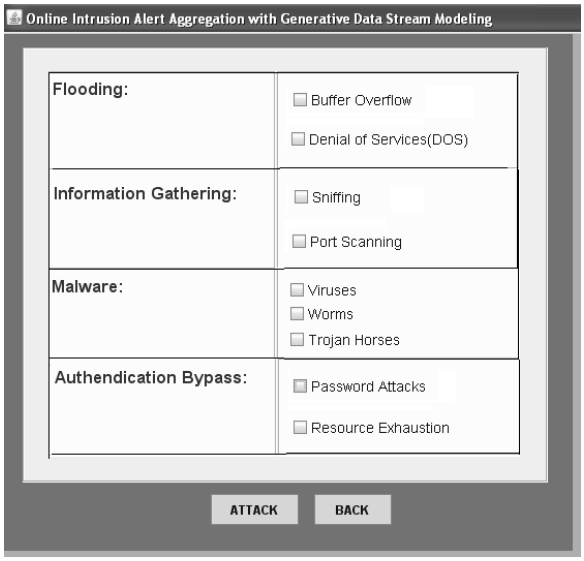

Figure 2: Different Types of Attacks may detected

As shown in figure different attacks can be simulated into information gathering, authentication failure, malwares, and flooding of data. Following is the GUI for alert aggregation

Figure 3: Simulation of Alerts

As shown in above figure there is separate space for each and every layers aggregation messages. When attack is done the relevant or appropriate action or message is displayed as shown in figure

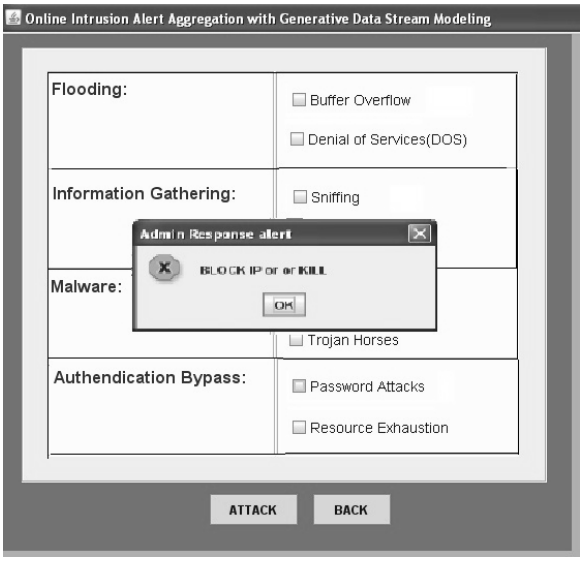

Figure 4: Response when attack is done

Alerts can be sent to users registered mobile as shown in figure.

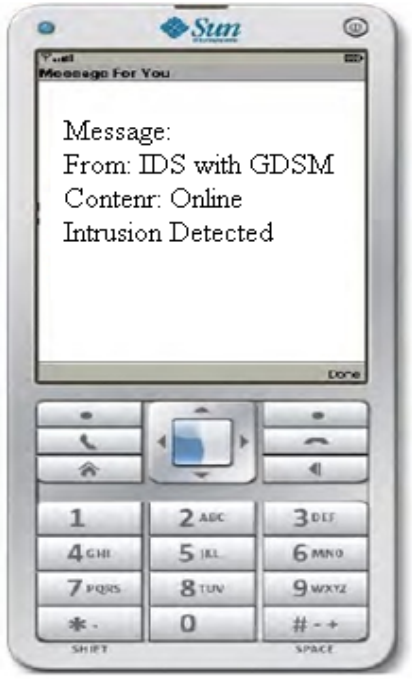

Figure 5: GUI of Mobile Alert

Once the alert is received on the mobile it can be processed by alert processing layer and reaction layer will suggest the way to handle the intruder. The action is also can be send to registered mobile as shown in below figure.

