RESEARCH ARTICLE

SAMRIDDHI Volume 14, Special Issue 2, 2022 Print ISSN : 2229-7111 Online ISSN : 2454-5767

Stock Price Prediction Using Long Short Term Memory

D.G. Bhalke[1*], Daideep Bhingarde[2], Siddhi Deshmukh[3], Digvijay Dhere[4]

[1*] Department of Electronics and Telecommunication Engineering, Dr. D. Y. Patil Institute of Technology (DIT), Pune, India; e-mail : bhalkedg2000@gmail.com

[2-4] Department of Electronics and Telecommunication Engineering, AISSMS College of Engineering, Pune, India.

ABSTRACT

Stock market price prediction is difficult and complex task. Prediction in stock market is very complex and unstable Process. Stock Price are most of the time tend to follow patterns those are more or less regular in stock price curve. Machine Learning techniques use different predictive models and algorithms to predict and automate things to reduce human effort. This research paper focuses on the use of Long Short Term Memory (LSTM) to predict the future stock market company price of stock using each day closing price analysis. LSTM is very helpful in sequential data models. In this paper LSTM algorithm has been used to train and forecast the future stock prices.

Keywords: Long Short Term Memory (LSTM), Sequential data, Machine Learning, Regression, Stock Market, Price Prediction.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, (2022); DOI : 10.18090/samriddhi.v14spli02.12

INTRODUCTION

The stock market broadly refers to the group of exchanges where the buying, selling, and issuance of shares of publicly traded companies take place. While both the terms “stock market” and “stock exchange” is often used but the meaning is same, the later term generally comprises a subset of the former. Trading in the stock marketmeans buyingor sellingthe shares of listed companies on exchange. A given country or region may have one or more exchanges comprising their stock market.Technical analysis is a trading analysis domainused to evaluate stock price movements using charts and identify trading opportunities in future by studying statistical trends collected from trading activity, like price movement and volume of stock transactions. Unlike fundamental analysis, which evaluate a company value based on business results such as sales and earnings, technical analysis focuses on the study of price and volume.

The paper mainly focuses on automating the process of technical analysis of stocks. Research will be carry through using the Python programming language on a Jupyter environment.

This is software based research which includes cutting edge technologies like data science, machine learning and data driven frameworks for building the price prediction system. There are various machine learning models available for prediction of time series data. LSTM has been used becauseof its ability to back propagation with feedback and LSTM cells allowthe data to be filtered with gates.

Corresponding Author : D.G. Bhalke, Department of Electronics and Telecommunication Engineering, Dr. D. Y. Patil Institute of Technology (DIT), Pune, India; e-mail : bhalkedg2000@gmail.com

How to cite this article : Bhalke, D.G., Bhingarde, D., Deshmukh, S., Dhere, D., (2022). Stock Price Prediction Using Long Short Term Memory . *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology,* Volume 14, Special Issue (2), 271-273.

Source of support : Nil

Conflict of interest : None

LITERATURE SURVEY

LSTM shows more accuracy than other sequential data machine learning models. LSTM also overcome the gradient weight loss problem in traditional recurrent neural network. Recurrent neural network (RNN) andLSTM has been used to deal with anticipated stock market [1].Stock forecasting or predictionhas been done using Deep Learning with LSTM. In survey

materials authorscompares the LSTM and other similar models. Author concluded that LSTM was able to make more accurate predictions on stock price movements compared to CART Model [2].In [3] authors proposed Recurrent Neural Network and Bi-directional LSTM for forecasting of the stock price. Authors did research by varying epochs, hidden algorithm layers and dense layers. In paper [4] authors proposed Long Short Term Memory machine learning algorithm for stock price prediction. Presented how LSTM cell works.Article [5] aims to build a model using recurrent neural network and LSTM to predict future stock market values. Paper shows effect of epochs in models compilation on the accuracy of the machine learning model.In [6] this research paper authors talked about comparison of various recurrent neural network models with Long Short Term. s. In comparisons with RTRL, BPTT, Recurrent Cascade-Correlation, Elman nets, and Neural Sequence Chunking, LSTM runs more successfully compared to these algorithms, and learns much faster. LSTM also solves complex, artificial long time tasks that have never been solved by previous recurrent network algorithms.

METHODOLOGY

The methodology for stock priceforecasting is shown in figure 1. It includes Testing and training part. First the data is trained using multi-layer perceptron, convolutional neural network, single-layer LSTM which is type of recurrent neural network, etc.

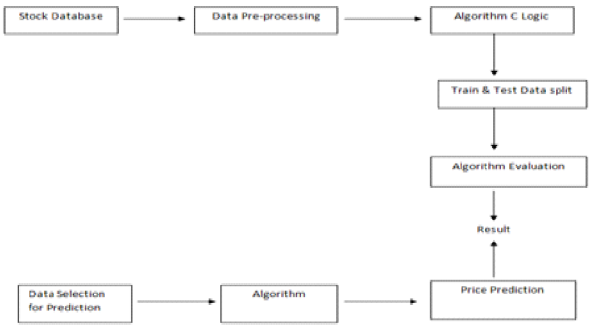


Figure 1: Block Diagram

Data Set

Various sources for historic stock prices are available. Most commonly used is from kaggle and yahoo finance. Kaggle data set has one drawback that is stock splits and bonuses are not optimised in price data, so its shows sharp price drop where such financial activities happed for particular stock. Yahoo finance data is optimised with stock splits and stock bonuses. Data can be download manually from website according to the time period you want. We have selected NIFTY 50 companies with time period from 1 January 2008 to 14 March 2022. Data file format is .csv file.

Data Pre-processing

In Yahoo finance data, as stock splits and stock bonuses are already optimised, we did data pre-processing for only null values. Null values / NAN cells removed from closing price column. Keeping NAN values generated error in metrics generation.

Parameters

We have chosen 'Closing Price' of the day as base parameter. Each day closing price is input for LSTM cell. We consider batch of 100 inputs to predict 1-day price which is 101th day. Adam optimizer is used and loss is calculated and showed in the form of mean squared error and root mean squared error.

```
model=Sequential()
model.add(LSTM(50,return_sequences=True,input_shape=(100,1)))
model.add(LSTM(50,return_sequences=True))
model.add(LSTM(50))
model.add(Dense(1))
model.compile(loss='mean_squared_error',optimizer='adam')
```

```
model.summary()
```

```
Model: "sequential"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
lstm (LSTM)                  (None, 100, 50)           10400
_________________________________________________________________
lstm_1 (LSTM)                (None, 100, 50)           20200
_________________________________________________________________
lstm_2 (LSTM)                (None, 50)                20200
_________________________________________________________________
dense (Dense)                (None, 1)                 51
=================================================================
Total params: 50,851
Trainable params: 50,851
Non-trainable params: 0
```

Figure 2: Model Summary

Performance Metrics

For testing the performance of algorithm we used RMSE (Root Mean Squared Error) for training data and predicted data.If model is good, then RMSE of test data is quite similar to train dataset. Otherwise following conditions exist.

RMSE of test > RMSE of train => OVER FITTING of the data.

RMSE of test < RMSE of train => UNDER FITTING of the data.

We tested 50 stocks, for most of the time our algorithm model over fitted the data. This happened because of the small size of the testing data set. Removing machine learning model layers reduces the over fitting of the model.

Long Short Term Memory (LSTM)

LSTM is a remarkable neural network structure with three 'Gate' structure. Each LSTM unit has three gates, they are called first input gate, second forgetting gate and last one output gate. When information is given to thethe LSTM's network, it can be passed forwardor forgotten by rules of the network. Information which is assured to the algorithm will be remembered, and the information that does not assured the algorithm will be forgotten through the forgetting gate. The speculative stock historicdataused for research in this paper is the actual historical data downloaded from the Internet from Yahoo finance website.

The precision of this LSTM model used in this project is around 50% to 60 %.

RESULT

We implemented sample algorithm on Bajaj Auto stock. Algorithm run successfully. In the figure 3 blue line shows the actual data while orange colour shows training data and green colour shows the testing output. Figure 4 shows the predicted output for month May 2021 which is shown in orange colour. As it already passed it can see the real time data in figure 5 where similar type of curve is present.

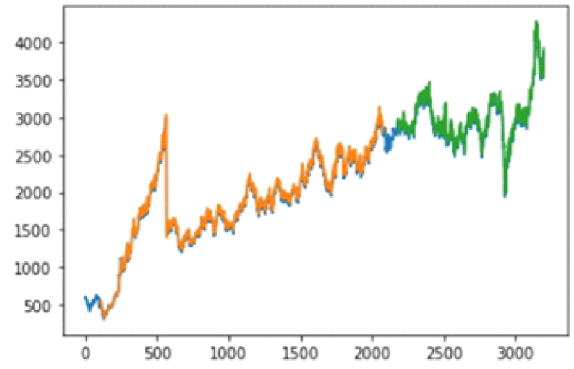


Figure 3: Days vs Price for Bajaj Auto

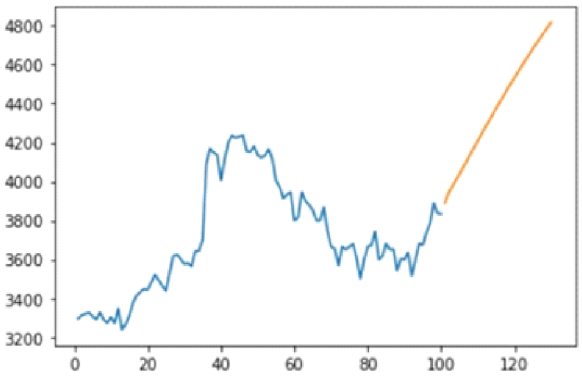


Figure 4: Days vs Price Prediction for May 2021

Figure 5: Real Time curve

CONCLUSION

The preferred algorithm grasp the raw set of data from the dataset or the .csv file and processes it. The cleaning of data is done and then further processed to gain the effective outcomes. After the computational mean the output is displayed in the screen in the form of graph.Long Short Term Memory can be successfully implemented over short period of the time to predict the stock price. As prediction period increases accuracy of the predicted value mismatch with the actual data.

REFERENCES

[1] Dr. KarunakarPothuganti "Long Short Term Memory (LSTM) Algorithm Based Prediction of Stock Market Exchange", International Journal of Research Publication and Reviews, Volume 2, Issue 1, ISSN 2582-7421, page 90-93.

[2] Carol, Leran Chen "Stock Prediction Using Deep Learning with Long-Short-Term-Memory Networks", International Journal of Electronic Engineering and Computer Science, Vol. 5, No. 3, 2020, pp. 22-32

[3] M. A. Istiake Sunny, M. M. S. Maswood and A. G. Alharbi, "Deep Learning-Based Stock Price Prediction Using LSTM and Bi-Directional LSTM Model," *2020 2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES)*, 2020, pp. 87-92, doi: 10.1109/NILES50944.2020.9257950.

[4] MallikarjunShastri Pm "Stock Price Prediction Using LSTM" , Test Engineering and Management · January 2021, ISSN: 0193-4120 Page No. 5246-5251, The Mattingley Publishing Co., Inc.

[5] Adil, Mhamed "Stock Market Prediction Using LSTM Recurrent Neural Network", International Workshop on Statistical Methods and Artificial Intelligence (IWSMAI 2020) April 6-9, 2020

[6] SeppHochreiter "Long Short Term Memory", Neural Computation available: Dec. 1997, Neural computation 9(8):1735-80, DOI: 10.1162/neco.1997.9.8.1735

RESEARCH ARTICLE

SAMRIDDHI Volume 14, Special Issue 2, 2022 Print ISSN : 2229-7111 Online ISSN : 2454-5767

Contribution of Multiprotocol Label Switching Traffic Engineering in Throughput Enhancement

M. M. Swami[1*], D. P. Gaikwad[2], S. S. Kolte[3], M. M.Phadatare[4]

[1*-4] Department of Computer Engineering, AISSMS College of Engineering, Pune, India; e-mail*: mmswami@aissmscoe.com

ABSTRACT

Multiprotocol Label Switching traffic engineering offers competency to all types of service providers including mobile,internet. Service provider should provide highly stable and seamless connections over the globe for customers connected to network. This paper describes designing of Multiprotocol Label Switching along with traffic engineering with the help of Interior Gateway Protocol. Multiprotocol Label Switchingtraffic engineering also assures path, link and node protection functionality along with router reflector features which always ensure better efficiency and easy administration. The efficient use of available resources in internet service provider infrastructures is one of the key requirement to meet today's highly demanding business which can be possible with the help of Multiprotocol Label Switchingtraffic engineering. In this paper, one of solution has been demonstrated to mitigate subjected the requirement.

