Implementing Hybrid Security Mechanism for Cloud Considering Intrusion, Sql Injection and Performance Degradation

Manju Sharma, Mukesh Kumar Sharma

Abstract**: *Considering the demand of cloud services research has considered the issues or problems related to cloud computing. Various approaches adopted by existing research have limited scope and there is need to increase the security of cloud computing environment. The issues of security threat in cloud environment are explained in this paper. There have been several security threats to cloud environment such as Intrusion, brute force, Sql injection, Trozen horse that could affect the security of cloud services. There remains issue of Un-authentic access. Moreover the identity management is becoming a great challenge. Previous researches have proposed cryptographic approach while some provided solution to hacking attempts along with unauthentic external access but these security mechanisms are not sufficient to protect the cloud. Research paper is introducing intelligent system that is capable to trace the intrusion using LSTM based training model. The model is trained in order to categorize intrusion accordingly. The focus of research is to increase the security from intrusion by providing intelligent LSTM approach. This mechanism would classify the transmission in different categories such as Dos-synflooding, MITM ARP spoofing, Mirai-Ackflooding, Mirai-Http flooding, Mirai-Hostbruteforceg, Mirai-UDP Flooding, scan hostport and Normal. Moreover research paper has focused on prevention of Sql injection attacks. In order to increase the security between sender and receiver research has also allowed two way port based hand shaking in order to transmit data more securely. The transmission would be initiated using default port but the actual transmission would be made using random port that would be set for specific time slot.***

Keywords**: *Cloud computing, IDS, Port, Sql Injection***

I. INTRODUCTION

Need of cloud services has been increasing day to day but there are issues or problems related to security and performance of cloud computing. Various approaches adopted by existing research have limited scope and there is need to increase the security of cloud computing environment. There are many security threats to cloud environment like Intrusion, brute force, Sql injection, Trozen horse which are affecting the performance of cloud services and breach the security. The research paper focused on building smart system for intrusion detection, sql injection prevention mechanism, multiport based security system during security deployment.

A. Cloud computing

Cloud computing has been termed as on-demand delivery of IT resources. This delivery is performed over Internet using pay-as-you-go pricing. User could access technology services like computing power as well as storage without buying and maintaining data centers or servers. It has been frequently used in AI, IOT, Healthcare, Distance education Services.

Security ***threats***

Most common computer security threats to cloud are hacking attempt from intruders. The security threats could be in form of virus, malware, intrusion or sql injections. There have been cryptographic approach and firewall to provide security against such threats. But the security mechanisms are suffering from their own limitations. The encryption mechanism many times reduces the performance of network. Moreover it becomes difficult for a system to secure cloud from every type of security threats. Thus there always remains to enhance the security mechanism.

B. IDS

An Intrusion Detection System has been considered as network security technology that has been built in order to find the vulnerability exploits for system. Intrusion Detection System has been termed as system which is monitoring the network traffic in case of suspicious activity. It issues alerts in case of such activities. This could be stated as software application which is scanning a network as well a system in case of harmful activity as well as policy breaching. Several malicious venture or violation is normally reported either to an administrator or collected centrally with support of security information as well as event management system. Such system is integrating outputs from several sources. It is using alarm filtering mechanism to differentiate harmful activity from wrong triggering of alarms.

C. SQL Injection

The SQL Injection is meant for injection attack where attacker could implement nasty SQL statements which are controlling web application's database server. SQL Injection vulnerability could probably influence websites as well as web applications that are able to use of SQL dependent database.

Manuscript received on March 10, 2021.
Revised Manuscript received on March 20, 2021.
Manuscript published on March 30, 2021.
***** Correspondence Author

Manju Sharma*, Research Scholar, UIET Department, MDU, Rohtak, India. Email: manju.sharmag@gmail.com

Dr. Mukesh Kumar Sharma, Department of Computer Science & Engineering, TIT & S, Bhiwani, India. Email:drmukeshji@gmail.com

D. Port based security

The port from 0 to 1023 is reserved for predefined protocol. The proposed work considers the security enhancement by applying multiport mechanism where during initial transmission the random port above 1023 would be transferred from one node to another and actual transmission would take place in next cycle

by via random port stated at initial transmission to restrict unauthentic access of data.

E. Data compression

It has been observed that the data encryption slows down the performance when it is applied in cloud environment for security. In proposed work the data would be compressed in order to reduce the length of string that is to be encrypted. This would support the improvement in performance during encryption. The issues of security threat in cloud environment have been explained in this section 1. Existing research related to cloud security are presented in section 2. The section 3 is presenting the problem or issues found in previous researches. Section 4 has focused on the proposed work and its process flow that has fulfilled objective of research. Process flow of the research is proposed work is shown in this section. Section 5 is presenting the result and discussion according to proposed work. Finally section 6 has presented the conclusion of research.

II. LITERATURE REVIEW

There have been several researches that have focused on cloud security, intrusion detection, sql injection and cryptography. The existing researches in field of cloud security are explained in this section. the researches have been discussed along with their author, year, objective, methodology and results.

