECC and AES Algorithm using the Encrypted and deciphered the dataset Translated train will be Stored in Cloud Garçon and stoner grounded on Semantic Searching system Algorithm. User grounded keyword Entering is done to re-collect the corresponding data train from the Cloud storage.Finally recapture the Affiliated train grounded on Query. This will fluently Find out Cyber security Problem like, the fault train will be detected. False data injection attacks are considered to be one of the most dangerous hazards against ML and data driven technologies.Assaulters can damage the whole system and degrade its performance by edging in vicious data in a training sequence set of the ML. This paper presents a cyber security scheme suitable to identify attacked sequence using our SVM Algorithm. Numerical results and simulations demonstrate the strength of the proposed algorithm to discover FDIA and prize the right values. As a coming workshop, this composition can be extended for a large scale with realistic test bed considering the Denial of the Service(DoS)and ransomware crypto-ransomware attacks. Privacy Conserving Synonym Grounded Fuzzy Multi-Keyword Ranked Hunt over Encrypted Cloud Data, a scheme which enhances stoner hunt experience to a consummate by furnishing both fuzzy and reverse grounded multi-keyword ranked hunt, thereby taking translated hunt experience closer to free textbook hunt engines. The scheme also improves upon indicator generation time and hunt time in comparison to being schemes by exercising a double tree grounded dynamic index. Experimental results portray the effectiveness of this proposed scheme as it reduces the hunt time To give better electricity service for the guests and minimize the losses for the providers, a vault in the power grid is being, which is applied to as the smart grid. The smart grid is Ideated to increase the discovery delicacy to an respectable position by exercising ultramodern technologies, similar as pall computing. With the end of carrying achievements of anomaly discovery for electricity consumption with pall computing, we originally introduce the introductory description of anomaly discovery for electricity consumption. Then, we check the framework for anomaly finding for power usage that has been proposed, and we suggest a new framework using cloud computing.

VI.REFERENCES

[1] L. Zhang, Y. Zhang and H. Ma, "Privacy-Preserving and Dynamic Multi-Attribute Conjunctive Keyword Search Over Encrypted Cloud Data", IEEE Access, vol. 6, pp. 34214-34225, 2018.

[2] Z. Xiangyang, D. Hua, Y. Xun, Y. Geng, and L. Xiao, "MUSE: An Efficient and Accurate Verifiable Privacy-Preserving Multi-keyword Text Search over Encrypted Cloud Data", Security and Communication Networks, vol. 2017, pp. 1-17, 2017.

[3] L. Chen, L. Qiu, K-C. Li, W. Shi, and N. Zhang, "DMRS: an efficient dynamic multi-keyword ranked search over encrypted cloud data", Soft Computing, vol. 21(16), pp. 4829–4841, 2017.

[4] R. Zhang, R. Xue, L. Liu, and L. Zheng, "Oblivious Multi-Keyword Search for Secure Cloud Storage Service",2017 IEEE 24th International Conference on Web Services, pp. 269-276, 2017.

[5] P. K. Samantaray, N. K. Randhawa, and S. L. Pati, "An Efficient Multi-keyword Text Search Over Outsourced Encrypted Cloud Data with Ranked Results", Computational Intelligence in Data Mining, pp. 31-40, 2018.

[6] Z. Fu, F. Huang, K. Ren, J. Weng, and C. Wang, "Privacy-Preserving Smart Semantic Search Based on Conceptual Graphs Over Encrypted Outsourced Data",IEEE Transactions On Information Forensics And Security, vol. 12(8), pp. 1874-1884, 2017.

[7] B. Lang, J. Wang, M. Li, and Y. Liu, "Semantic-based Compound Keyword Search over Encrypted Cloud Data", IEEE Transactions On Services Computing, 2018.

[8] Z. Fu, L. Xia, X. Sun, A. X. Liu, and G. Xie, "Semantic-aware Searching over Encrypted Data for Cloud Computing", IEEE Transactions on Information Forensics and Security, vol. 13(9), pp. 2359-2371, 2018.

[9] Z. Wu, and K. Li, "VBTree: forward secure conjunctive queries over encrypted data for cloud computing", The VLDB Journal, pp. 1–22, 2018.

[10] Y. Yang, X. Liu, and R. H. Deng, "Multi-user Multi-Keyword Rank Search over Encrypted Data in Arbitrary Language", IEEE Transactions on Dependable and Secure Computing, 2018.
[11] X. Ding, P. Liu, and H. Jin, "Privacy-Preserving Multi-keyword Top-*k* Similarity Search Over Encrypted Data",IEEE Transactions on Dependable and Secure Computing, 2018.
[12] Y. Li, F. Zhou, Y. Qin, M. Lin, and Z. Xu, "Integrity-verifiable conjunctive keyword searchable encryption in cloud storage", International Journal of Information Security, vol. 17(5), pp. 549–568, 2018.
[13] C. Guo, X. Chen, Y. Jie, Z. Fu, M. Li, and B. Feng, "Dynamic Multi-phrase Ranked Search over Encrypted Data with Symmetric Searchable Encryption", IEEE Transactions On Services Computing, 2018.