Licensed Under Creative Commons Attribution CC BY

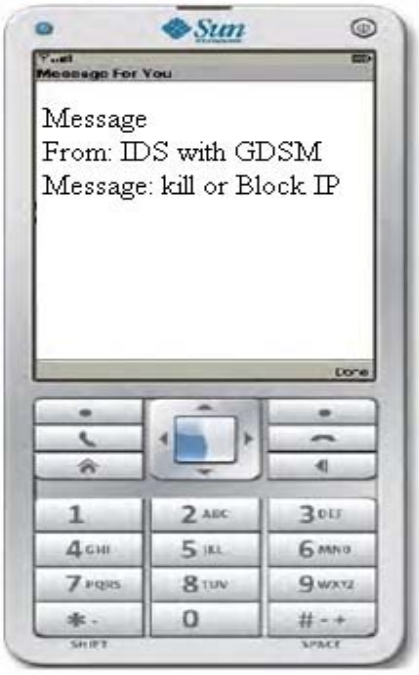

Figure 6: Relative action send by Reaction Layer

5. Conclusion

This paper suggests impressive way for online alert aggregation generation with generative data stream modeling. It has been implemented and it found that meta alerts can be generated effectively. Missing false positive rate gets decreased as it uses property of data streaming i.e. it executes a few times only before processed. The experimental result shows that it is very effective and helpful when it gets implemented in real time application. Also IDS accuracy gets increased very much. More alerts can be detected but compare to number of attacks detected very few false positive alerts gets introduced. So online intrusion alert aggregation with data streaming system is extremely efficient in information technology field to provide security to information.

References

[1] Kothawale Ganesh S., Borhade Sushama R., B. Raviprasad, "Online Intrusion Alert Aggregation with Generative Data Stream Modeling", International Journal of Modern Engineering Research IJMER | ISSN: 2249–6645 Vol. 4 | Iss.7| July. 2014 | 88.

[2] M. Hanock, K. Srinivas, A. Yaganteeswarudu, "Online Intrusion Alert Aggregation with Generative Data Stream Modeling",International Journal of Electronics and computer Science Engineering, ISSN-2277-1956

[3] S. Mangesh kumar, K. Mohan, G. Kadirvelu, S. Muruganandam, "Online Intrusion Alert Aggregation Through Mobile", International journal of advancement in Research and Technology, volume 1, issue3, August-2012

[4] Ravindra Bhat,"Intrusion Detection System with Data Stream Modeling using Conditional Privilages", International journal of computer science and technology, vol.3 no.7july 2012 ISSN:2299-3345

[5] Rupali Shewale, Yugandhar Pandey, Maheshkumar A. Sali, " Distributed Intrusion Alert Aggregation with Data Stream Modeling", International journal of electronics, communication and soft computing science and engineering, ISSN:2277-9477 March-2012

[6] Alexander Hofmann, Bernhard Sick, "Online Intrusion Alert Aggregation with Generative Data Stream Modeling", IEEE transaction on dependable and secure computing, vol 8 No. 2 March-April 2011.

[7] S. Axelsson, "Intrusion Detection Systems: A Survey and Taxonomy," Technical Report 99-15, Dept. of Computer Eng., Chalmers Univ. of Technology, 2000.

[8] M.R. Endsley, "Theoretical Underpinnings of Situation Awareness: A Critical Review," Situation Awareness Analysis and Measurement, M.R. Endsley and D.J. Garland, eds., chapter 1, pp. 3-32, Lawrence Erlbaum Assoc., 2000.

[9] C.M. Bishop, Pattern Recognitin and Machine Learning. Springer, 2006.

[10] M.R. Henzinger, P. Raghavan, and S. Rajagopalan, Computing on Data Streams. Am. Math. Soc., 1999.

[11] A. Allen, "Intrusion Detection Systems: Perspective," Technical Report DPRO-95367, Gartner, Inc., 2003.

[12] F. Valeur, G. Vigna, C. Kru¨ gel, and R.A. Kemmerer, "A Comprehensive Approach to Intrusion Detection Alert Correlation," IEEE Trans. Dependable and Secure Computing, vol. 1, no. 3, pp. 146-169, July-Sept. 2004.

[13] H. Debar and A. Wespi, "Aggregation and Correlation of Intrusion-Detection Alerts," Recent Advances in Intrusion Detection, W. Lee, L. Me, and A. Wespi, eds., pp. 85-103, Springer, 2001.

[14] D. Li, Z. Li, and J. Ma, "Processing Intrusion Detection Alerts in Large-Scale Network," Proc. Int'l Symp. Electronic Commerce and Security, pp. 545-548, 2008.