Table- I: List of existing research

Sno	Author/Year	Objective of research	Methodology/ technique	Result
1.	Li, Peisong / 2019	To provide Novel approach for Intrusion Detection Method in Internet of Things	Intrusion detection mechanism	Research proposed novel approach to secure system from Intrusion in case of IoT
2.	Yin, Chuanlong / 2017	Proposing the deep learning approach for intrusion detection using recurrent neural networks	RNN	Research introduced smart system to train and test IDS system
3.	Dong, Bo / 2016	Performing comparison between deep learning method to traditional methods using for network intrusion detection	Deep learning	Learning system built for IDS had been proven better than traditional approaches.
4.	Ullah, Imtiaz /2020	Proposing scheme to generate a Dataset for Anomalous Activity Detection in IoT Networks	Anomalous activity detection	System is suitable to enhance security to IoT System
5.	Althubiti, Sara A / 2018	To propose Lstm for anomaly-based network intrusion detection	LSTM	Research proposed high accuracy to IDS system
6.	Jianghong Wei /2015	To provide secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption	Identity based encryption	Research has proposed the security during data sharing in cloud environment
7.	S. Ruj, M/2014	Providing decentralized access control with anonymous authentication of data stored in clouds	Access control mechanism	Research found suitable to implement access control in decentralized environment.
8	X. Huang, J. Liu / 2014	To apply cost-effective authentic and anonymous data sharing with forward security	Authentication mechanism	Research has provided cost security mechanism.
9	C.-K. Chu/2014	Implementing Key-aggregate cryptosystem in case of scalable data sharing in cloud storage	Cryptographic approach	This work has given scalable data sharing using encryption
10	D. Boneh and M. Franklin/2003	Proposing Identity based encryption from the weil pairing	Cryptographic approach	Research increased the security for weil pairing
11	W. Aiello / 1998	To implement rapid digital identity revocation	Identity security mechanism	This work is capable to provide quick digital revocation to secure identity
12	A. Boldyreva / 2008	To provide Identity dependent encryption with efficient revocation	Identity based encryption	Work is suitable to enhance security for identity
13	K. Liang, J. K. Liu / 2014	To propose efficient cloud based revocable identity-based proxy re-encryption scheme for public clouds data sharing	Identity based proxy re-encryption mechanism	Research focused on identity protection in cloud environment
14	Pratik H Sailor/2014	To find and prevent attacks by SQL Injection	Sql Injection security mechanism	Research is restricting the sql injection
15	Tejinderdeep Singh Kalsi/2015	To make use of Novel mechanism in Web Applications find and restrict Of Sql Injection Attacks	Sql Injection security mechanism	Web application are kept secured from sql injection using this mechanism
16	Atefeh Tajpour/2011	To propose efficient mechanism to prevent the SQL Injection	Sql injection security mechanism	Research is providing efficient solution to sql injection.

III. PROBLEM STATEMENT

It has been observed that need of cloud computing is growing day to day but the main issue with cloud computing services are its security. There have been several security threats such as Intrusion, brute force, Sql injection, Trozen horse that could affect the performance of cloud services and breach the security. There remains issue of Un-authentic access. Moreover the identity management is becoming a great challenge.

However there have been several researches related to cloud security that has proposed several security mechanisms. Some of them have proposed cryptographic approach while some provided solution to hacking attempts as well as unauthentic external access. Still there is need to introduce intelligent system that should be capable to trace the intrusion and categorize it accordingly so that it could be managed easily. Thus there is need to propose intelligent IDS system that should be smart enough to manage the intrusion on the basis of training LSTM network. It has been observed that there was lack of accuracy during predicting IDS in previous system. Moreover previous research has focused on limited type of attacks.

IV. PROPOSED WORK

The objective of this research is to understand the security threats and identify the appropriate security techniques used to mitigate them in cloud computing. This work mainly concerned with the problem of identity management and access control in application and service level. During identity control the authentication is provided on the basis of identity of user. Only authentic user is provided the access control. The main objectives of this research are to understand the infrastructure layers (architecture) and working of security mechanism in cloud. Research has studied different aspects of services and cloud challenges from customer's and provider's perspectives. Research is considering the various security feature offered to the application running on the cloud for comparative analysis of the security features. Proposed work has provided a broad comparison of cloud services, deployment strategies and security mechanisms for deciding that which cloud provider or service is suitable for the user. Designing of a framework has been made to suggest counter measures for the future challenges to be faced in cloud computing and how to best use the cloud computing.

Infrastructure layer (Architecture)

Cloud environment consists of interconnectivity between client infrastructures to remote running application, services, storage that are hosted on remote cloud environment.

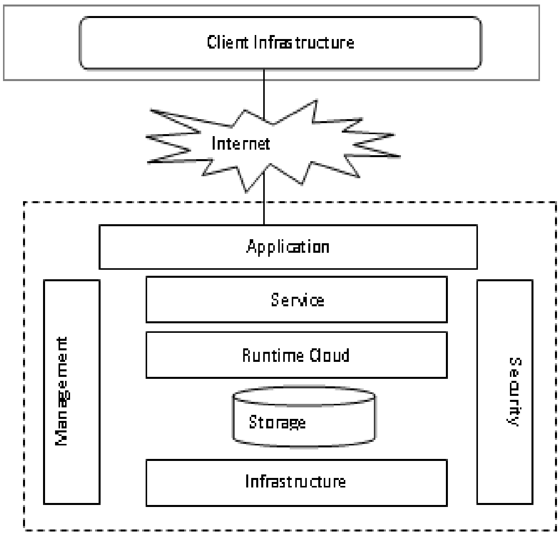


Fig. 1.Architecture of Cloud infrastructure layer

The management module of cloud allows the secure and efficient transmission of data among different layers of cloud. Data is transferred from different remote application to storage and sometime it is transferred to client infrastructure too. But the security of this data is essential. These remote services, files stored on remote storage and application running on cloud are provided security using different security mechanism such as encryption, firewall.

