Step 1: READ Source Bytes, Destination Bytes, logged in, dst_same_src_port_rate, dst_host_srv_diff_host_rate, dst_host_serror_rate, dst_host_srv_serror_rate, dst_host_same_srv_rate, dst_host_diff_srv_rate, dst_host_count, diff_srv_rate, same_srv_rate

Step 2: IF Source Bytes = 0 THEN GOTO Step 14

Step 3: Else IF Destination Bytes =0 THEN GOTO Step 14

Step 4: Else IF logged in =0 THEN GOTO Step 14

Step 5: Else IF dst_same_src_port_rate =0 THEN GOTO Step 14

Step 6: Else IF dst_host_srv_diff_host_rate =0 THEN GOTO Step 14

Step 7: Else IF dst_host_serror_rate =1 THEN GOTO Step 14

Step 8: Else IF dst_host_srv_serror_rate=1 THEN GOTO Step 14

Step 9: Else IF dst_host_same_srv_rate= 'fuzzy' THEN GOTO Step 14

Step 10: Else IF dst_host_diff_srv_rate ='fuzzy' THEN GOTO Step 14

Step 11: Else IF dst_host_count=255 THEN GOTO Step 14

Step 12: Else IF diff_srv_rate ='fuzzy' THEN GOTO Step 14

Step 13: Else IF same_srv_rate= 'fuzzy' THEN GOTO Step 14 Else GOTO Step 15

Step 14: Display the network traffic belongs to 'Attack' class

Step 15: STOP

But for the support and confidence calculated for other combinations with class= 'normal' or when class='normal' did not carry or reflect any meaningful information. Though those combinations had showed some interesting trend and pattern in training data set but during validation with the test data set the result has been deviated with large differences, hence could be considered for develop a general rule based on the findings from Training data set.

3.0 Conclusion:

This research work is a noble effort to develop a network intrusion detection system by understanding and using the concept of data mining. Association rule mining of data mining technique which was not used in wide extent for intrusion detection research will open a new idea and guide in the field of research in a new dimension. The graphical representation after analysing different features of the network traffic by calculating support and confidence reflects the findings very precisely and concisely. The rule that has been generated using [IF-THEN-ELSE] format can draw a conclusion to explain the behaviour of different features of network traffic which can cause network traffic intrusive.

Reference:

[1] Agrawal R, Imielinski T and Swami A (1993) Mining association rules between sets of items in large databases, in: Proceedings of the ACM SIGMOD Conference on Management of Data, Washington, DC: 207–216.

[2] Bhattacharjee M and Kalita P (2012) Application of Market Basket Analysis to Understand Students Career Options: A Study on Management Under Graduate at IU, Mzoram, Indian Journal of Marketing 42(4) :42- 49

[3] Hipp J, Guntzer U and Nakhaeizadeh G (2000) Algorithms for association rule mining - a general survey and comparison, in Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining: 58–64.

[4] Hipp J, Guntzer U and Nakhaeizadeh G, (2002) Data Mining of Association Rules and the Process of Knowledge Discovery in Databases, Advances in data mining : applications in E-commerce, medicine, and knowledge management Springer: 15-36

[5] Hussain J and Kalita P, (2015 a) Designing a Data Cube for NSL-KDD data set to improve the quality of network intrusion detection, Proceedings of ICFM 2015, March 26-28, Gauhati University, ISBN: 978-81-928118-9-5: 78-81

[6] Hussain J and Kalita P, (2015 b) Understanding Network Intrusion Detection System Using OLAP on NSL-KDD Dataset, IUP Journal of Computer Science, Jul 2015, Vol 9, Issue 3: 59-66

[7] Lee W and Stolfo SJ (1998), Data mining approaches for intrusion detection, in Proceedings of the 7th USENIX Security Symposium SECURITY-9: 79–94.

[8] Lee W, Nimbalkar RA,Yee KK, Patil SB, Desai, PS Tran TT and Stolfo SJ (2000 a) A data mining and CIDF based approach for detecting novel and distributed intrusions, in Proceedings of the 3rd International Workshop on Recent Advances in Intrusion Detection (RAID 2000): 49–65

[9] Lee W, Stolfo SJ and Mok KW (2000 b), Adaptive intrusion detection: a data mining approach, Artificial Intelligence Review 14: 533–567

[10] Patcha A and Park JM, (2007) An overview of anomaly detection techniques: Existing solutions and latest technology trends, Computer Networks 51:3448-3470

[11] Singhal A and Jajodia S (2006) Data warehousing and data mining techniques for intrusion detection system, Distributed parallel database, Springer

[12] Tsai FS, (2009) Network Intrusion Detection Using Association Rules, International Journal of Recent Trends in Engineering, 2:202-204

[13] Ziauddin, kammal S, Khan KZ and Khan M.I (2012) Research on Association Rule Mining, Advances in computational mathematics and its applications 2: 226-236