Keywords: MPLS, IGP, Traffic Engineering, OSPF, RSVP, IS-IS

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, (2022); DOI : 10.18090/samriddhi.v14spli02.13

INTRODUCTION

The India being highly potential market for cellular business technology need to provide user service which is enabled with high speed & capacity. Todays, cellular network is not onlylooking for connectivity but also looking for seamless roaming capability & stable network availability across the globe. Cellular network is not limited to voice or data calls but also for providing end to end connectivity to all types for business traffic. For every business; technology is one the critical part & in that seamless & stable connectivity plays a vital role.Downtime in a cellular network has adverse effect on all part of business which in-turn affect human life. Due to this its mandate that cellular network should function precisely.

In cellular network any activity or changes in one part of network may impact the other part may in positive or negative impact but network being contiguous in nature this can be taken as an advantage provided that activity should be carried out with all critical measures so that overall network should remain stable & customer traffic should remain intact.

Corresponding Author : M. M. Swami, Department of Computer Engineering, AISSMS College of Engineering, Pune, India; e-mail : mmswami@aissmscoe.com

How to cite this article : Swami, M.M., Gaikwad, D.P., Kolte, S.S., Phadatare, M.M. (2022). Contribution of Multiprotocol Label Switching Traffic Engineering in Throughput Enhancement.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, Volume 14, Special Issue (2), 274-279.

Source of support : Nil

Conflict of interest : None

RELATED WORK

MPLS techniques can be applied to any network layer protocol. However, we focus on the use of IP as the network layer protocol [3]. It is a forwarding technology employed by most modern ISPs. It operates between Layer 2 and 3-a layer that is commonly known as 'Layer 2.5'- in the OSI model. This is because it enables IP traffic to be forwarded on Layer 2 devices such as ATM (Asynchronous Transfer Mode) and frame-relay switches as well as on Layer 3 devices such as routers

IGP (InteriorGateway Protocol)

These protocols are explored within an Autonomous System (AS). IGP's are playing vital roles in finding best routes within AS.Few IGPs are described in brief below:

OSPF (Open shortest path first)

In the Interior Gateway Protocol (IGP) family OSPF which is Link State protocol is the most famous protocol. It is developed by the OSPF working group of the IETF in 1980.

OSPF has below few key features

- OSPF uses IP multicast to send link-state updates. This ensures less processing on routers that are not listening to OSPF packets. Also, updates are only sent in case routing changes occur instead of periodically. This ensures a better use of bandwidth.
- OSPF allows for better load balancing.
- OSPF allows for a logical definition of networks where routers can be divided into areas. This limits the explosion of link state updates over the whole network. This also provides a mechanism for aggregating routes and cutting down on the unnecessary propagation of subnet information.
- OSPF allows for routing authentication by using different methods of password authentication.
- OSPF allows for the transfer and tagging of external routes injected into an Autonomous System. This keeps track of external routes injected by exterior protocols such as BGP

By using OSPF hierarchy and different areas for different part of network , cellular network will get advantage as below:

- Network Scalability
- Reduced frequency of SPF calculations
- Smaller routing tables

ISIS (Intermediate System to Intermediate System)

ISIS Protocol (Intermediate System to Intermediate System Protocol) is a Link-State routing protocol that is developed by ANSI ISO. It is an open standard and classless Interior Gateway Protocol (IGP). IS-IS Protocol uses Dijkstra SPF (Shortest Path First) algorithm like OSPF, to build the IS-IS Protocol databases and calculate the best path. It uses Cost value at the best path calculation. ISIS Protocol is a stable protocol and it has a very fast convergence. It has also large scalability that IS-IS Protocol is a very good protocol for Service Providers and large enterprises. IS-IS Protocol is also a very good protocol used with MPLS-TE. Dynamic Link-State protocol IS-IS Protocol is designed to use in CLNS (Connectionless Network Service).

IS-IS Protocol is a Hierarchical routing protocol like OSPF. IS-IS network is also consisting of small Areas connected to the Backbone. So like OSPF, IS-IS Protocol has also two hierarchical levels:

Level 1 (Areas)

Level 2 (Backbone)

With IS-IS, an individual router is in only one area, and the border between areas is on the link that connects two routers that are in different areas. IS-IS has a two-level hierarchy. Contiguous Level 2-capable routers form the backbone. Both Level 2 and Level 1 routers live in areas. Routers can be Level 1 (L1), Level 2 (L2), or both (L1/L2). A Level 2 router may have neighbors in the same or in different areas, and it has a Level 2 link-state database with all information for inter-area routing. By default, all Cisco IS-IS routers are level 1/level 2 routers which enables them to carry both L1 and L2 link state databases. The type of link-state information exchanged between 2 IS-IS routers is dependent on the adjacency type formed. L1 adjacency routers exchange L1 link-state information. L2 adjacency routers exchange L2 link-state information. L1/2 adjacency routers can exchange both L1 and L2 link-state information.

Need of Traffic Engineering

In the IP network, path chosen by IGP is always the shortest path, because of which some of paths remains unused which intern creates a situation where bandwidth utilization is not up to the mark. To explore all available network path MPLS TE plays very important role in cellular or ISP network. MPLS TE uses RSVP (resource reservation protocol) for the same.

RSVP is a signaling protocol that reserves resources, such as for IP unicast and multicast flows, and requests quality-of-service (QoS) parameters for applications. The protocol was extended in MPLS RSVP TE to enable RSVP to set up label switched paths (LSPs) that can be used for TE in MPLS networks. RSVP interacts with TE to support the MPLS TE functionality. The TE process contains the following functionalities:

- End-point control, which is associated with establishing and managing TE tunnels at the headend and tail-end.Link-management, which manages link resources to do resource-aware routing of TE LSPs and to program MPLS labels.

- Fast Reroute (FRR), which manages the LSPs that need protection and to assign backup tunnel information to these LSPs. When a router's link or neighboring node fails, the router often detects this failure by receiving an interface down notification.

RSVP establishes backup LSP-based tunnels for the local repair of TE LSPs. RSVP uses the facility backup method in which a PLR creates one or more bypass tunnels that can be used to protect multiple LSPs.

Table-1: RSVP Protocol Characteristics

RSVP Protocol characteristics	Description
RSVP	Yes
Authentication	No
Tunnel Characteristics	
Secondary Paths	Yes with Path Option and pre-signaled
Administrative Groups	No
Traffic Protection - Fast Reroute	Yes
Bidirectional Forwarding Detection (BFD)	No
Explicit Path	Yes with Path Option
QoS marking and honoring	Yes

SIMULATION SOFTWARE

There are many software'savailable for simulation like GNS3, EVE-NG. For the simulation of above network topology, EVE-NGis used. EVE-NG (Emulated Virtual Environment- Next Generation) is a new version of Unetlab 2.0 after Unetlab 1.0. The name has been changed and the original name is Unified Networking Lab.

EVE-NG covers Dynamips, IOL, and QEMU. These three components complete the virtualization of all devices on the EVE-NG platform and are the core of the EVE-NG platform. EVE-NG can run many network device operating systems such as Cisco, Juniper, F5, Fortinet, H3C, Huawei, Palo Alto, Check Point, etc. It can run Windows, Ubuntu, CentOS, MacOS and other host operating systems, as well as VMware, Open Stack, Proxmox VE Citrix, KVM, QEMU, Docker and other virtualization environments/cloud computing operating systems.This software not only been explored for certification like CCNA,CCNP,CCIE but also has been exclusively getting used in industry for simulation almost all new emerging technologies.

EXPERIMENTAL SETUP

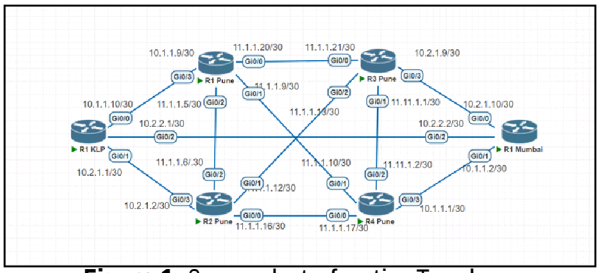


Figure 1: Screenshot of entire Topology

In this paper above topology has been explored to highlight impact of traffic engineering in cellular as well as in data network. Here in this topology the connectivity between provider edge (PE) nodes named as Mumbai & Kolhapur thru provider network placed at Pune at 4 points R1, R2, R3 and R4 is shown. All links are considered to be geared with 100 Gig bandwidth as its telecom or ISP network's backbone. All WAN links are provisioned with /30 IP address as showed above.

```
interface GigabitEthernet0/0
 no shutdown
 description link to PuneR1
 ip address 10.1.1.10 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
 mpls traffic-eng tunnels
 mpls ip
!
interface GigabitEthernet0/1
 no shutdown
 description link to PuneR2
 ip address 10.2.1.1 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
 mpls traffic-eng tunnels
 mpls ip
```

Figure 2: KLP Node physical Interface Configuration

```
!
interface GigabitEthernet0/0
 no shutdown
 description link to Pune R3
 ip address 10.2.1.10 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
 mpls traffic-eng tunnels
 mpls ip
!
interface GigabitEthernet0/1
 no shutdown
 description link to Pune R4
 ip address 10.1.1.2 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
 mpls traffic-eng tunnels
 mpls ip
!
```

Figure 3: MUM Node physical Interface Configuration

Figure 2 and Figure 3 depicts the Configuration of physical interface at PE nodes i.e. at Kolhapur & Mumbai end. Also these interfaces are resourced with two key commands to assure below key deliverables.

1. **Mpls traffic-engineering tunnels :** This command is explored for pulling these interface in MPLS traffic engineering
2. **Mplsip :** This command is assuring Lable distribution protocol (LDP) to its directly connected neighbor. LDP is used to exchange MPLS lable in ISP backbone network.

```
!
interface Loopback0
 no shutdown
 ip address 2.2.2.2 255.255.255.255
!
```

Figure 4: KLP Loopback Configuration

```
!
interface Loopback0
 no shutdown
 ip address 1.1.1.1 255.255.255.255
!
```

Figure 5: MUM Loopback Configuration

This is show run output of loopback interface of Kolhapur & Mumbai nodes/routers. Its highly recommended that loopback interface should be configured on all nodes though the network could be LAN or WAN. The loopback interface being logical interface which always remains up & due to this in telecom network this interface in used for exchange of BGP routes.

```
!
interface Tunnel20
 no shutdown
 description Tunnel to KLP
 ip unnumbered Loopback0
 mpls ip
 tunnel source Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 2.2.2.2
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 explicit name MUM-KLP
 tunnel mpls traffic-eng path-option 2 explicit name MUM-KLP-VIA-PUN-R3-R1
 tunnel mpls traffic-eng path-option 3 explicit name MUM-KLP-VIA-PUN-R4-R2
 no routing dynamic
!
```

Figure 6: Traffic Engineering Tunnel at Mumbai

```
!
interface Tunnel10
 no shutdown
 description Tunnel to Mumbai
 ip unnumbered Loopback0
 tunnel source Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 1.1.1.1
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 explicit name KLP-MUM
 tunnel mpls traffic-eng path-option 2 explicit name KLP-MUM-VIA-PUNR1
 tunnel mpls traffic-eng path-option 3 explicit name KLP-MUM-VIA-PUNR2
 no routing dynamic
!
```

Figure 7: Traffic Engineering Tunnel at Kolhapur

Above is the one of key Configuration where traffic engineering tunnel resourced for below merits.

1. Tunnel is sourced with loopback 0 interface (this is logical interface and will always remain logically up)
2. Here it is made sure that tunnel is equipped with 3 paths minimum
3. Tunnel mode defined as mpls traffic engineering exclusively.
4. To assure IGP should take tunnel interface in account while performing SPF route calculation auto route command has been deployed in tunnel Configuration.

```
router ospf 10
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 network 0.0.0.0 255.255.255.255 area 0
!
```

Figure 8: IGP Configuration at MUM & KLP

This above fig shows IGP Configuration which has been explored at KLP & Mumbai nodes.Basic purpose of IGP is to give IPV4 reachability between all PE & P nodes. Here OSPF is used as IGP. Here also loopback 0 interface has been deployed to exchange LSA's between PEs & Ps.

To integrate traffic engineering with IGP, "mpls traffic-engineering area 0" has been used.This being simulation version, all IPV4 network has been announced in IGP.