Working security mechanism over cloud

In order to transmit data securely over cloud encryption and decryption operations are performed. Data that is in plain format is converted from readable form to unreadable form using encryption mechanism as shown in figure 2. Function used during encryption is acting as key for encryption on other hand at the time of decryption data is again converted from unreadable to readable format.

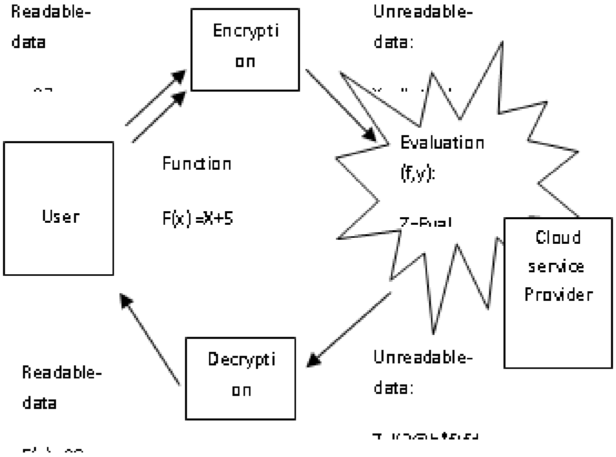


Fig. 2.Working of security mechanism over cloud

Cloud challenges

It has been observed that cloud environment is facing several challenges such as security issues, lack of appropriate resources, cost issues, downtime issues, and management issues in multi cloud environment.

More over it has been observed that there are issues related to portability and interoperability. However cloud is gaining popularity day to day but there are several challenge in usage of cloud from customer as well as cloud service provider perspectives.

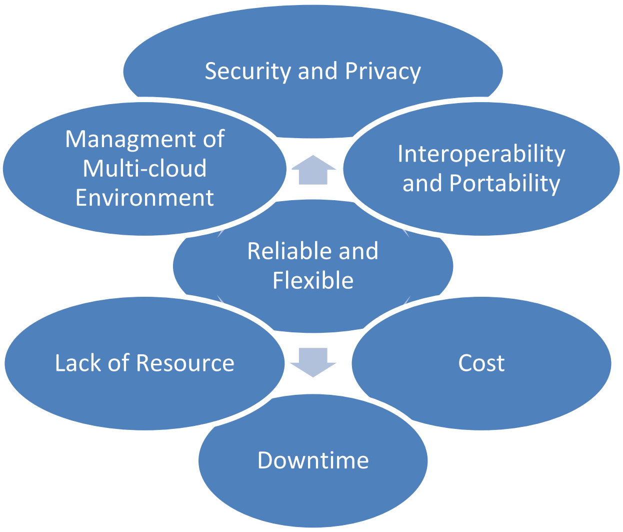


Fig. 3.Cloud challenges

Challenges from Customer's perspective

Customer need to depend on internet to access the cloud services. The availability of internet and unavailability of internet influences the quality of services in different areas. The customer from rural area, finds themselves uncomfortable to afford the cloud services because the internet services are very poor in rural areas. Moreover due to lack of technical skills customers could use limited cloud services.

Challenges Provider perspectives

The setup of cloud environment requires lot of technical skill. However it reduces the cost for customer but its initial setup cost is much for service provider. Moreover the service providers need to expend on the security of cloud. The management of application and service is quite challenging job for cloud service provider.

Comparison of cloud services

The cloud is a broad concept embracing different sorts of online services. For those who consider cloud services for their business, it's important to grasp the difference between IaaS, PaaS and SaaS — the core cloud models available. You should choose the particular model depending on your business requirements and on the number of tasks you want to perform yourself or delegate to the service provider.

The -aaS acronyms are always confusing. They mean "something" as a service. Today, practically everything can be presented as a service. One of the most popular questions is the difference between IaaS, PaaS and SaaS. SaaS, PaaS, IaaS have been explained in order to help you develop the right understanding of the concept and create a suitable cloud migration strategy for your organization.

- **IaaS** — Infrastructure as a Service
- **PaaS** — Platform as a Service
- **SaaS** — Software as a Service

Table- II: Comparison between IaaS, PaaS, SaaS

	IAAS	**PaaS**	**SaaS**
Who uses it	System Administration	Developers	End users
What Uses get	Virtual data center to store information and develop platforms for the services and application development, testing and deployment.	Virtual platform and tools to develop, test and deply application and services	Web software and application to complete business operations
Provider Controls	Servers Storage Networking Virtualization	Servers Storage Networking Virtualization OS Middleware Runtime	Servers Storage Networking Virtualization OS Middleware Runtime Applications Data
User Controls	OS Middleware Runtime Applications Data	Applications Data	-

Proposed work has been classified in three section

- LSTM based training to IDS dataset to predict category of intrusion
- Proposing prevention mechanism for Sql Injection
- Proposing multiport mechanism for secured data transmission

A. LSTM BASED TRAINING TO IDS DATASET TO PREDICT CATEGORY OF INTRUSION

To simulate the deployment model that considers the training of a dataset of 4,28,500 record is used.

