Crime Prediction and Intrusion Detection with IoT and Machine Learning

Anirudh Kumar Tiwari[1], Prof. (Dr.) Bhavana Narain[2]

Email ID: tiwarianirudh646@gmail.com,narainbhawna@gmail.com

Abstract

In this era of digitalization crime investigation and prediction is top and foremost necessity. An action or commission which constitutes an offence and is punishable by Law is called crime. It can be performed by individual or group .it can commit against government or private sector.it may be harm someone reputation, physical harm or mental harm crime can cause direct harm or indirect harm to whoever the victim is.

The purpose of our work is to design a prototype that helps the police in detecting crime locations. We have taken a condition that if any person is going somewhere and after seeing an accident, when the photo of that accident is taken then automatically it will be sent to nearest police Station. For this, it is necessary to have an application designed by us both in the sender and the receiver. This whole matter will directly connect the police with crime location which ease the police can reach that location. GPS will be used for location detection. In our work we have collected dataset with the help of digital camera which is attached with IoT device. In first part of our paper we have discussed the grounds of our work under introduction of crime, digital image processing, GPS and IoT. In second part of our work we have discussed the methodology of our work here sensor board, GPS setting has been discussed along with dataset. There is a number of data collection technologies in the IoT. The most widely used technology is the Wireless sensor network (WSN) uses multi-hopping and self-organization to maintain control over the communication nodes.
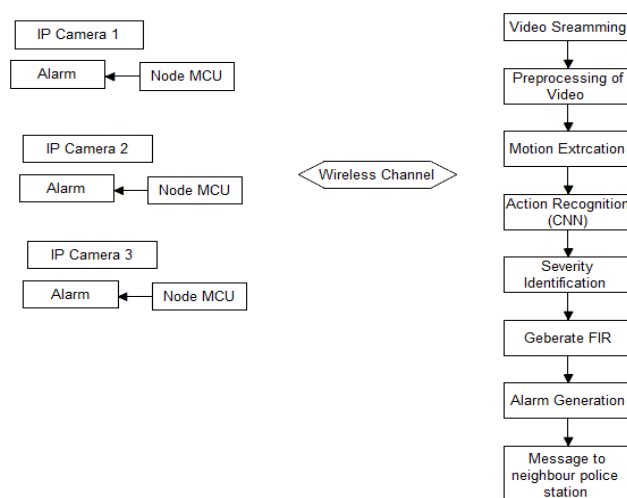
Figure 1. Flow Diagram of Workmodel

References

[1] Francisco Macia-Perez, Francisco J. Mora-Gimeno, Diego Marcos-Jorquera," Network Intrusion Detection System Embedded on a Smart Sensor", IEEE, 2010.

[2] Santosh Kumar Sahu, SauravranjanSarangi, Sanjaya Kumar Jena,"A Detail Analysis on Intrusion Detection Dataset", IEEE, © 2014, 978-1-4799-2572-8/14.

[3] Sravan Kumar Jonnalagadda, Ravi Prakash Reddy, "A Literature Survey and Comprehensive Study of Intrusion Detection", International Journal of Computer Applications, November 2013, 0975 – 8887, Vol. 81, No.16.

[4] Kai Peng, Victor C. M. Leung, and Qingjia Huang, "Clustering Approach Based on Mini Batch Kmeans for Intrusion Detection System Over Big Data", Special Section on Cyber-Physical-Social Computing and Networking, February 28, 2018, Digital Object Identifier 10.1109/ ACCESS.2018.2810267, Vol. 6, 2169-3536, 2018 IEEE.

[5] R. Vinayakumar, MamounAlazab, K. P. Soman, PrabaharanPoornachandran, Ameer Al-Nemrat, and SitalakshmiVenkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System", IEEE Access, April 11, 2019, 10.1109/ACCESS.2019.2895334. Vol.7, 2169-3536, 2019 IEEE.

[6] Longzhi Yang, Jie Li, Gerhard Fehringer, Phoebe Barraclough, Graham Sexton, Yi Cao, "Intrusion Detection System by Fuzzy Interpolation", 2017 IEEE international conference on fuzzy systems (FUZZ-IEEE), 2017, pp.1-6.