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor ibgp peer-group
 neighbor INTERNAL peer-group
 neighbor INTERNAL remote-as 100
 neighbor INTERNAL update-source Loopback0
 neighbor 2.2.2.2 peer-group INTERNAL
 neighbor 1.1.1.1 peer-group INTERNAL
 !
 address-family ipv4
  neighbor INTERNAL route-reflector-client
  neighbor INTERNAL next-hop-self
  neighbor 2.2.2.2 activate
  neighbor 1.1.1.1 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor INTERNAL send-community both
  neighbor 2.2.2.2 activate
  neighbor 1.1.1.1 activate
 exit-address-family
 !
```

Figure 9: MPiBGP& Route reflector configuration at Pune R1 & R2

IBGP Configuration is deployed along with group Configuration which is highly recommended to ease the BGP administration. At P nodes Route reflector has been enabled & this is one of key Configuration in telecom network. Purpose of route reflector is to reflect best routes to his all peers & avoid bulky IBGP Configuration at PE nodes. At PE nodes only one IBGP peer with these RR nodes need to enable & post to which all PE nodes are able to exchange their IPV4 & VPNV4 routes with each other as best route information will be served by this RR. At RR, IPV4 & VPV4 both address family has been defined to assure IPV4 & VPNV4 route exchange.

MP-iBGP Configuration At Mumbai & KLP End pointing to Pune R1 (Loopback IP 11.11.11.11) & Pune R2(Loopback IP 33.33.33.33)