The model has been used to perform accurate classification in IDS. Before the training network model, there is a need for dataset pre-processing. During the initial dataset pre-processing, Shapiro wilk has been used to eliminate the attribute with less significance. Then useless attributes that have a single value in all records are eliminated. Then data is classified as 70% for training and 30% for testing. In the proposed deployed model two LSTM layers are used. 12 hidden layers are used in the first LSTM layer and 5 hidden layers are used in the second LSTM layer. However hidden layer has a quality of retaining the previous value but it also raises a problem overfitting that network will not be robust and will increase the loss function, it will make network to be useless when there is need for new dataset or new values of data thus there is need of improvement in the network. Thus dropout layer with 20% is used that would drop 20% neurons from the network. This dropout would be quite helpful in removing the problem of overfitting the network as it will make the network more robust towards a new dataset that can be used in the proposed system. To find the label correctly, a fully connected layer is used. Such a layer does not drop any neurons.

The softmax layer is applied afterward which is an activation layer used in place of the sigmoid function. It is used where there is a classification of more the 2 classes takes place. Classification layers are used to perform different predictions of different attacks in IDS.

After the training of the network model, testing is performed on the dataset. 30% of the dataset has been used for the testing of IDS. Afterward, a confusion matrix is produced considering predicted and actual value to get True positive, False positive, True negative, False negative. The accuracy, precision, recall, f-score is obtained to get overall accuracy.

B. SQL INJECTION PREVENTION MECHANISM FOR CLOUD

SQL injection has been known as a code injection technique. It can easily destroy and hack the important and sensitive data located in a database of a Web based app. Out of different Web hacking technique, SQL injection is one of them. In SQL injection technique, user of a web application inputs SQL statements at the place of his information for example at the time of login, use may input a malicious code in the form of SQL statement instead of his user name. In order to secure a web site, it is essential to use SQL parameters. Generally, SQL injection attacks take place by user of a web app when he is asked to ender his detail for login for example username/userid, and instead of a name/id. But instead of actual detail, he enters an SQL statement which runs on the Web database of his app for example .

UserId: 105 OR 1=1

As this input will reach in SQL, it becomes an SQL statement and behaves as a statement:

SELECT * FROM Users WHERE UserId = 105 OR 1=1;

The SQL above is valid and will return ALL rows from the "Users" table, since OR 1=1 is always TRUE.

As it is discussed above that to avoid SQL Injection attack, it is essential to use statement parameters. It is required that SQL engine make proper checking of each input entered by user. The input must be correct according to its column. This input would be treated literally not as a part of SQL Query.

To execute the SQL queries, close the database server. Often the Attacker gets an input surrounded by web application that includes in the SQL query. For an SQL Injection attack, find a susceptible websites and take clients input within an SQL statement. Then attacker can insert a payload that have SQL query. After that he is capable to compile against database server.

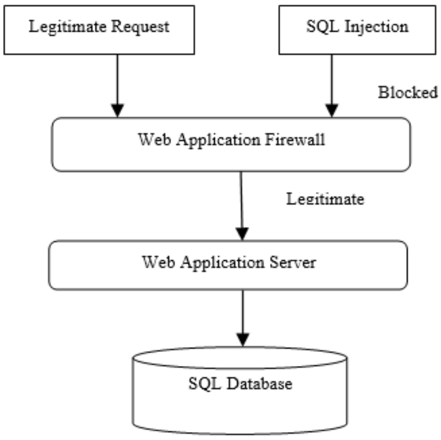


Fig. 4.Structured query language injection working

Algorithm for the work done in case of sql injection

1. A database for user would be created.
2. An interface to login is created.
3. if the login is successful then login proceed and if login is failure then display login failure.
4. Develop a sql injection to login without any authentication.
5. Develop a module to check the sql injection.
6. Test make test of sql injection prevention mechanism.
7. Make time comparison of tradition sql injection mechanism with proposed sql injection.
8. Make unauthentic access probability in case of tradition and proposed sql injection.

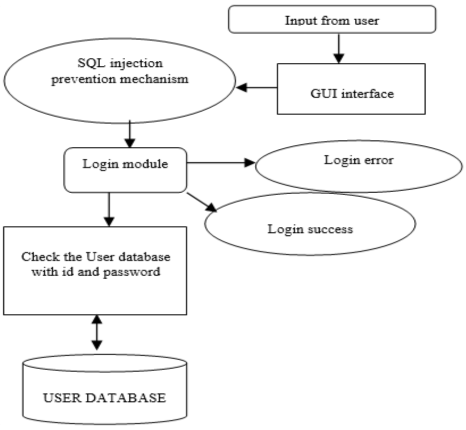

Input from user
SQL injection prevention mechanism
GUI interface
Login module
Login error
Login success
Check the User database with id and password
USER DATABASE

Fig. 5.Working of sql injection prevention mechanism

C. Proposing multiport mechanism for secured data transmission

It is observed that port from 0 to 1023 are already reserved thus The proposed work is considering the security enhancement by applying multiport mechanism. During this work transmission the random port that is above 1023 is made from one node to another. After confirmation of port to be used for actual transmission, transmission is performed in next cycle. This transmission would make use of random port stated at initial transmission to restrict unauthentic access of data.