[7] BiswanathMukharjee, L. Todd Heberlein and Karl N. Levitt, "Network Intrusion Detection", IEEE Network, May/June 1994, 0890-8044/94/$0.4.00, © 1994.

[8] Clive Grace, "Understanding Intrusion Detection Systems", PC Network Advisor, www.itp-journals.com, September 2000, Issue 122, pp.11.

[9] Ahmed Awad E. Ahmed, and IssaTraore, "Anomaly Intrusion Detection based on Biometrics", 2005 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY, June 2005, ISBN 555555555, © 2005 IEEE.

[10] Robert Mitchell and Ing-Ray Chen, "A Survey of Intrusion Detection Techniques for Cyber-Physical Systems", ACM Computing Surveys, March 2014, Vol.46, No.4.

[11] Nasrin Sultana, Naveen Chilamkurti, Wei Peng, RabeiAlhadad, "Survey on SDN based network intrusion detection system using machine learning approaches", Peer-to-Peer Networking and Applications, https://doi.org/10.1007/s12083-017-0630-0, 12 January 2018.

[12] Christos Xenakis, ChristoforosPanos, IoannisStavrakakis, "A Comparative Evaluation of Intrusion Detection Architectures for Mobile Ad Hoc Networks", computer & security 30(1), 63-80, 2011.

[13] AbdelouahidDerhab, AbdelghaniBouras, Mustapha RedaSenouci, and Muhammad Imran, "Fortifying Intrusion Detection Systems in Dynamic Ad Hoc and Wireless Sensor Networks", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, December 2014, Article ID 608162, pp. 15, http://dx.doi.org/10.1155/2014/608162.

[14] kirtichoudhary, KomalDhing, ShivaniPacharne, SweetySamanta, Anujaphapale,"Hybrid Approach towards IDS IPS IRS using Reinforcement Learning", IJRECE, APRIL - JUNE 2019, Vol.7, ISSUE: 2, ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE).

[15] QuamarNiyaz, Weiqing Sun, Ahmad Y Javaid, and MansoorAlam, "A Deep Learning Approach for Network Intrusion Detection System", BICT 2015, December 03-05, New York City, United States, Copyright © 2016 ICST, DOI 10.4108/eai.3-12-2015.2262516.

[16] Chirag N. Modia, Dhiren R. Patela, AviPatelb, MuttukrishnanRajarajanb," Integrating Signature Apriori based Network Intrusion Detection System (NIDS) in Cloud Computing", 2nd International Conference on Communication, Computing & Security (ICCCS-2012), 6, 2012, 905 – 912.

[17] Hu Zhengbing, Li Zhitang,WuJunqi, "A Novel Network Intrusion Detection System(NIDS) Based on Signatures Search of Data Mining", e-Forensics 2008, January 21-23, 2008, Adelaide, Australia, © 2008 ICST 978-963-9799-19-6.

[18] Jihyun Kim, Jaehyun Kim, Huong Le Thi Thu, and Howon Kim, "Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection", International Conference on Platform Technology and Service, Deccember 31, 2015

[19] V. Jyothsna, V. V. Rama Prasad, "A Review of Anomaly based IntrusionDetection Systems", International Journal of Computer Applications, September 2011, 0975 – 8887, Vol. 28, No.7.

[20] Abhishek Das, David Nguyen, Joseph Zambreno, GokhanMemik, and AlokChoudhary, "An FPGA-Based Network Intrusion Detection Architecture", IEEE Transactions on Information Forensics and Security, March 2008, Vol. 3, NO.1.

[21] Chuanlong Yin, Yuefei Zhu, JinlongFei, Xinzheng He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks", IEEE Access, 2169-3536, 2017 IEEE, Vol. 5, 2017.

[22] Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, Kuang-Yuan Tung, "Intrusion detections system A comprehensive review", Journal of Network and Computer Applications 36, Accepted 11,September 2012, Available online 23, September 2012, 16–24.