[15] F. Cuppens, "Managing Alerts in a Multi-Intrusion Detection Environment," Proc. 17th Ann. Computer Security Applications Conf. (ACSAC '01), pp. 22-31, 2001.

[16] A. Valdes and K. Skinner, "Probabilistic Alert Correlation," Recent Advances in Intrusion Detection, W. Lee, L. Me, and A. Wespi, eds.pp. 54-68, Springer, 2001.

[17] K. Julisch, "Using Root Cause Analysis to Handle Intrusion Detection Alarms," PhD dissertation, Universita¨ t Dortmund, 2003.

[18] T. Pietraszek, "Alert Classification to Reduce False Positives inIntrusion Detection," PhD dissertation, Universita¨ t Freiburg, 2006.

[19] F. Autrel and F. Cuppens, "Using an Intrusion Detection Alert Similarity Operator to Aggregate and Fuse Alerts," Proc. Fourth Conf. Security and Network Architectures, pp. 312-322, 2005.

[20] G. Giacinto, R. Perdisci, and F. Roli, "Alarm Clustering for Intrusion Detection Systems in Computer Networks," Machine Learning and Data Mining in Pattern Recognition, P. Perner and Imiya, eds. pp. 184-193, Springer, 2005.

[21] O. Dain and R. Cunningham, "Fusing a Heterogeneous Alert Stream into Scenarios," Proc. 2001 ACM Workshop Data Mining for Security Applications, pp. 1-13, 2001.

[22] P. Ning, Y. Cui, D.S. Reeves, and D. Xu, "Techniques and Tools for Analyzing Intrusion Alerts," ACM Trans. Information Systems Security, vol. 7, no. 2, pp. 274-318, 2004.

Licensed Under Creative Commons Attribution CC BY

[23] F. Cuppens and R. Ortalo, "LAMBDA: A Language to Model a Database for Detection of Attacks," Recent Advances in Intrusion Detection, H. Debar, L. Me, and S.F. Wu, eds. pp. 197-216, Springer,2000.
[24] S.T. Eckmann, G. Vigna, and R.A. Kemmerer, "STATL: An Attack Language for State-Based Intrusion Detection," J. Computer Security, vol. 10, nos. 1/2, pp. 71-103, 2002.
[25] A. Hofmann, "Alarmaggregation und Interessantheitsbewertung in einem dezentralisierten Angriffserkennungsystem," PhD dissertation, Universita¨t Passau, under review.
[26] M.S. Shin, H. Moon, K.H. Ryu, K. Kim, and J. Kim, "Applying Data Mining Techniques to Analyze Alert Data," Web Technologies and Applications, X. Zhou, Y. Zhang, and M.E. Orlowska, eds. pp. 193-200, Springer, 2003.
[27] J. Song, H. Ohba, H. Takakura, Y. Okabe, K. Ohira, and Y. Kwon, "A Comprehensive Approach to Detect Unknown Attacks via Intrusion Detection Alerts," Advances in Computer Science—ASIAN 2007, Computer and Network Security, I. Cervesato, ed., pp. 247-253, Springer, 2008.
[28] R. Smith, N. Japkowicz, M. Dondo, and P. Mason, "Using Unsupervised Learning for Network Alert Correlation," Advances in Artificial Intelligence, R. Goebel, J. Siekmann, and W. Wahlster, eds. pp. 308-31 , Springer, 2008.
[29] A. Hofmann, D. Fisch, and B. Sick, "Identifying Attack Instances by Alert Clustering," Proc. IEEE Three-Rivers Workshop Soft Computing in Industrial Applications (SMCia '07), pp. 25-31, 2007.
[30] M. Roesch, "Snort—Lightweight Intusion Detection for Networks," Proc. 13th USENIX Conf. System Administration (LISA '99), pp. 229-238, 1999.
[31] O. Buchtala, W. Grass, A. Hofmann, and B. Sick, "A Distributed Intrusion Detection Architecture with Organic Behavior," Proc. First CRIS Int'l Workshop Critical Information Infrastructures (CIIW '05), pp. 47-56, 2005.

Licensed Under Creative Commons Attribution CC BY