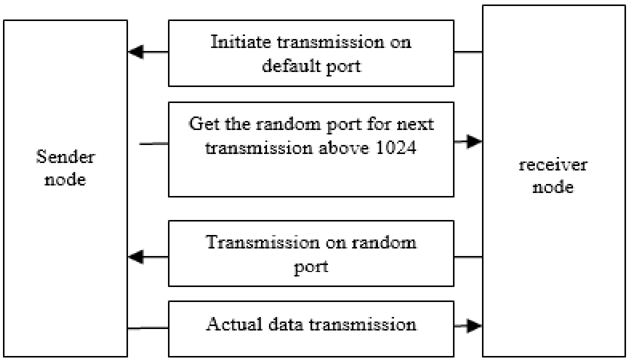

Sender node
Initiate transmission on default port
Get the random port for next transmission above 1024
Transmission on random port
Actual data transmission
receiver node

Fig. 6.Proposed model for multiport based secure transmission

V. RESULT AND DISCUSSION

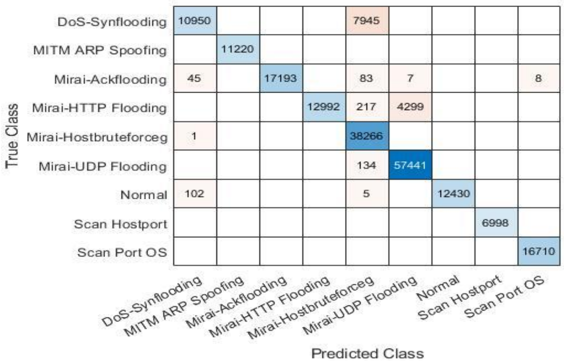
A. Simulation to train and test LSTM based IDS

The training is one of the important steps in IDS. Gradually the progress of the model is increasing. The progress simulation has been the following figure.

Fig. 7.Training in Proposed LSTM model

Confusion matrix

After training of the dataset testing module is run then the confusion matrix is generated. The following confusion matrix is considering 9 attributes Dos-Synflooding, Mimt Arp spoofing, Mirai-Ackflooding, Mirai-Http flooding, Mirai-Host brute-force, Mirai-UDP flooding, normal, scan host port, scan port os. The true classes are presented on the y-axis and predicted classes are presented on the x-axis. With the help of this matrix we can calculate different parameters to the efficiency of the system also we can compare them



	DoS-Synflooding	MITM ARP Spoofing	Mirai-Ackflooding	Mirai-HTTP Flooding	Mirai-Hostbruteforceg	Mirai-UDP Flooding	Normal	Scan Hostport	Scan Port OS
DoS-Synflooding	10950				7945				
MITM ARP Spoofing		11220							
Mirai-Ackflooding	45		17193		83	7			8
Mirai-HTTP Flooding				12992	217	4299			
Mirai-Hostbruteforceg	1				38266				
Mirai-UDP Flooding					134	57441			
Normal	102				5		12430		
Scan Hostport								6998	
Scan Port OS									16710

Fig. 8.Confusion Matrix of proposed model

B. Result

Considering the above confusion matrix chart presenting accuracy, precision, recall value, and f-score is generated. The accuracy chart in the case of existing work is presented below.

Table- III: Accuracy chart of Proposed Model

Class	Accuracy	Precision	Recall	F-Score
1	97.53%	0.751	1	0.861
2	99.99%	1	1	1
3	99.96%	0.991	1	1
4	97.74%	0.751	1	0.851
5	94.15%	0.701	0.991	0.821
6	89.57%	1	0.741	0.851
7	99.97%	1	1	1
8	99.99%	1	1	1
9	99.99%	1	1	1

Comparison in case of previous and proposed work

The comparison of the proposed work and traditional LSTM model with a single layer is presented below. The following chart is presenting that the proposed work has more accuracy, precision value, recall value, and F-scores value as compare to previous LSTM.

The comparison chart for accuracy in case of previous and proposed is shown below:

Table- IV: Comparison of accuracy in case of previous and proposed model

Class	Accuracy in case of previous model	Accuracy in case of proposed model
1	95.89%	97.53%
2	99.9%	99.99%
3	99.95%	99.96%
4	97.66%	97.74%
5	95.77%	94.15%
6	97.74%	89.57%
7	99.96%	99.97%
8	99.99%	99.99%
9	99.99%	99.99%

On basis of above table following chart has been plotted to present difference in accuracy on both model in graphical format.