[23] Mehdi HosseinzadehAghdam, and PeymanKabiri, "Feature Selection for Intrusion Detection System Using Ant Colony Optimization", International Journal of Network Security, May 2016, Vol.18, No.3, PP.420-432.

[24] RenHui Gong, Mohammad Zulkernine, PurangAbolmaesumi, "A Software Implementation of a Genetic Algorithm Based Approach to Network Intrusion Detection", ACIS International Workshop (IEEE), 2005, 0-7695-2294-7/05 $20.00, © 2005.

[25] Wei Lu and IssaTraore, "Detecting New Forms of Network Intrusion using Genetic Programming", Computational Intelligence, 2004, Vol. 20, No. 3.

[26] B. M. Aslahi-Shahri, R. Rahmani, M. Chizari, A. Maralani, M. Eslami, M. J. Golkar, A. Ebrahimi," A hybrid method consisting of GA and SVM for intrusion detection system", Neural Comput&Applic, 30 July 2015, DOI 10.1007/s00521-015-1964-2

[27] ManoranjanPradhan, Chinmaya Kumar Nayak, Sateesh Kumar Pradhan," Intrusion Detection System (IDS) and Their Types", IGI Global, Copyright © 2016, DOI: 10.4018/978-1-4666-8761-5.ch009.

[28] Elike Hodo, Xavier Bellekens, Andrew Hamilton, Christos Tachtatzis and Robert Atkinson,"Shallow and Deep Networks Intrusion Detection System: A Taxonomy and Survey", arxiv preprint arxiv:1701.02145, 2017.

[29] Xuhang Ying, Sang UkSagong, Andrew Clark, Linda Bushnell, and RadhaPoovendran, ,"Shape of the Cloak: Formal Analysis of Clock Skew-Based Intrusion Detection System in Controller Area Networks",IEEE Transactions on Information Forensics and Security, 24 Jan 2019.

[30] ShadiAljawarneh, MontherAldwairi, MuneerBaniYassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model", Journal

of Computational Science, 2017 http://dx.doi.org/10.1016/j.jocs, 2017.03.006, 1877-7503/© 2017.

[31] T. Shekari, C. Bayens, M. Cohen, L. Graber, and R.Beyah, "RFDIDS: Radio Frequency-based Distributed Intrusion Detection System for the Power Grid", Network and Distributed Systems Security(NDSS), 2019, 24-27 February 2019, San Diego, CA, USA, ISBN 1-891562-55-X.

[32] Herve Debar, Marc Dacier, Andreas Wespi, "Towards a taxonomy of intrusion-detection systems", Computer Networks 31, 1999, 805–822.

[33] Tapiwa M. Chiwewe, Colman F. Mbuya, Gerhard P. Hancke, "Using Cognitive Radio for Interference-Resistant Industrial Wireless Sensor Networks: An Overview", Telecommunications Engineering for the Information Society (CeTEIS), South Africa, September 20, 2015, Pp.13, 0799.

[34] Martin Botha &Rossouw von Solms, "Utilizing Neural Networks For Effective Intrusion Detection", ISSA, 1-15, 2004.

[35] Florian Sagstetter, Martin Lukasiewycz, Sebastian Steinhorst, Marko Wolf, AlexandreBouard, William R. Harris, SomeshJha, Thomas Peyrin, Axel Poschmann, SamarjitChakraborty, "Security Challenges in Automotive Hardware/Software Architecture Design", 2013 design, automation & test in Europ conference & exhibition , 458-463, 2013.

[36] SriramSundarRajan, Vijaya Krishna Cherukuri, "An Overview of Intrusion Detection Systems", pdfs.semanticscholar.org, may, 2010.

[37] Stefan Axelsson, "Combining a Bayesian Classifier with Visualisation: Understanding the IDS", VizSEC/DMSEC'04, October 29, 2004, Washington, DC, USA, ACM, 2004 1581139748/04/0010.

[38] TejvirKaur, VimmiMalhotra, Dr. Dheerendra Singh," Comparison of network security tools-Firewall, Intrusion Detection System and Honeypot", International Journal of Enhanced Research in Science