```
router bgp 100
 bgp log-neighbor-changes
 neighbor 11.11.11.11 remote-as 100
 neighbor 11.11.11.11 update-source Loopback0
 neighbor 33.33.33.33 remote-as 100
 neighbor 33.33.33.33 update-source Loopback0
 !
 address-family vpnv4
  neighbor 11.11.11.11 activate
  neighbor 11.11.11.11 send-community both
  neighbor 22.22.22.22 activate
  neighbor 22.22.22.22 send-community both
 exit-address-family
```

Figure10: MPiBGP Configuration at Kolhapur and Mumbai

Here at PE nodes only IBGP peering with RR need to enabled to assure IPV4 & VPNV4 route exchange between all PEs & in-turn this will assure end-end reachability

Results And Discussions

Packet Size Vs Latency Vs Throughput

Below Table-1 is the one of key take-way of traffic engineeringtunnel. It shows overall impact of latency on network throughput. In telecom network due to traffic engineering features network is leveraged with multiple paths & different priorities due to which its assuring efficient use of available resource. In this table latency is calculated from sending five packets from KLP-Mumbai over direct path and over indirect path which is via Pune.Please note formula used to calculate throughput. TCP-Window-Size-in-bits / Latency-in-seconds = Bits per mili-second-throughput

Table-2: Throughput analysis

Packet Size in bits	Latency in ms	Path	Throughput in Bits-per-seconds
100	6	Direct (Mumbai-KLP)	17
100	8	Indirect (Mumbai-Pune-KLP)	13
200	6	Direct (Mumbai-KLP)	33
200	8	Indirect (Mumbai-Pune-KLP)	25
300	6	Direct (Mumbai-KLP)	50
300	8	Indirect (Mumbai-Pune-KLP)	38

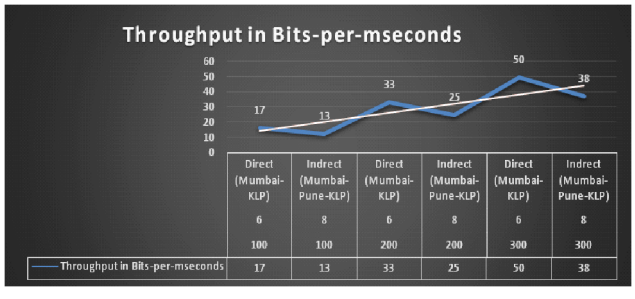


Figure 11: Graph for throughput in Bits per mili-seconds

Conclusions

Service provider point of view Traffic engineering is crucial and Internet service provider (ISP) backbones. MPLS traffic engineering delivers an integrated method to traffic engineering. MPLS traffic engineering features allow an MPLS backbone to replicate and expand upon the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks. In this paper we have simulated and proved that even though network has been subjected to handle different size of packets /traffic which is today's minimum expectations from network, Multiprotocol Label Switching traffic engineering assures the overall increasingthroughput while keeping efficient use of network resources.

References

[1] https://www.sciencedirect.com/topics/computer-science/interior-gateway-protocol

[2] Iversen, V.B., "Traffic Engineering of Cellular Mobile Communication Systems", ITC Regional Seminar in Bangkok, November 28 – December 1, 1995. 10 pp.

[3] https://datatracker.ietf.org/doc/rfc3031/

[4] S. Adibi; M. Naserian; S. Erfani , "Mobile-IP MPLS-based networks", Canadian Conference on Electrical and Computer Engineering, 2005, ISSN: 0840-7789

[5] Omer Mahmoud; Othman Khalif; Ali Sellami; A. AishAbdallah Rashid, "Mobility support in MPLS network", 6th International Conference on Telecommunication Systems, Services, and Applications (TSSA), 2011

[6] SavinyaPolvichai; PrawitChumchu,"Mobile MPLS with route optimization: The proposed protocol and simulation study", Eighth International Joint Conference on Computer Science and Software Engineering (JCSSE),2011

[7] Gous, Alan, ArashAfrakhteh, and John Evans, "A Comparison of Approaches for Traffic Engineering in IP and MPLS Networks."arXiv preprint arXiv: 1608.03770 (2016).

[8] Foteinos, Vassilis, et al. "Operator-friendly traffic engineering in IP/MPLS core networks." IEEE Transactions on Network and Service Management 11.3 (2014): 333-349.

[9] Shruthi Hiranmayi Sridhar, J. Arunnehru, "Traffic Engineering: An Application of MPLS L3 VPN

Technology", 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018).

[10] Khan, Mohsin, "MPLS Traffic Engineering in ISP Network." International Journal of Computer Applications 59.4 (2012).

[11] Wei, Luo. Layer 2 VPN architectures.Pearson Education India, 2008.

[12] Xiao, Xipeng, et al. "Traffic Engineering with MPLS in the Internet", IEEE network 14.2 (2000): 28-33.

[13] Awduche, Daniel O. "MPLS and traffic engineering in IP networks.", IEEE communications Magazine 37.12 (1999): 42-47.

RESEARCH ARTICLE

SAMRIDDHI Volume 14, Special Issue 2, 2022 Print ISSN : 2229-7111 Online ISSN : 2454-5767

Investigation of Adjustable Radial Basis Function estimations for Non-Linear System

Aabid C Mulla[1*], Sudarshan L. Chavan [2], Kushal Lodha[3],Sandeep S Gaikwad[4], Rahul Ankushe[5], Vijay Mohale[6]

[1*,2-5] Department of of Electrical Engineering, JSPM's Rajarshi Shahu College of Engg.,Pune, India; e-mail*: mullaaabid1234@gmail.com*

[6] Department of of Electrical Engineering, WCE , Sangli, India.

ABSTRACT

This paper gives idea about design method for adaptive neural controller is proposed and it is applied to the non-linear system Continuous stirred tank reactor CSTR. The investigating controller used in this paper is designed in tuned with adaptive process. To analyze the performance of effect of foot print of uncertainty on the controllers' performance two various types of algorithms namely state feedback control and observer based control are used Radial basis function Neural network is utilized for approximation of the nonlinear function . Software validation result of suggested method is discussed below.

Keywords : Adaptive neural network (ANN), CSTR, Radial basis function (RBFNN).

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, (2022); DOI : 10.18090/samriddhi.v14spli02.14

INTRODUCTION

It is a well-known that conventional PID controllers are the most common controllers used in industry because of their simple structure and low price [1].The application of PID controllers in controlling linear system might be an effective way to achieve desired performance, but when the process model is uncertain or the process is non-linear, PID controllers might not achieve better result.

In the few years back, research of advance control algorithms is mostly depends on modernized and typical control algorithms. A modernized control algorithm contains adaptive and optimal control. Advanced control strategy such as adjustable and finest control and typical control algorithm is depends on the parameterization of system. As per utilization view, mathematical modeling is prior necessary. Robust control of nonlinear system is important topic in control system in both of the manners i.e. theoretically and practically, it gives impressive performance in previous few years. It has been specified in [3].Basically; it contains two main disadvantages of unpredictability in the nonlinear system. The initial one is the matching condition [4] and to control such type of the system some methods are proposed [5]. Final one is triangularity assumption. Various analytical approaches are utilized to limit the unpredictability system with conflict unpredictability [6]. In view of conflict unpredictability is demanding problem because it gives effect on the system behavior adversely. Some of the real applications can be seen in [7]. In these few years, acceptable contribution is has done to develop conflict control systems with zero consideration over unpredictability [8].

Furthermore RBFNN is implemented many times for practical applications due to nice approximation.

Corresponding Author : Aabid C Mulla, Department of of Electrical Engineering, JSPM's Rajarshi Shahu College of Engg., Pune, India; e-mail : mullaaabid1234@gmail.com

How to cite this article : Mulla, A.C., Chavan, S.L., Lodha, K., Gaikwad, S.S., Ankushe, R., Mohale, V. (2022). Investigation of Adjustable Radial Basis Function estimations for Non-Linear System.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, Volume 14, Special Issue (2), 280-283.

Source of support : Nil

Conflict of interest : None

properties and simple structure. RBF neural network is now addressed few decades early but it is now growing technique due to its excellent specific solution and good analytical ability that removes unwanted and complex analytical steps in comparison with the multilevel feed forward network. Previous history of research also had proven that shown that any unpredictability functions over compact set with generalized performance can be examined by RBFNN. In the area of mathematical modeling, a RBFNN is an ANN Make use of radial basis functions as main functions. The response of the system is consecutive integration of radial basis function of the input and neural network variables.

Even though various techniques are available for limiting the unpredictable system, many of the last performances are analyzed with the consideration that state variables are used. If these states are not used, these performances are not authentic in real time world. In this paper two adaptive Equalizer investigators for unreliable system with unpredictability are discussed. The initial control design is depend upon the condition response and final one is depend upon the analyzed conditions.

1) These paper advances use of ANN for nonlinear system with unreliability.
2) An intelligent system is developed to find immeasurable condition for limiting reason.
3) By applying robust Simplifying parameters in limiting signal, the effects of generalized inaccuracy in neural network is removed.

PROBLEM ANALYSIS

Assume the following unpredictable network with unreliable instances.

$$\dot{x} = Ax + f(x) + Bu \quad (1)$$

Where

x = [x1 ... ... xz] Rp z is the track of system condition u = [u1 ... ... un] ∈p is the track of system inserts $f(x)$ = [f1(x) ... ... f n(x)]T R^m is the track of flat Unpredictable network with unreliable instance functions. In this paper, the Gaussian RBFNN is used to estimate a Unpredictable function h(.)s given as,

$$h(z) = \theta\, \xi(z) \quad (2)$$

here z is insert vector θ= [θ1.....θn] is the mass

Vector, I is the number of junctions, ξ = [ξ 1 ... ... ξ n] ∈ *Rm* is the basis function is selected as Gaussian functions. that the symbols in your equation have been

$$\xi i = \exp \frac{(-\| z - ui \|^2)}{ni} \quad (3)$$

Where μi = [μi1 ... ... μin] are the middle and breadth of Gaussian functions. By selecting sufficient junctions, Neural network can Estimate function h(.)

$$h(z) = \theta * \xi(z) + \delta \quad (4)$$

here δ is the estimation inaccuracy of Neural network. The minimal mass Vector θ^* is called as

$$\theta^* = \arg\min \{ |h(z) - h(z)| \}, \quad (5)$$

The set of (A, B) is tractable. This consideration satisfies that a gain matrix Kc present in such a way that the polynomial equation of *A-BKT* is Hurwitz. This assure for a given non-negative explicit matrix Q, there exists a non-negative explicit solution P for given polynomial equation is

$$(A - BK\,C\,T)P + (A0 - BK\,C\,T) + Q = 0 \quad (6)$$

CONDITION RESPONSE EQUAILIZER MODELING:

In order to model condition response equalizer, the controllable insert is defined below

$$u = -K\,C\,Tx - u\,adp - u\,R - u\,d \quad (7)$$

Here *u adp* is an adjustable bit to recompense the cause of mismatched unpredictability. Additionally to this, *uR* and *ud* are modeled to recompense the cause of Neural Network estimation inaccuracy and outside noise, independently.

Now, let us declare the functions η *T* and g(x) and g(x) is given below,

$$\eta\, T(x) = xTPB \quad (8)$$

$$g(x) = \frac{xTPf(x)}{\eta \| (x) \|} \quad (9)$$

$$(x) = \theta\, (x) \quad (10)$$

The adequate variable track θ* is described below as

$$\theta^* = \text{argument minimum } \{\sup \| g(x) - g(x)^{\wedge} \|\} \quad (11)$$

Consider the Adjustable Neural control, where

$$uadp = (x)\, \theta\, (x) \quad (12)$$

$$u = k\, \eta\, (x) \quad (13)$$

$$ud = k\,(BTPx) \quad (14)$$

The adjustable law for renovate the determination line is

$$\theta = \gamma \| \eta \| (x) \quad (15)$$

OBSERVER BASED EQUAILIZER MODELLING

In a practical vigorous network, the condition of the network shall not accessible for analysis. In such cases, the performances in Section III are not suitable in real time & Neural Network based adjustable regulator using determined conditions is then necessary. Now, unpredictable nonlinear process

$$x = Ax + f(x) + B[u + d] \quad (16)$$

$$y = CTx \quad (17)$$

Where y are the quantifiable response of the system. The control aim is that the network conditions are changes by making use of ready response. Now the condition line x is Considered to be not measurable, it cannot be implemented in the regulator modeling... For some reason, a watcher must be modeled to approximate the not measurable conditions. In view to model observer based equalizer, the supervision process is defined below

$$u = - K C Tx- (x) \theta\varepsilon (x) - ua – uR– ud \quad (18)$$

$$ua=K0 \quad Px \quad (19)$$

$$uR = k1\eta(x) \quad (20)$$

$$ud = k2sgn (BTPx) \quad (21)$$

ua is a response of approximate conditions; *uR* and *ud* is the regulator to recompense NN estimation inaccuracy and outside noise, respectively. Figure 12 states about the conditions of the closed loop system and respective determined conditions. If you have a look in below Figure, both estimated condition and conditions are equalized by using the observer-based controller.

The adequate variable track θ^* is described below

$$\theta^*= mi\{|g(x) - g(x)|\} \quad (22)$$

Assume the adjustable neural regulator, where

$$uadp = \eta (x) \theta (x) \quad (23)$$

$$uR = k1\eta(x) \quad (24)$$

$$ud = k2s(BTPx) \quad (25)$$

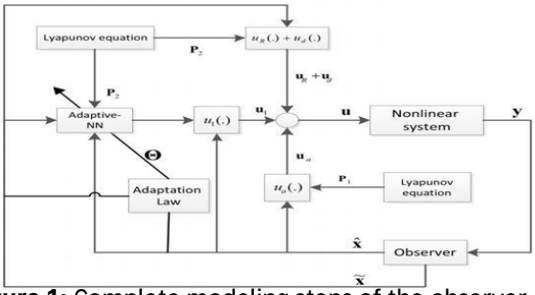


Figure 1: Complete modeling steps of the observer-based adjustable neural equalizer for unpredictable mismatch network

SOFTWARE SOFTWARE RESULTS

In this part, the software simulation analysis is done to understand the capabilities of the suggested adjustable neural regulator. Two different occurrences are analyzed to determine the performance of suggested control algorithm. Additionally, both condition and observer-based regulator are discussed for each situation.

Condition-Response Modeling

The system assumed here is a Solo raw data unpredictable network getting by inserting non-linear unreliable parameters to network discussed in [28]. The final network is described in below equations:

$$A = \begin{bmatrix} 1.33 & -0.33 \\ 1 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$f(x)= \quad -1.25x1(t)+0.072(1-x1(t))$$

$$\quad -1.55x1(t)+0.576(1-x1(t))$$

The aim is to determine equalization of this system with the condition-response equalizer suggested put forward in this research work. The Planned variables of condition-response equalizer mentioned below

K_C^T= 2.61 0.09.

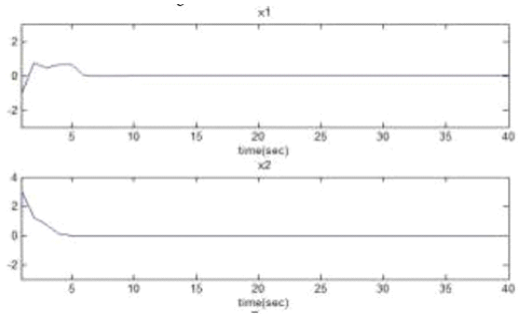


Figure 2: Condition curves of the system based on condition response adjustable-Neural network controller

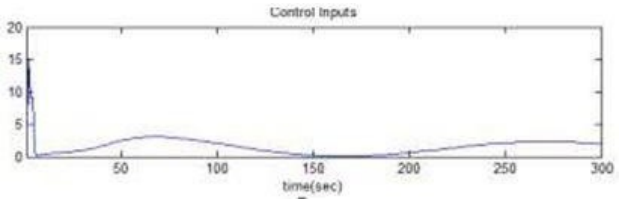


Figure 3: Command insert of the network, based on condition response adjustable - Neural network controller