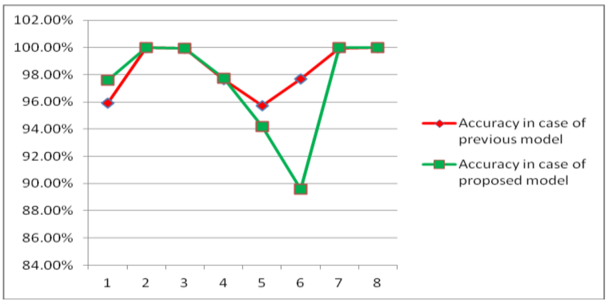


Fig. 9.Comparison of Proposed and previous in case of Accuracy

The comparison chart for Precision in case of previous and proposed is shown below

Table- V: Comparison of precision in case of previous and proposed model

Class	Precision in case of previous model	Precision in case of proposed model
1	0.581	0.751
2	1	1
3	0.991	0.991
4	0.741	0.751
5	1	0.701
6	1	1
7	0.991	1
8	1	1
9	1	1

On the basis of above table following chart has been plotted to present the difference in Precision on both model in graphical format.

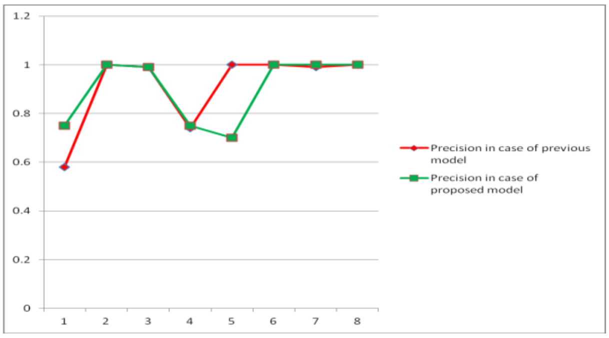


Fig. 10. Comparison of Proposed and previous in case of Precision

The comparison chart for Recall in case of previous and proposed is shown below

Table- VI: Comparison of recall in case of previous and proposed model

Class	Recall in case of previous model	Recall in case of proposed model
1	0.99	1
2	1	1
3	1	1
4	1	1
5	0.82	0.99
6	0.93	0.74
7	1	1
8	1	1
9	1	1

On the basis of above table following chart has been plotted to present the difference in recall value on both model in graphical format.

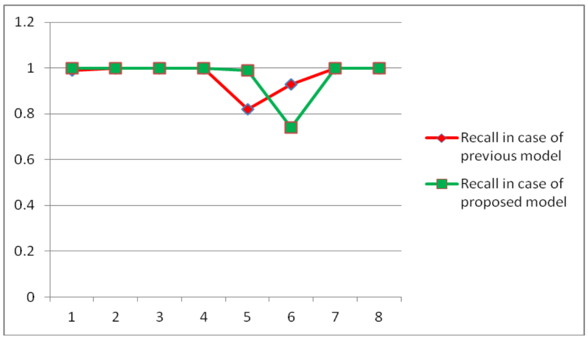


Fig. 11. Comparison of Proposed and previous in case of Recall

The comparison chart for F-Score in case of previous and proposed is shown below

Table- VII: Comparison of F-Score in case of previous and proposed model

Class	F-Score in case of previous model	F-Score in case of proposed model
1	0.73	0.86
2	1	1
3	1	1
4	0.85	0.85
5	0.90	0.82
6	0.96	0.85
7	1	1
8	1	1
9	1	1

On the basis of above table following chart has been plotted to present the difference in F-score on both model in graphical format.

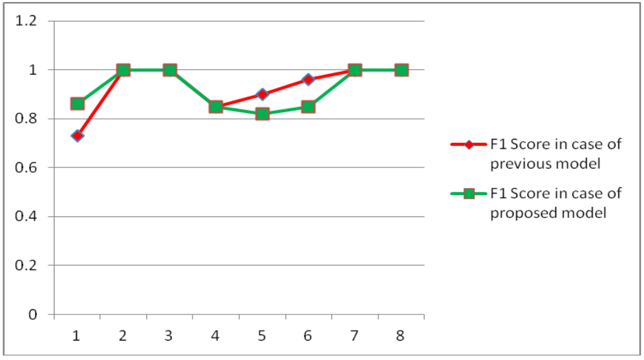


Fig. 12. Comparison of Proposed and previous in case of F-score

Average of accuracy, precision, recall, f-score in both previous and proposed model have taken in table 8 and 9 respectively.

Table- VIII: Getting average accuracy, precision, recall, f-score in case of previous work

Class	Accuracy	Precision	Recall	F1 Score
1	95.89%	0.581	0.99	0.73
2	99.9%	1	1	1
3	99.95%	0.99	1	1
4	97.66%	0.74	1	0.85

5	95.77%	1	0.82	0.90
6	97.74%	1	0.93	0.96
7	99.96%	0.99	1	1
8	99.99%	1	1	1
9	99.99%	1	1	1

Table- IX: Getting average accuracy, precision, recall, f-score in case of proposed work

Class	Accuracy	Precision	Recall	F1 Score
1	97.53%	0.75	1	0.86
2	99.99%	1	1	1
3	99.96%	0.99	1	1
4	97.74%	0.75	1	0.85
5	94.15%	0.70	0.99	0.82
6	89.57%	1	0.74	0.85
7	99.97%	1	1	1s
8	99.99%	1	1	1
9	99.99%	1	1	1

Considering average value of accuracy, precision, recall and f-score from previous and proposed work in from table above tables, Table 10 has been produced to compare both models.