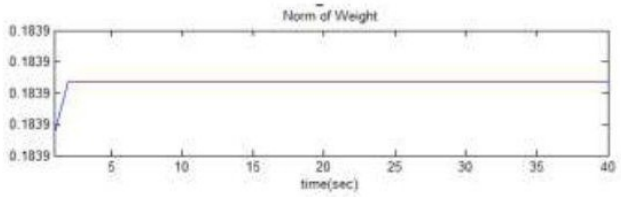


Figure 4: Norms of magnitude of Neural network Observer-Based balanced Modeling

This section is considered condition line x is never analyzed. Consequently, a observer is to be modeled for the determination of the not analyzed conditions. Assume the system with the variables. Consider the output matrix CT is given as follows.

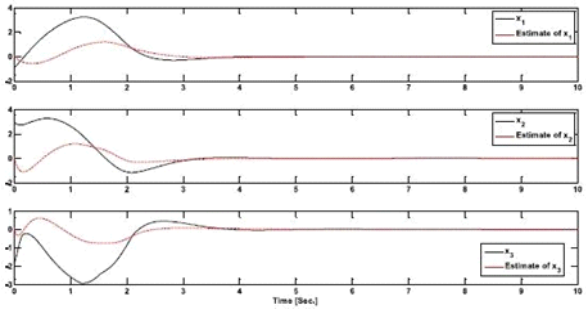


Figure 5: Real conditions and determined conditions of the closed-loop system

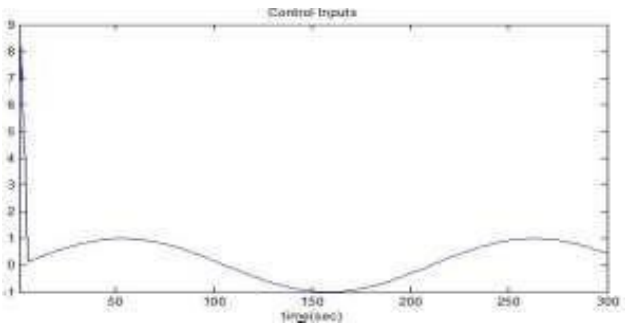


Figure 6: Command wave for network based on Watcher-based adjustable-NN controller

CONCLUSION

Two condition response and Watcher-based adjustable Neural network regulator for equalization of unpredictable network with non-linear unreliability is discussed. It proves that the symptomless convergent of the closed-loop network to null is obtained by keeping border conditions. The suggested control strategy tackles both conditions with p d" 2q and p > 2q, here p & q is count of network conditions and command inserts, appropriately. Software Simulation performance proven the reliability of the suggested strategy in the equalization of unpredictable network with non-linear unreliability.

Future scope contains actual real time practical implementation on hardware system.

REFERENCES

[1] Jianhui Lu;Fan Luo;Yujia Wang;Mingxin Hou;Hui Guo, "Observer-based Fault Tolerant Control for a class of Nonlinear Systems via Filter and Neural Network" *in IEEE Access, 2021.*

[2] Asmaa Swief;Amr, El-Zawawi; Mohamed, El-Habrouk;Amr Nasr Eldin, "Approximate Neural Network Model for Adaptive Model Predictive Control" *2020 16th International Computer Engineering Conference (ICENCO)*.

[3] Mohammad M. Arefi, Mohammad R. JahedMotlagh, Hamid R. Karimi., ¯Robust output tracking of nonlinear systems with mismatched uncertainties", *Proceeding of the 11th World Congress on Intelligent Control and Automation, 2014.*

[4] Nassira Zerari;Mohamed Chemachema;Najib Essounbouli, "Neural network based adaptive tracking control for pure feedback non-linear system with input saturation*"IEEE/CAA Journal of Automatica Sinica,2019.*

[5] Duidi Wu;Bo Long;Yaozong Cheng,"RBF-NN based Upper-bound Adaptive learning Sliding Mode Control for Grid-Connected Converter, *2020 IEEE International Conference on Mechatronics and Automation (ICMA).*

[6] Sudeep Sharma;Prabin Kumar Padhy"Discrete transfer function modeling of non-linear systems using neural networks, *2019 Fifth International Conference on Image Information Processing (ICIIP)*

[7] JagannathanS, LewisFL (1994) Discrete-time neural network controller with guaranteed performance. *In: Proceedings of the American control conference*..

RESEARCH ARTICLE

SAMRIDDHI Volume 14, Special Issue 2, 2022 Print ISSN : 2229-7111 Online ISSN : 2454-5767

Growth of Individualizing Web Services using APIs: REST and SOAP

Abhijit Banubakode[1*], Priya Chore[2]

[1*,2] MET Institute of Computer Science, Mumbai, India; e-mail*: abhijitsiu@gmail.com

ABSTRACT

Web Services are a collection of open protocols and standards that enable clients and servers to connect with one another. It allows various programmes to communicate with one another. Representational State Transfer (REST) and Simple Object Access Protocol (SOAP) are the two most extensively utilized web services today (SOAP). REST is an architectural approach, whereas SOAP is an underlying protocol. Both services are used to manage internet communication (www). Both services have advantages and downsides, and it is up to the web developer to decide which the better option is for their purposes. The purpose of this research is to construct a REST API and a SOAP API, respectively, using JAX-RS and JAX-WS, and to compare the two APIs.

Keywords: Postman, Protocol, REST, SOAP, Tomcat, Web Service.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, (2022); DOI : 10.18090/samriddhi.v14spli02.15

INTRODUCTION

A web service is a client-server programme that allows numerous programmes to communicate with each other via the internet. Because XML can be used to encrypt all data, it's a type of server or programme that sends XML messages in a standard format via the Internet. TCP/IP, HTTP, Java, HTML, and XML can all be used to create it. It allows for interoperability across different apps as well as language freedom. It is a networked software object that provides services through the Internet. The virtual representation of a web service is shown in Figure 1. A web service receives a client's request and responds to the client's applications. SOAP, WSDL, and UDDI are the three main components of web services. SOAP (Simple Object Access Protocol) is an XML-based protocol.

It can communicate using the CORBA, SOAP, and Java RMI protocols. The use of a web service allows you to discover the functionality of code over the internet. There are primarily two types of web services: REST and SOAP. REST is a web service development architectural style. The client submits a request to the server, which the server responds to using resources. Nouns and verbs make up the REST language. Despite the fact that REST web services are not protocol-agnostic, almost every REST service uses HTTP verbs to govern resource activities. Resources include videos, web pages, photographs, and anything else that can be allowed in a computer-based system. There are no limitations to what you can do with REST.

Both services are excellent for communication, but there is a distinction between them. REST is an architectural style for constructing web services, whereas SOAP is a protocol. The Java APIs for REST and SOAP are JAX-RS and JAX-WS, respectively. In some

Corresponding Author : Abhijit Banubakode, MET Institute of Computer Science, Mumbai, India; e-mail : abhijitsiu@gmail.com

How to cite this article : Banubakode, A., Chore, P. (2022). Growth of Individualizing Web Services using APIs: REST and SOAP.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, Volume 14, Special Issue (2), 284-290.

Source of support : Nil

Conflict of interest : None

areas of concern, both services have advantages and disadvantages. As a result, it is preferable to determine which service can be employed in particular case to achieve the best outcomes. The purpose of this research paper is to provide such a judgement between these two internet services based on our thorough investigation. The rest of the paper is organised as follows: The second section looks at the research that has been done in this area. In part III, the background research is briefly presented. In Section IV, we present our primary planned work. In section V, state-of-the-art parameters are used to compare REST and SOAP.

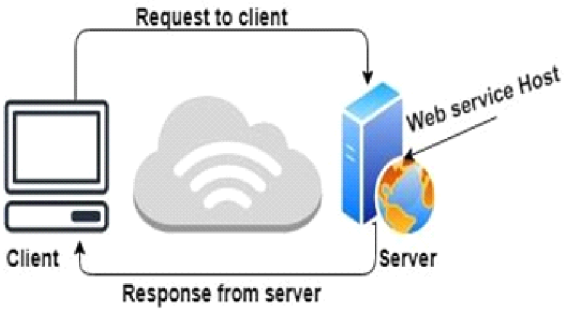


Figure 1: Virtual representation of web service

- Researching various web service requirements. In today's corporate environment, web-based apps are created using a variety of programming platforms. Angular JS, Node.js, and other frameworks are used in some apps, while others are created in Java. To work together, these diverse programmes almost always require some type of communication. It's tough to ensure accurate communication between them because they're written in different programming languages
- Web services have a role here. Web services provide a common framework for connecting several applications developed in different computer languages.

Associated Work

Chuangwei Zhang et al. [1] have developed a design for web services management that makes it easier, decreases system installation time, and increases efficiency. Paul Adamczyk [3] differentiates two architectural styles, REST and SOAP, and succinctly explains Restful web services as displaying four REST principles proposed by Roy Fielding, based on a study of current web services.

Chia Hung Kao et al. [4] describe and assess a REST- based web application testing framework. The software tester follows a consistent method for developing test cases and test scripts. The proposed framework cuts down on the amount of time and effort required to comprehend application design and implementation.

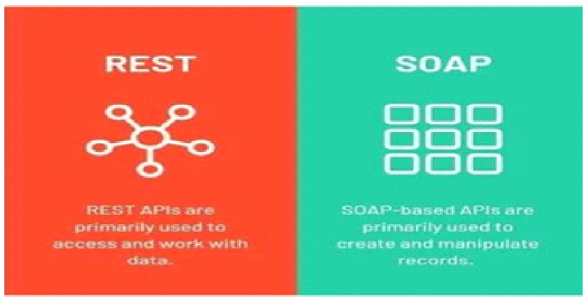
Florian Haupt et al. [5] provide a framework for REST API structural analysis that includes metrics and graphical API representations. They also convert the rest API description, which is available in a variety of languages, into a model that has been authorised and clearly illustrates the rest API design. to investigate the many types of RESTful Web Services.

Web services can be divided into two categories. Web services based on SOAP.

Web services that are Restful**.**

There are certain components that must be present in order for a web service to be fully functional. Regardless of the development language used to programme the web service, these components must be present.

Let's take a closer look at these elements.



Representational State Transfer (REST) was suggested by Roy Fielding in the year 2000 as a design methodology for the evolution of web services. It's a collection of rules designed to encourage people to use web services. In their PhD dissertation, Roy Fielding [2] lists seven limitations:

- **Start by using the NULL style**: It's a list of restrictions that hasn't been addressed yet. It lays the ground work for explaining REST.
- **Client-Server Architecture:** Client and server architectural styles are separated so that they can evolve independently. you may improve consumer interface flexibility and scalability by simplifying server components. Stateless:The customer and server ought to speak in a stateless way. The client's request will not be saved. A client request should not be recorded in a session or in a history. Resource allocation and management.
- **Cache:** Cache limitation is paired with client and server communication to increase network efficiency. This requirement specifies that the catchability (or non-catchability) of the response is expressed clearly

(or implicitly). The client must reuse the response in order for it to be cacheable. Client-side caching enhances performance, while server-side caching promotes scalability.

- **Uniform Interface:** The uniform Interface constraint distinguishes REST from other network styles. It simplifies and decouples the architecture, allowing it to evolve independently.

Assets identity, sources manipulation with the aid of representations, self-descriptive messages, and hypermedia because the engine of application country are the 4 interface regulations that have been diagnosed (HATEOAS).

- **Code-on-Demand:** REST functionality for downloading and executing code could be introduced. It allows the customer to restriction the quantity of functionalities that ought to be pre-implemented.

This constraint promotes the extensibility of the machine. API is a communication interface that allows two software programmes to communicate with each other. APIs are web services that use the HTTP protocol to communicate with one another (REST or SOAP). API interaction is defined as the sort of request and response sent between a client and a server. REST API refers to an API that builds web services using REST rules or standards. REST is not specified as an HTTP protocol, although it does adhere to limitations when designing APIs. REST leverages HTTP to define the desired action for requests and responses. There are several resource methods or request kinds that can be used to facilitate communication:

- **GET:** Get information about a resource.
- **POST:** The development of a new subordinate resource has been completed.
- **PUT:** There will be an upgrade to the present resource.
- **DELETE:** Remove any existing resources indicated by Request URI.

For Example,

POST /users: It create a user.

GET /users/ {id}: It retrieves the details of a user. GET /users: It retrieve the details of all users.

DELETE/users: It delete all users.

DELETE /users/ {id}: It delete a user.

GET/users/ {id}/posts/post_id: It retrieve the details of a specific post.

POST/ users/ {id}/posts: It create a post of the user.

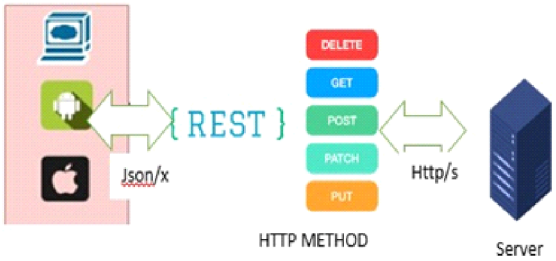


Figure 2: Represents REST API work flow following HTTP methods and return response to clients in JSON/XML format

The aforementioned HTTP techniques can be both safe and idempotent. Table-1 shows the features of idempotent and secure HTTP methods. Idempotent methods are HTTP methods that can be called several times without having any effect on the data stored, whereas safe these are HTTP methods that do not update the state of the server. These methods and resources are read-only.

Table-1: Characteristics of Http Methods

HTTP Method	Idempotent	Safe
GET	Yes	Yes
POST	No	NO
PUT	Yes	No
DELETE	Yes	No

SOAP Web Services API

The Simple Object Access Protocol (SOAP) is a network communication protocol that uses the XML messaging language. Service-Oriented Architecture (SOA) and SOA-related web services rely heavily on SOAP. Mentor, User Land Company, and Microsoft built it for the first time in 1998. In 1999, the initial version of the programme was released. The most recent version of SOAP is 1.2.

The service was enthusiastically utilised. SOAP's primary objective is to transport data across a network. It sent and received data over the internet via HTTP. The operations are started through SOAP messages. The SOAP service is also independent of platform and language.

Figure 3 depicts the format of a SOAP message sent between a server and a client.

- Envelope - A key component of the SOAP message format that identifies a document as SOAP and

determines the message format's start and end points. It is necessary for the SOAP message format to function.

- Header - This element provides optional information such as authorisation and verification information.
- Body - This is a required element that holds XML data. It comprises data that is sent to the programme, as well as request and response metadata.
- Fault - This element contains information about message transmission issues such as Version Mismatch, Client Fault (when the message was created incorrectly), and Server Fault (when there was a server difficulty). Errors and status data are also provided.

SOAP Binding is a transport layer mechanism for exchanging messages. Two SOAP communications requests with different binding styles are RPC (Remote Procedural Call) and Document Style.

- RPC - It's essentially a client-server request-and-response communication. Both the request and response formats are XML, with the message's general architecture determined by the root element Envelope. RPC used the representation and design of the message that was used for request and response. In RPC, synchronous communication occurs when a response is received before a message request is made. Because it is intended to deliver smaller messages, it is a simpler and less competent style.
- Document Style - It has a lot of substance and is also quite sophisticated. It's also mentioned.

In a SOAP request, two headers are defined: Content-Type and Content-Length. Content-Type is an example of a MIME type for message request and response, and character encoding is also provided for the XML body. The Content-Length header, on the other hand, indicates the number of bytes required in the request and response for the message body.

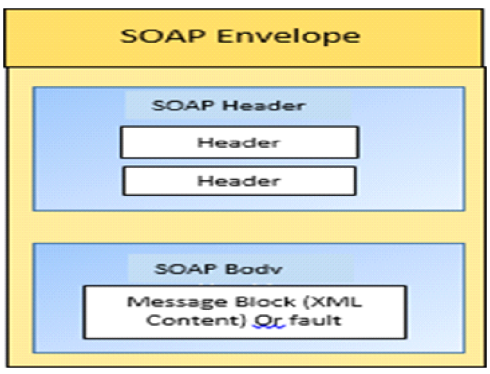


Figure 3: SOAP Messaging format

PROPOSED APPROACH

This study compares REST and SOAP web services in terms of response time, architecture, security, dependability, and efficiency, as well as their development and architectural styles. Also calculates which service is the best to choose depending on the criteria. It is also determined which service is the best appropriate for client-server communication. In a summary, this research article builds a REST API with JAX- RS and a SOAP API with JAX-WS, as well as additional visual aids, and tests them in Postman 7.1.1 to evaluate web service performance and response time.

Technologies used to create REST API with JAX-RS and SOAP with JAX-WS:

- Jersey version - 2.25
- JAX-WS - 2.1
- Apache Maven - 3.8.0
- Tomcat 7.0
- Eclipse Java IDE Mars 2.0
- Postman 7.7.1

Jersey [25] is a Java-based open source framework that supports JAX-RS APIs for constructing REST services. JAX-RS was created to enable the creation of RESTful web services in Java easier.

When creating a REST service with the URL Pattern "rest," as shown in Fig.4, these changes should be replicated in web.xml. Some of the JAX-RS annotations are listed in Table II. JAX- RS is a Java API that aids in the creation of Restful web services. It has annotations that export the java package javax.ws.rs, which makes creating web services easier.

Figure 4: Description of web.xml

SOAP with JAX-WS [26] with two styles: RPC style and Document Style (default) annotated with @SOAP Binding. As seen in Figure 5, @Web Service is utilized for interface implementation.

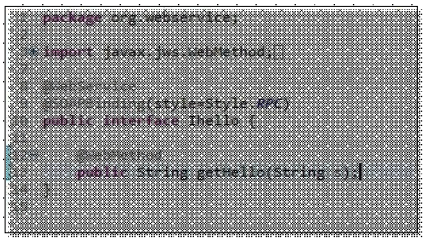


Figure 5: SOAP with JAX-WS

TABLE-2: JAX-RS Annotations

Annotations	Description
@Path	Specify the URI path
@GET	Annoate HTTP GET request method
@POST	Annotate HTTP POST request method
@DELETE	Annotate HTTP DELETE
@Path Param	Extract URI Path Parameters
@ Query Param	Extract URI Path Query Parameters
@ Products	Specify Media Type to be produced
@ Consumes	Specify Media Type to be produced by REST

Table-3 lists some of the JAX-WS annotations that make developing web services easier. The Java API for XML-based web services, primarily SOAP, is known as JAX-WS. It exports the javax.jws package, which contains Java to WSDL annotations. Javax.xml.ws is the basic JAX-WS package. The JAX-WS annotations are listed in Table -3.

Table-2: JAX-RS Annotations

Annotations	Description
@ WebService	Used for implementing web service over class or over an Interface.
@SOAPBinding	Specify SOAP Messaging Style
@Web Method	Only apply over a method specify web service operation
@Web Result	Specify how WSDL file looks.

These internet services are tested using Postman [27], an API testing tool. It's an API development tool for testing, building, and modifying APIs. HTTP requests can be made with Postman (GET, POST, PUT, and Patch). When an API request is performed, Postman may perform integration tests to confirm that APIs work as intended, as well as return response time and response size.

Figure 6 shows a flow chart illustrating the differences between REST and SOAP development techniques. We can infer that REST is less difficult to build than SOAP since REST uses HTTP methods that are easier to understand than SOAP WSDL files. Data is added using the SOAP standard, which uses an envelope style that makes the payload bigger when utilizing the SOAP service. REST, on the other hand, sends data without a payload through the URI Interface. As a result, REST is lighter and consumes less bandwidth than SOAP, which consumes more.

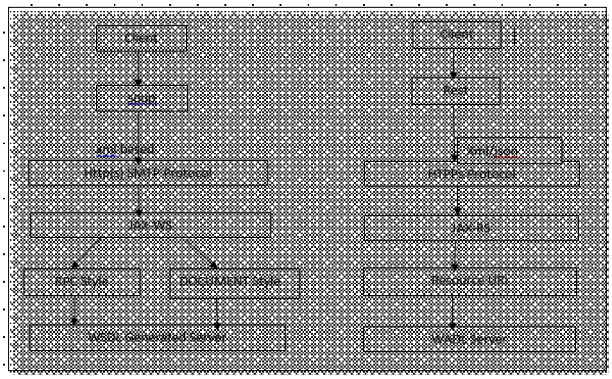


Figure 6: Flow chart of REST and SOAP

Process a big volume of credit card transactions in [7] real time - A large credit card corporation situated in the United States

Objective: Process billions of API calls in real time with a latency of less than 70 milliseconds.

Problem: The Company's current API management solution contributed 500ms of latency to every API call, resulting in a direct revenue loss.

When income is at stake, performance overcomes feature richness in API management systems.

Background Information and The Difficulty

A big credit card company was having problems with transaction delays. When paying with a credit card, most point-of-sale (POS) systems will time out once a specified limit has been reached. Cards will need to be processed again, however transactions will fail automatically to avoid the card from being charged twice.

At the same time, the company was moving to Open Banking standards, which provide API specifications that allow third- party developers and corporations to build applications and services based on customer-permissioned data and analytics, resulting in hundreds of billions of API calls.

As a result, the organization began looking for a scalable solution that could manage billions of API calls.

How real-time API management made a difference

The old API solution introduced 500ms of latency to each API call, causing a tiny proportion of transactions to fail. Even a modest percentage of billions of transactions, however, is a significant proportion, especially when money is lost. Users frequently try paying with a different credit card when a transaction fails. Millions of dollars could be lost due to timed-out API requests if the second card they use isn't issued by the same company as the first.

The firm pioneered a real-time API reference architecture to ensure API calls were executed as close to real-time as feasible. They created clusters of two or more high availability API gateways to improve the stability and resiliency of their APIs. The organization also chose to provide dynamic authentication by pre-providing authentication information (through API keys and JSON Web Tokens, or JWT), allowing for near-instantaneous authentication. Additionally, they chose to delegate authorization to their back end's business-logic layer, allowing their API gateways to concentrate entirely on authentication, resulting in faster call response times.

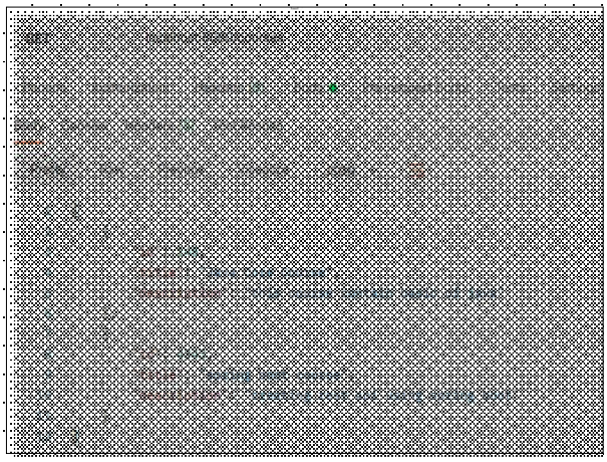
By using these best practices, the company was able to consistently achieve response times of less than 10 milliseconds, exceeding the performance criteria by 85 percent. This resulted in quick and measurable cost savings, allowing them to not only restore but also handle more transactions than previously. These speed gains were deemed more significant to the organization's business goals than some of the added features provided by the incumbent solution, such as a more robust developer site, API design tools, and API transformation capabilities.

The creation and consolidation of new revenue streams were also facilitated by improved transaction latency and dependability. As part of its open banking goals, the company may now make its core transactional engine available to ISVs and developers, allowing them to win more business by proving speed and reliability benefits over competitors.

IMPLEMENTATION, TESTING AND RESULT

Hear we implemented and tested rest API using spring boot:

Output:- When The GET Request Is perform. This is the client side output and we used postman to get the data post the data



FUTURE WORK

Several future work directions were identified that could build on the foundations. APIs are the foundation of online connectivity. They serve as a conduit for multiple applications, data, and devices to communicate with one another. Simply put, an API is a messenger that accepts requests, informs the system of what you want to do, and then returns the response to the user. For each API, documentation may create in future which includes specifications for how information is transferred between two systems. APIs can publicly interact with third-party applications. Finally, expanding an organization's business reach. So, when we book a ticket through Ticketnew.com, we include information about the movie we intend to watch.

Name of the Movie, Location, 3D/2D, Language.

These details are retrieved via API and then routed to servers associated with various movie theatres in order to return the aggregated response from multiple third-party servers. Giving the user the option of selecting the best theatre for them? This is how various applications interact with one another. And nowadays API is used all over word technology.

CONCLUSION

In our research work we conclude that REST is a type of data transfer that is based on the HTTP protocol's architecture. It enables you to send and retrieve data between two services using XML or JSON.It's usually a good idea to structure your web applications using RESTful architecture. This means that collections and resources can be easily identified and used to build a RESTful API. When developing an application that requires a Javascript-heavy front-end or integration with a smartphone app, a RESTful architecture is

required because it allows data to be transferred from the API to the client. It's often a good idea to plan out your RESTful collections and resources from the start.

REFERENCES

[1] C.Zhang and X.Yin, "Design and implementation of a single-service multifunction webservice," Nanjing, 2011 International Conference on Computer Science and Service System (CSSS), pp. 3912-3915.

[2] R.T.Fielding, DISSERTATION, 2000, "Architectural Styles and the Design of Network-based Software Architectures."

[3] P. Adamczyk, P.H. Smith, R.E. Johnson, and Munawar Hafiz, "REST and Web Services: In Theory and Practice," Springer Science+Business Media, 2011, DOI 10.1007/978-1-4419-8303-9 2.

[4] O'Reilly Media, "Designing Consistent RESTful Web Services Interface," ISBN: 978-1-449-31050-9.

[5] C.H.Kao, C.C.Lin, and J.Chen, "Performance Testing Framework for REST-basedWeb Applications," 13th

[6] International Conference on Quality Software, 2013, IEEE, DOI 10.1109/QSIC.2013.32, 2013. 6. F.Haupt, F.Leymann, A.Scherer, and K.Vukojevic-Haupt, "A Framework for the Structural Analysis of REST APIs," IEEE International

[7] Process billions of API calls in real time with a latency of less than 70 milliseconds.

RESEARCH ARTICLE

SAMRIDDHI Volume 14, Special Issue 2, 2022 Print ISSN : 2229-7111 Online ISSN : 2454-5767

Crop Disease Detection System Using Deep Learning Method

D. P. Gaikwad[1*], Akhilesh Sonone[2], Saket Patil[3], Supriya Limbole[4], Nishi Jain[5]

[1*-5] Department of Computer Engineering, AISSMS College of Engineering, Pune 411001; e-mail*: dp.g@rediffmail.com

ABSTRACT

Agriculture forms a crucial part of the economy of India. More than 50 percent of India's population is reliant on on agriculture for their income. India export many crops like wheat and other cereals. It can thus be seen that wheat is a big part of the Indian agricultural system and the economy of India. Therefore, it is very important to maintain the steady production of wheat and cereals. Planning for agriculture plays a major role in agro-based economy of country development and food security. In agricultural planning, the selection of crops is a significant question. It relies on different parameters, such as the rate of production, market price and policies of the government. Many researchers have researched crop yield rate prediction, weather prediction, soil classification and crop classification using statistical methods or machine learning techniques for agricultural planning. In this paper, novel crop diseases detection system based on deformable model have proposed to handle the segmentation of crop images.

Keywords: Crop disease, pre-processing, classifier algorithm, feature extraction Convolutional neural network.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, (2022); DOI : 10.18090/samriddhi.v14spli02.16

INTRODUCTION

Predictive Analysis in order to increase productivity and crop production efficiency, agricultural systems are very efficient. Population, however, increases slowly, while the crop production resource declines day by day. Traditionally, farming includes planting the crop or harvesting it according to a predetermined timetable. With the impact of weather variation in India, majority of the agricultural crops are being severely affected in terms of their performance [1]. Attaining maximum yield rate of crop using restricted land resource is a goal of agriculture planning in an agro-based country [2]. In their study they have shown that a method name crops selection method to solve crops selection problem. Recently, modern people don't have cognizance about the cultivation of the crops in a right time and at a right place [3]. For improving prediction of crop yield under different climatic scenarios, machine learning methods are widely being used.

In this paper, the reviews on use of such machine learning technique for Indian rice cropping areas have presented [4]. If plants and crops suffer from pests, it impacts the country's agricultural production [5], in their study suggested identify the symptoms of plants at very early stage. Precision agriculture requires the collection of real-time weather data, air quality, soil, crop maturity, machinery, labor costs and current data convenience. This prognostic analytics can be used to make cleverer decisions in agricultural field. Farmers, through their experience, predict the diseases; however this is also not the correct approach. Crop diseases are triggered by bacteria, fungi, viruses etc. To control this, diseases in crop are classified based on diseased leaf types using ANN and

Corresponding Author : D.P. Gaikwad, Department of Computer Engineering, AISSMS College of Engineering, Pune 411001; e-mail : dp.g@rediffmail.com

How to cite this article : Gaikwad, D.P., Sonone, A., Patil, S., Limbole, S., Jain, N. (2022). Crop Disease Detection System Using Deep Learning Method.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, Volume 14, Special Issue (2), 291-295.

Source of support : Nil

Conflict of interest : None

therefore we can take necessary steps in time to minimize loss of production. In this impression, people take the picture of leaf of crop which he has swon in his farm. After connecting it will be uploading on server and then uploaded image is processed and accordingly the features of that image are extracted. Oculus observation by consultants is the most adopted method for the detection and identification of plant diseases.