Table- X: Comparison of previous model with proposed work

	Previous	Proposed
Accuracy	97.661	98.54
Precision	91	92.22
Recall	97	97.11
F1 score	93.11	97.77

Following chart is presenting comparison of accuracy, precision, recall and F-score in case of previous and proposed LSTM model.

It has been observed that there is slight change in recall value but there is significant difference in F1score.

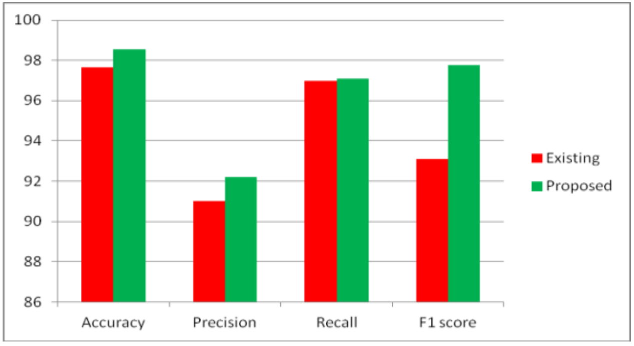


Fig. 13. Comparison of Proposed and previous LSTM model

C. SIMULATION OF PREVENTION FROM SQL INJECTION

In order to prevent sql injection the web interface input box to read password would not receive data from key board. It will receive data from keyboard on web interface. That would restrict entry of special character that could raise sql injection. At the time of entering private data such as login and password for an online banking account from a regular keyboard, there remains risk of data interception by spyware. These programs record the keys pressed on the keyboard. Therefore capture the data entered from the regular keyboard to pass it to the malefactor. These keyboards also restrict attacker to use sql injection as programmer could restrict the input of wild characters such as % or _ in order to prevent attacker to enter sql command in password field.

The password field would be read only to get input from keyboard. User would be unable to feed data from keyboard. An online key pattern would be visible bellow the password field in order to take input. This would make the system more secure. This would not allow user to insert SQL injection. The password fed by pattern based key board would definitely increase the protection of web application. Here the web security has been enhanced using addition security code. Administrator of site would specify the code for particular date and time. That code would e applicable in that particular time slot along with user id and password. Following is the login simulation.

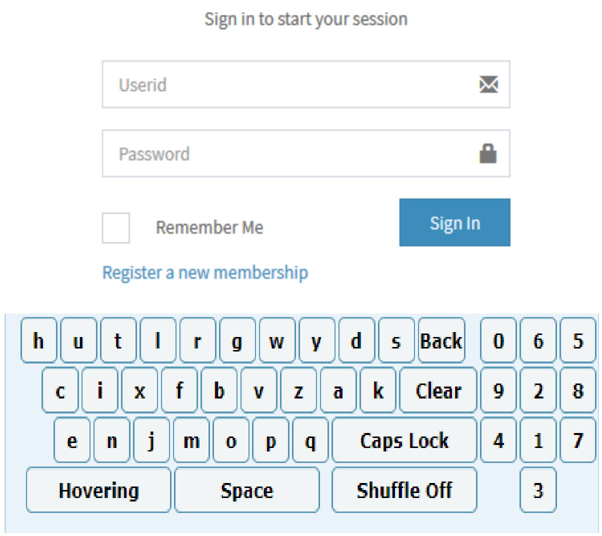
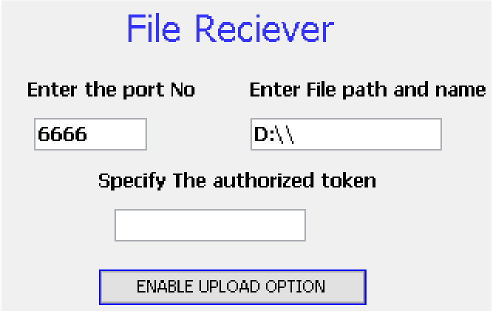

Sign in to start your session
Userid
Password
□ Remember Me
Sign In
Register a new membership
h u t l r g w y d s Back 0 6 5
c i x f b v z a k Clear 9 2 8
e n j m o p q Caps Lock 4 1 7
Hovering Space Shuffle Off 3

Fig. 14. Virtual key board provided to restrict Sql Injection

D. Simulation for encryption based and multiport based sender and receiver mechanism along with data compression during transmission

During simulation the random port no is get from the sender side after initializing by default port. In following simulation , the random port received from sender is shown. Then path of file where data to be received would be stored and token to decode data would be filled by user on receiver side.



Enter the port No: 6666

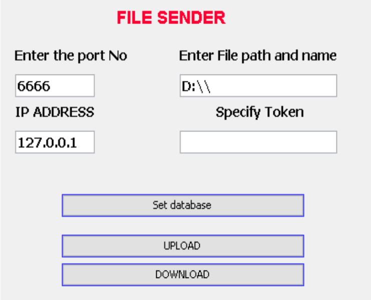
Enter File path and name: D:\\

Specify The authorized token:

Fig. 15. Simulation of receiver node

Similarly on sender side the sender would set the file name to be transferred and along with token to encode the data.

The IP address where data is to be transfered, is set. The data would be transferred by pre specified random port above 1023 as shown in following figure.