In this section, some existing detection system has presented. Shruthi, Nagaveni V, Dr. Raghavendra B K [6] proposed the review that does a comparative analysis different machine learning classification methods for plant disease recognition. When compared to other classifiers, the SVM classifier is applied by many authors for disease classification. Machine learning algorithms for disease identification and classification have been compared in a large survey.We investigated the effectiveness of the Support Vector Machine (SVM) Classification Technique, the K-Nearest Neighbor Classification Technique, and the Fuzzy C-Means Classifier techniques for detecting plant illnesses. Kirti, Navin Rajpal [7] proposed the review where Black Rot is a fungal disease that affects both yield and wine quality, and can even result in crop loss. The Plant Village Dataset is used, which includes photos of grape plant leaves that have been afflicted by Block Rot Disease as well as healthy leaves. For segmentation, the HSV and L*a*b* colour models are utilized. Color-based approaches are used to differentiate the healthy and diseased parts of the leaves, and the features are saved for each leaf. The colour of the diseased half of the leaf is extremely different from the healthy part, making it simpler to spot. Jayraj Chopda, Sagar Nakum, Vivek Nakrani ,Prof. Hiral Raveshiya [8] have presented a method that uses a 'Decision Tree Classifier' to predict cotton crop illnesses based on temperature, soil moisture, and other variables. This would benefit farmers by allowing them to produce higher-quality products, and we would also focus on developing an Android application that would provide real-time output to farmers in an efficient manner. : Zeel S.Ramesh, D.vydeki [9] described Rice blast disease is a big issue in the agriculture industry all over the world. The farmer will save a significant financial loss if the sickness is detected early. In this research, a machine learning technique is proposed for detecting disease symptoms in rice plants. The use of a machine learning algorithm allows for the automatic detection of plant disease. For the suggested method, photographs of healthy and diseased leaves are taken.

ARCHITECTURE OF THE PROPOSED CROP DISEASE DETECTION SYSTEM

In figure 1, the architecture of proposed crop disease detection system has depicted. In figure 1, Image processing steps for detecting plant illnesses have given. The entire procedure is broken down into three stages.

1. Users produce input photographs on an Android device or upload them to our web application.

2. Separation Picture segmentation, image enhancement, and colour space conversion are all examples of pre-processing. First, a filter is applied to the digital picture of the image. Then, for each image, create an array. Each image name is converted to a binary field using the scientific term for Binaries' Diseases.

CNN classifiers are programmed to recognize illnesses in different plant classes. The Level 2 results are used to activate a classifier that has been trained to classify various plant illnesses

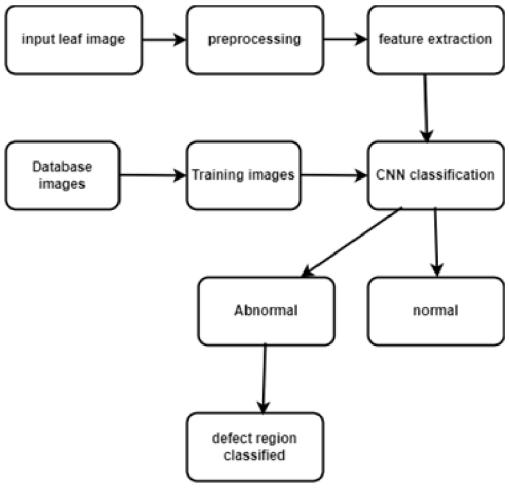


Figure 1: Image Processing Steps

Training Process

The amplitude of F at any pair of coordinates (x, y) is called the intensity of that picture at that place. An image is defined as a two-dimensional function, F(x,y), where x and y are spatial coordinates. A digital image is one in which the x, y, and amplitude values of F are all finite. To put it another way, an image can be defined as a two-dimensional array with rows and columns. A digital image is made up of a limited number of elements, each of which has a specific value at a specific

position. Picture elements, image elements, and pixels are all terms used to describe these elements. A pixel is the most common unit of measurement for the elements of a digital image. BINARY IMAGE– As the name implies a binary image has only two pixel elements: 0 and 1, where 0 denotes black and 1 denotes white. Monochrome is another name for this image. BLACK AND WHITE IMAGE– a BLACK AND WHITE IMAGE is an image that exclusively has black and white colors. COLOR FORMAT OF 8 BITS– This is the most well-known image format. Grayscale Image is a type of image that contains 256 different shades of colour. In this format, 0 represents black, 255 represents white and 127 represents grey. COLOR FORMAT OF 16 BITS– This is a colour image format. It contains 65,536 distinct colours. High Color Format is another name for it.

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & f(0,2) & \dots & f(0,N-1) \\ f(1,0) & f(1,1) & f(1,2) & \dots & f(1,N-1) \\ . & . & . & & . \\ . & . & . & & . \\ . & . & . & & . \\ f(M-1,0) & f(M-1,1) & f(M-1,2) & \dots & f(M-1,N-1) \end{bmatrix}$$

- ACQUISITION– It could be as basic as being given a digital image to work with. The major tasks are: a) scaling
- b) Color transformation (RGB to Gray or vice-versa)
- IMAGE ENHANCEMENT– It is one of the most basic and appealing aspects of Image Processing, and it is also used to extract some hidden elements from an image. It is subjective.
- Picture RESTORATION– This likewise has to do with making an image appealing, but it is more objective (Restoration is based on mathematical or probabilistic model or image degradation).
- COLOR IMAGE PROCESSING– This section covers pseudocolor and full colour image processing, as well as colour models that can be used in digital image processing.
- WAVELETS AND MULTI-RESOLUTION PROCESSING– This is the foundation for portraying images in a variety of ways.

Overlapping Fields with Image Processing

Following figure 2 depicts the different methods of image processing**.**

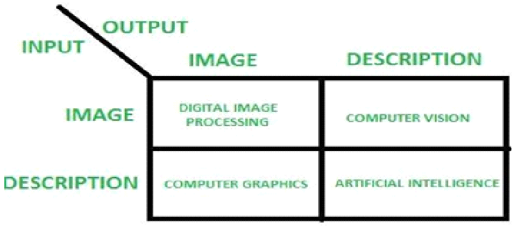


Figure 2: Overlapping Fields with Image Processing

According to block 1, if the input is an image and the output is an image, the process is known as digital image processing. Computer Vision is defined as an input that is an image and an output that is some kind of information or description, according to block 2. Computer graphics, according to block 3, is when the input is a description or code and the output is an image. According to block 4, if the input is a description, keywords, or code, and the output is a description or keywords, it is referred to as Artificial Intelligence. Secure and efficient system. The study showed the advantages of this method in addressing problem in land grading. The advantage of support vector regression is to avoid difficulties of using linear function in large input samples space and optimization of a complex problems transformed into simple linear function optimization. SVM calculation has a regularization parameter, which stays away from over-fitting.

CNN Algorithm

CNN analyses the picture piece by piece. Highlights are the pieces that CNN looks for. CNNs are better at seeing closeness than complete picture coordinating plans when it comes to finding harsh element matches in two photographs in similar places. Each component resembles a little version of a larger image, a two-dimensional cluster of attributes. Figure 3 depicts the diagram of CNN. The CONVOLUTIONAL LAYER is the first layer of a CNN network, and it is the main building block that handles the majority of the computational work. Filters or kernels are used to convolve data or images. The second layer is the ACTIVATION LAYER, which uses the ReLu (Rectified Linear Unit). In this stage, we use the rectifier function to increase the CNN's non-linearity. Different things that are not linear to each other are used to create images. The third layer is the POOLING LAYER, which incorporates feature down sampling. It is applied to each layer in the three-dimensional volume. The FULLY CONNECTED LAYER, which involves Flattening, is the final step. The complete pooling feature map matrix is converted into

a single column, which is then supplied to the neural network for processing.

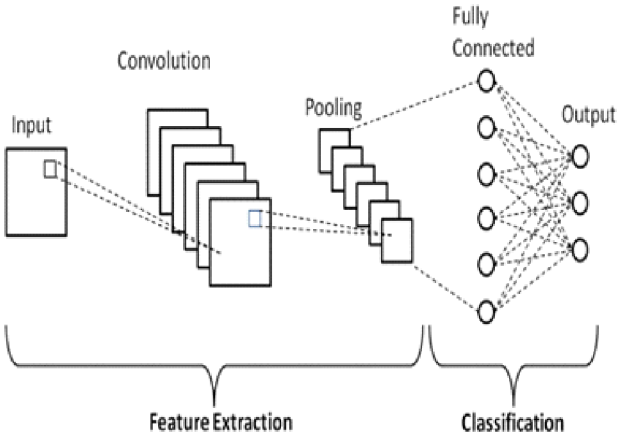


Figure 3: Block Diagram Of CNN

SYSTEM OUTPUTS

Figure 4 depicts the screen output of this project.

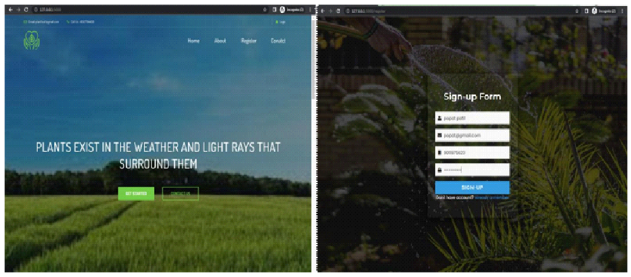


Figure 4. Screenshot of GUI (Home Page and Sign Up form)

In figure 5, the loss values on training and validation are shown. In figure 6, the accuracy of the proposed crop disease detection has shown. Figure 7 is used to show the output showing the disease on tomato leave.

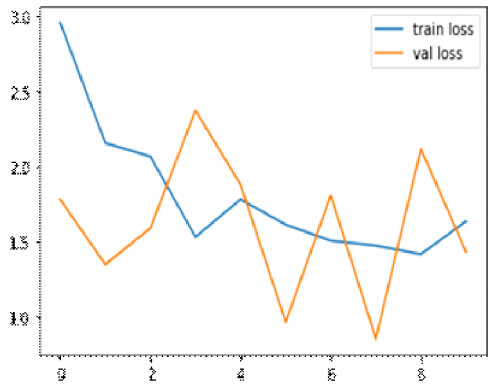


Figure 5: Training loss and Validation loss values

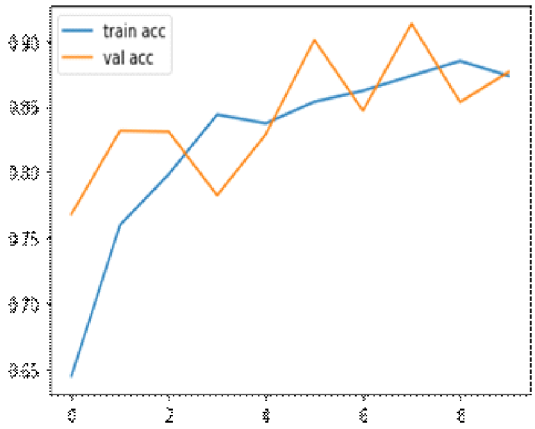


Figure 6: Train Accuracy and Accuracy

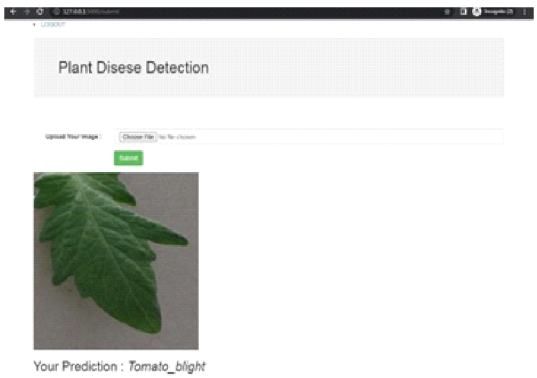


Figure 8: Screenshot of Actual Output Displayed on the user interface

CONCLUSIONS

In this paper, crop disease detection systems have proposed suing convolutional neural network. According to our observations, the scope is still open for the Outcome enhancement. During the research that we carried out, it is noted that the algorithm used for most of the A unified approach is not used by writers where all the variables are involved. It is possible to use the effect on crop yield simultaneously to estimate crop yield. The outcome can also be strengthened by using a neural network approach.

REFERENCES

[1] S. Veenadhari, B. Misra and C. Singh, "Machine learning approach for forecasting crop yield based on climatic parameters," 2014 International Conference on Computer Communication and Informatics, 2014, pp. 1-5, doi: 10.1109/ICCCI.2014.6921718.

[2] R. Kumar, M. P. Singh, P. Kumar and J. P. Singh, "Crop Selection Method to maximize crop yield rate using machine learning technique," 2015

International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015, pp. 138-145, doi: 10.1109/ICSTM.2015. 7225403.

[3] Devdatta A. Bondre, Santosh Mahagaonkar, "Prediction of crop yield and fertilizer recommendation using machine learning algorithm,"Vol. 4, Issue 5, ISSN No. 2455-2143, Pages 371-376

[4] Niketa G, Leisa A.J., Owaiz Petkar, and Amiya K.T. (2016). Rice Crop Yield Prediction in India using Support Vector Machines 978-1-5090-2033- 1/16/$31.00 ©2016 IEEE.

[5] K. Soujanya and J. Jabez, "Recognition of Plant Diseases by Leaf Image Classification Based on Improved AlexNet," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021, pp. 1306-1313, doi: 10.1109/ ICOSEC51865. 2021. 9591809.

[6] U. Shruthi, V. Nagaveni and B. K. Raghavendra, "A Review on Machine Learning Classification Techniques for Plant Disease Detection," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), 2019, pp. 281-284, doi: 10.1109/ ICACCS.2019.8728415.

[7] Kirti and N. Rajpal, "Black Rot Disease Detection in Grape Plant (Vitis vinifera) Using Colour Based Segmentation & Machine Learning," 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 2020, pp. 976-979, doi: 10.1109/ICACCCN51052. 2020.9362812

[8] J. Chopda, H. Raveshiya, S. Nakum and V. Nakrani, "Cotton Crop Disease Detection using Decision Tree Classifier," 2018 International Conference on Smart City and Emerging Technology (ICSCET), 2018, pp. 1-5, doi: 10.1109/ICSCET.2018.8537336.

[9] S. Ramesh and D. Vydeki, "Rice Blast Disease Detection and Classification Using Machine Learning Algorithm," 2018 2nd International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE), 2018, pp. 255-259, doi: 10.1109/ICMETE. 2018.00063.

RESEARCH ARTICLE

SAMRIDDHI Volume 14, Special Issue 2, 2022 Print ISSN : 2229-7111 Online ISSN : 2454-5767

Data Storage Security in Cloud Computing Using Aes Algorithm and Md5 Algorithm

Anil Kumar J Kadam[1*], Vaibhav Varma[2], Sonal Patil[3], Mohit Patil[4], Madhuri Patil[5]

[1*-5] Department of Computer Engineering, College Name- AISSMS COE, Pune, India, e-mail :

ABSTRACT

The most intriguing computing paradigm shift in information technology today is cloud computing. However, security and privacy are seen as major roadblocks to widespread adoption. The authors present a list of important security concerns and encourage more research into security solutions for a secure public cloud environment. Cloud computing is a new term for a long- awaited technology. Computing as a utility is a vision. The cloud gives on-demand network access to a centralised pool of programmable computing resources that may be deployed quickly and effectively as well as little management overhead

Keywords: Cloud Computing, Security, AES Algorithm, MD5 Algorithm.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, (2022); DOI : 10.18090/samriddhi.v14spli02.17

INTRODUCTION

Since its beginnings, cloud computing has been used by billions of users all over the world as an innovation and final solution for utility and distributed computing on Web applications. Its use and impact are felt in a variety of industries, disciplines, and businesses all around the world. Nonetheless, cloud computing has encountered some challenges; the purpose of this research is to identify the factors impacting performance and provide some remedies or advice to cloud users who may encounter performance issues:

1. Information integrity and protection in the cloud domain, as opposed to the traditional approach to information storage.
2. The ability to transform data from a variety of sources into intelligence and deliver it to the appropriate individuals and systems.
3. When several users access the cloud service, load balancing and traffic control are required.
4. Large-scale data, high-performance computing, automation, response speed, rapid prototyping, and rapid time to production are all issues that must be addressed.

Corresponding Author : Anil Kumar J Kadam, Department of Computer Engineering, College Name- AISSMS COE, Pune, India, e-mail :

How to cite this article : Kadam, A.K.J., Varma, V., Patil. S., Patil, M., Patil, M. (2022). Data Storage Security in Cloud Computing Using Aes Algorithm and Md5 Algorithm.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, Volume 14, Special Issue (2), 296-300.

Source of support : Nil

Conflict of interest : None

5. End-users of cloud services have concerns about security, privacy, and trust.
6. Using the cloud as a platform to help create a more dynamic business intelligence environment.

LITERATURE SURVEY

1. Paper Name : Security Challenges for the Public Cloud Author : Kui Ren, Cong Wang, and Qian Wang

   Description : The most intriguing computing paradigm shift in information technology today is cloud computing. However, security and privacy are seen as major roadblocks to widespread adoption. The authors present a number of significant security

concerns and encourage more research into security solutions for a secure public cloud environment.