FILE SENDER

Enter the port No: 6666

Enter File path and name: D:\\

IP ADDRESS: 127.0.0.1

Specify Token:

Fig. 16. Simulation of sender node

VI. CONCLUSION

The proposed work is providing a scalable and flexible approach to perform intrusion detection considering the training model. The probability of error would be less while calculating overall accuracy as the proposed model has made use of a huge dataset for training and utilized the LSTM model with multiple layers. Moreover the propose research has provided approach to manage Sql injection. The multi port mechanism has also increased the reliability of data transmission in cloud environment.

VII. SCOPE OR RESEARCH

Research would play a significant role in predicting intrusion with high accuracy. Moreover the research is providing significant solution for sql injection. The concept of multiport would make the data transmission more reliable. The data compression mechanism used during data transmission in two nodes would support the security improvement.

Future research could have the benefit of rapid training from this research.

APPENDIX

It is optional. Appendixes, if needed, appear before the acknowledgment.

ACKNOWLEDGMENT

It is optional. The preferred spelling of the word "acknowledgment" in American English is without an "e" after the "g." Use the singular heading even if you have many acknowledgments. Avoid expressions such as "One of us (S.B.A.) would like to thank ... ." Instead, write "F. A. Author thanks " Sponsor and financial support acknowledgments are placed in the unnumbered footnote on the first page.

REFERENCES

1. Li, Peisong, and Ying Zhang. "A Novel Intrusion Detection Method for Internet of Things." In 2019 Chinese Control And Decision Conference (CCDC), pp. 4761-4765. IEEE, 2019.
2. Yin, Chuanlong, Yuefei Zhu, Jinlong Fei, and Xinzheng He. "A deep learning approach for intrusion detection using recurrent neural networks." Ieee Access 5 (2017): 21954-21961.
3. Dong, Bo, and Xue Wang. "Comparison deep learning method to traditional methods using for network intrusion detection." In 2016 8th IEEE International Conference on Communication Software and Networks (ICCSN), pp. 581-585. IEEE, 2016.
4. Ullah, Imtiaz, and Qusay H. Mahmoud. "A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks." In Canadian Conference on Artificial Intelligence, pp. 508-520. Springer, Cham, 2020.
5. Althubiti, Sara A., Eric Marcell Jones, and Kaushik Roy. "Lstm for anomaly-based network intrusion detection." In 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), pp. 1-3. IEEE, 2018.
6. Jianghong Wei, Wenfen Liu, Xuexian Hu, "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption". In JOURNAL OF LATEX CLASS FILES, VOL. 14, NO. 8, AUGUST 2015
7. S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.
8. X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," Computers, IEEE Transactions on, 2014, doi: 10.1109/TC.2014.2315619.
9. C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 468–477, 2014.
10. D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586– 615, 2003.
11. W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology–CRYPTO 1998. Springer, 1998, pp. 137–152.
12. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008, pp. 417–426.
13. K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloudbased revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Computer Security-ESORICS 2014. Springer, 2014, pp. 257–272.
14. Pratik H Sailor, Prof. Jaydeep Gheewala. "Detection and Prevention of SQL Injection Attacks", International Journal of Engineering Development and Research (IJEDR), ISSN: 2321-9939, Vol.2, Issue 2, and pp.2660-2666, June 2014, Available: http://www.ijedr.org/papers/IJEDR1402215.pdf
15. Tejinderdeep Singh Kalsi, Navjot Kaur, "Detection and Prevention Of Sql Injection Attacks Using Novel Method In Web Applications", Int J Adv Engg Tech/Vol. VI/Issue IV/Oct.-Dec.,2015/11-15, E-ISSN 0976-3945
16. Atefeh Tajpour, Suhaimi Ibrahim, Maslin Masrom, "SQL Injection Detection and Prevention Techniques" International Journal of Advancements in Computing Technology Volume 3, Number 7, August 201110.4156/ijact.vol3.issue7.11

AUTHORS PROFILE

Ms. Manju Sharma Research Scholar, University Institute of Engineering & Technology (UIET), Maharshi Dayanand University, Rohtak, Haryana, India. Overall 13 years of work experience in teaching and Solution Architect profession. Currently, pursuing PhD from Maharshi Dayanand University. Acquired M.Tech (Computer Science) degree from Vanasthali University, Rajasthan and B.Tech (Information Technology) degree with distinction from The Technological Institute Of Textile & Science, Bhiwani, Haryana. Areas of interest are Cloud Computing and security, hyperconverged solution and data protection & application archival solution design for on-premise Data Center infrastructure, public or private cloud including Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform.

Dr. Mukesh Kumar Sharma currently working as HOD & associate professor in the department of computer Engineering, The Technological Institute of Textile and Science, Bhiwani-127021 and received doing his Ph.D degree from M. D. University Rothak Haryana – India in 2012, M.Tech in Computer Science and Engineering from Guru Jambeshwer University of Science & Technology Hisar in 2004 and B.Tech .degree in Computer Science & Engineering from M. M. College of Engineering, Mullana (Kurushetra University, Kurukshetra) 2004. He is currently His area of interest is Adhoc Networks, Computer Networks, Cloud Computing and Network security. He has published various articles in International as well as National Journals. and presented many papers in national and International Conferences