2. Paper Name: Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

Author : Vipul Goyal Omkant Pandey Amit Sahai Brent Waters§

Description : As more sensitive data is exchanged and stored on the Internet by third-party sites, the demand to encrypt data saved on these sites will grow. One disadvantage of encrypting data is that it can only be communicated in a coarse-grained manner (i.e., giving another party your private key). We create Key-Policy Attribute-Based Encryption, a new cryptosystem for fine-grained sharing of encrypted data (KPABE). Ciphertexts are labelled with sets of attributes in our cryptosystem, and private keys are linked to access structures that control which ciphertexts a user can decipher. We show how our design can be used to share audit-log data and encrypt broadcast data. Hierarchical Identity-Based Encryption is subsumed by our structure, which allows delegation of private keys (HIBE).

3. Paper Name: Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization Author: Brent Waters

Description: A new way for realising Ciphertext-Policy Attribute is presented. Encryption (CPABE) is accomplished in the standard model under concrete and noninteractive cryptographic assumptions. Any encryptor can express access control in terms of any access formula over the system's attributes using our solutions. The amount of the ciphertext, encryption time, and decryption time all scale linearly with the complexity of the access formula in our most efficient approach. The only previous effort that had been done to obtain these parameters was a proof in the generic group model. Within our framework, we show three constructions. The decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption, which can be thought of as a generalisation of the BDHE assumption, is used to argue that our first system is selectively secure. Our following two solutions suggest performance compromises to achieve provable security under the (weaker) decisional Bilinear-Diffie-Hellman scheme.

4. Paper Name: A New Kind of Conditional Proxy Re-Encryption for Secure Cloud Storage

Author: PENG ZENG 1 AND KIM-KWANG RAYMOND CHOO

Description : Secure cloud storage has crucial uses in our big data-driven world, and we need to implement robust access control mechanisms to enable secure cloud storage. PRE (proxy re-encryption) has been proved to be a useful technique for building cryptographically enforced access control schemes. Once the proxy has the required re-encryption key from the delegator, a semi-trusted proxy can transform all ciphertexts for a delegator to ciphertexts for a delegate in a classic PRE scheme. However, in many real applications, fine-grained delegation of decryption abilities is required, hence the concept of conditional PRE (C-PRE) is proposed, which allows the proxy to convert only the ciphertexts that satisfy a specific criteria. We develop a new type of C-PRE called sender- specified PRE (SS-PRE) in this paper, which allows the delegator to delegate the decryption right of ciphertexts from a certain sender to a delegate. A formal definition of SS-PRE and its security model is provided. We also present concrete constructions of an IND-CPA secure SS-PRE scheme and an IND-CCA secure SS-PRE scheme with the properties of unidirectionality and single-use, as well as proofs of security in the standard model for both schemes. Our new IND-CCA secure SS-PRE scheme outperforms traditional C-PRE schemes in terms of calculation cost and ciphertext size, according to a rigorous examination.

5. Paper Name : oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks Author :Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin Description: Because of their convenience and simplicity, text passwords are the most used form of user authentication on websites. Users' passwords, on the other hand, are vulnerable to being stolen and compromised due to a variety of risks and vulnerabilities .For starters, people frequently choose weak passwords and reuse them across multiple websites. Reusing passwords on a regular basis has a domino effect; if an adversary gains access to one website, she will use that password to obtain access to others. Second, inputting passwords into untrusted computers exposes you to the risk of a password thief. To obtain passwords, an adversary can use phishing, keyloggers, and malware, among other methods. In this work, we propose oPass, a user authentication system that uses a user's smartphone and short message service to prevent password theft and reuse threats. oPass merely asks that each participating website have a unique phone number and that the registration and recovery phases involve a telecommunication service provider. Users only need to remember a long-term password for all websites when using oPass.

6. Paper Name: Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications

Author: Lein Harn and Jian Ren

Description: The use of a public-key digital certificate to offer user public key authentication is common in public-key infrastructure (PKI). The public key digital certificate, on the other hand, cannot be utilised as a security element for user authentication. The notion of a generalised digital certificate (GDC) is proposed in this work, which can be utilised to offer user authentication and key agreement. A GDC contains a digital signature of the public information signed by a trusted certificate authority, as well as the user's public information, such as the information from a digital driver's license, a digital birth certificate, and so on (CA). The GDC, on the other hand, does not hold any user's public key. Key management with GDC is significantly easier than with a public-key digital certificate because the user does not have a private and public key pair. The GDC's digital signature serves as a hidden token for each user that is never revealed to any verifier. Instead, by answering to the verifier's challenge, the owner proves to the verifier that he is aware of the signature. We propose discrete logarithm (DL) and integer factoring (IF)-based methods for user authentication and secret key establishment based on this approach.

7. Paper Name : Ensuring Data Storage Security in Cloud Computing With Advanced Encryption Standard (AES) and Authentication Scheme (AS)

Author: Mohamed Ismail, Badamasi Yusuf

Description:- Identification of different security threats related to stored data in cloud computing storage, strategies used to safeguard stored data while in cloud storage, system development using Advanced Encryption Standard as algorithm for data encryption and Authentication Scheme valid users verification and prevention of unauthorised access to all functional units of the system, and examination of the significance of using Advanced Encryption Standard as algorithm for data encryption and Authentication Scheme valid users verification and prevention of unauthorised access to all functional units of the system are some of the main objectives of this paper. This paper includes a general introduction, cloud storage and its key challenges, strategies for protecting saved data privacy while in storage, a literature review, methodology, the suggested system, a conclusion, and future improvements.

PROPOSED SYSTEM

The first user registration has been completed. After that, upload the file to the server with the id. Then convert plain text files into cypher text. Each file is secured with a unique encrypted key using the AES technique. The AES algorithm is a symmetrical block cypher that turns plain text into cypher text in blocks of 128 bits utilizing keys of 128, 192, and 256 bits. Using the md5 and sha1 algorithms, the file is stored on the server with a unique id called message digest. MD5 (Message Digest Method 5) is a cryptographic hashing technique that produces a 128-bit digest from any string. The digests are represented as 32-digit hexadecimal numbers. Hashing is the process of converting ordinary data into an unrecognisable format using a hash function. These hash functions, often known as the hash digest or digest in general, are a collection of mathematical calculations that convert the original information into hashed values. Regardless of the input size, the digest size for a hash function like MD5 is always the same. If a user wants to download a file, the AES algorithm is used to decrypt it. For each file, a unique decryption key is generated. Simple text was converted from cypher text. The user can download a file in readable format.

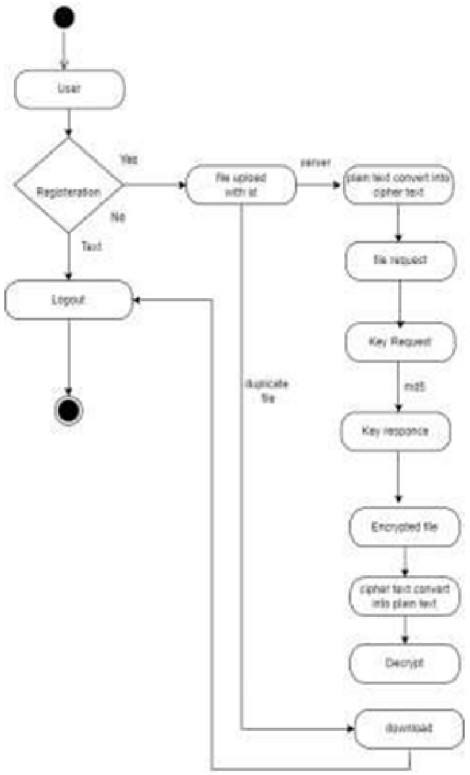


Figure 1: Architecture of The Proposed System

ALGORITHM

The researcher has chosen the Encryption Standard as the method for data encryption and decryption. The AES was used by the US government as a symmetric encryption standard for data processing (Gueron, 2012). After a 5-year standardisation process, the National Institute of Standards and Technology (NIST) announced this encryption method as the best symmetric encryption standard on November 26, 2001.

AES KEY AND BLOCK:-

There are 2^{128} potential keys for 128 bits, which is equal to 3.4×10^{38}. According to APC, breaking the AES cypher with 2^{55} keys per second would take about 149.00 billion years.

There are 2^{198} potential keys for the 192 bits, which is equal to 6.2×10^{57}.

There are 2^{256} potential keys for the 256 bits, which is equal to 1.1×10^{77}.

For a variable length key equal to (128, 192 and 256 bit). They are represented as a byte matrix having an Ai column and four rows, with Ai denoting key length split by 32 bits, as shown below:

(Ai = 4) represents 128 bits of key = 16 bytes.

(Ai = 6) represents 192 bits of key = 24 bytes.

(Ai = 8) represents 256 bits of key = 32 bytes.

A block of 128 bits, or 16 bytes, can be represented in a byte matrix with four rows and Ab columns, where Ab = block length divided by 32

PROCESS OF ENCRYPTION

The AES encryption technique consisted of four phases, as detailed below (Kak, 2016):

The first stage is to substitute bytes; the second step is to shift row; the third step is to mix columns; and the fourth step is to add a round key.

The final step was an exclusive-OR (XOR) of the output from the first three phases, with a four-word key schedule. There is no mix column in the last round of encryption.

PROCESS OF DECRYPTION

As with encryption, the decryption procedure included four rounds. The distinction between the encryption and decryption processes is that the decryption process reverses the shifting and substitution operations of the encryption process. The steps for decryption are:

The first step is to do an inverse shift round. The second step is to do an inverse bytes substitution.

The third step is to add a circular key.

The fourth step is to create an inverse mix column.

Exclusive oaring (XOR) of the first two steps made up the third step. There is no inverse mix column in the final phase of decryption. An example of AES encryption and decryption is provided below:

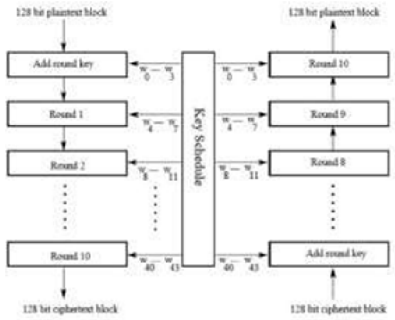


Figure 2: AES encryption and decryption process

MD5 Algorithm **:-**

The MD5 message-digest hashing algorithm uses 512-bit strings that are separated into 16 words of 32 bits each. As a result, MD5 generates a 128-bit message digest value. Each 512-bit block of data is processed along with the value produced in the previous stage to produce the MD5 digest value. In the first stage, the message-digest values are initialised using sequential hexadecimal numerical integers. Each stage includes four message-digest passes, which change values in the current data block as well as values digested from the previous block. The MD5 digest for that block is calculated using the previous block's final value.

CONCLUSION

In the proposed system, with all data stored on the cloud and the internet, it is critical to maintain data security as a top priority. To encrypt confidential data, we utilised the most secure algorithm we've ever used. To guarantee the highest level of security, we used the AES, and MD5 algorithms in the suggested system. However, there are still numerous holes that can be addressed by improving the effectiveness of these strategies.To make cloud computing acceptable to cloud service users, further effort is needed in this field. This project is about data security and privacy, with a focus on data storage and use in the cloud. It aims to develop trust between cloud service providers and consumers by protecting data in cloud computing environments.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, no. 1, pp. 69–73, 2012.

[2] L. Zhou, Y. Zhu, and A. Castiglione, "Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner," Computers & Security, vol. 69, pp. 84–96, 2017.

[3] S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, "Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data," IEEE Transactions on Image Processing, vol. 25, no. 7, pp. 3411–3425, 2016.

[4] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 651–663, 2012.

[5] L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," IEEE Transactions on Wireless Communications, vol. 10, no. 7, pp. 2372–2379, 2011.

[6] P. Zeng, K.-K. R. Choo, "A new kind of conditional proxy re-encryption for secure cloud storage", IEEE Access, vol. 6, pp. 70017-70024, 2018.

[7] Mohamed Ismail, Badamasi Yusuf " ENSURING DATA STORAGE SECURITY IN CLOUD COMPUTING WITH ADVANCED ENCRYPTION STANDARD (AES) AND AUTHENTICATION SCHEME (AS)" International Journal of Information System and Engineering Vol. 4 (No.1), ISSN: 2289-7615

[8] Khalid, U., Ghafoor, A., Irum, M. & Shibl, M. A., 2013." Cloud Based Secure and Privacy Enhanced Authentication and Authorization Protoco. Procedia", Volume 22, pp. 680-688.

[9] Tidke, P. M. P. a. P. B., 2014. "Improving Data Integrity for Data Storage Security in Cloud Computing". International Journal of Computer Science and Information Technologies (IJCSIT), 5(5), pp. 6680-6684

[10] Singh, R., Kumar, S. & Agrahari, S. K., 2013. "Ensuring Data Storage Security in Cloud Computing". International Journal Of Engineering And Computer Science ISSN:2319- 7242 , 2(3), pp. 825- 826

[11] Kokane, M., Jain, P. & Sarangdhar, P., 2013."Data Storage Security in Cloud Computing". International Journal of Advanced Research in Computer and Communication Engineering , 2(3), pp. 1388- 1389.

[12] Gadichha, N. M. Y. a. V. B., 2013. "Third Party Auditing (TPA) for Data Storage Security in Cloud with RC5 Algorithm." International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3(11), pp. 1032-1037

[13] Wang, G., Q. Liu, J. W. & Guo, M., 2011. "Hierarchical Attribute Based Encryption and Scalable User Revocation for Sharing Data in Cloud Servers. Computers and Security", 30(5), pp. 320-331.