Significance of Intruder Detection Techniques in the Context of Industry 4.0

M. B. Kiran
Associate Professor,
Department of Mechanical Engineering,
School of Technology,
Pandit Deendayal Petroleum University,
Gandhinagar, Gujarat-382007- INDIA
Kiranm.bhaskar@gmail.com

Abstract

With the advent of Industry 4.0, many physical systems are transforming into cyber-physical systems (CPS). As these CPS are connected to the internet, have a lot of vulnerabilities. There is a need to protect them from cyber-attacks. This is true across domains. Many cyber-attacks are being reported in the literature. These cyber-attacks had devastating effects. The cyber-attacks not only result in an economic loss but also resulted in the loss of effort and inconvenience. Hence a complete understanding of the type of cyber-attacks and predicting the behavior of intruders is very much important for protecting CPS. Though many cyber-attacks are reported across multiple domains, the type of attacks is unique about each domain. This makes solving security problems even more difficult. What is also observed from the literature review is that the security infrastructure that is available today may not be secure for tomorrow. This clearly shows the complexity of solving the security problems- Intrusion detection system(IDS). Hence, an effort has been made in this work to consolidate different types of attacks reported across multiple domains. This is valuable not only for academicians but also for researchers and practitioners, as this paper contains not only the work reported so far but also provides future directions for promoting further research in the area of intruder detection.

Keywords

CPS, Industry 4.0, Big Data, Intruder detection, Intruder Prevention

1.Introduction

The main objective of designing an IDS) is to identify all types of suspicious network related traffic that cannot be identified by a normal firewall. Normally an IDS is consisting of components such as Console, Sensors, and Detection engine. Many industrial applications use different types of IDS. Different type of IDS differs by the type of sensors used, position of these sensory devices and the method used for the generation alarms by the detecting engine. Security-based solutions can be of two types- prevention-based methods and detection-based methods. Prevention-based methods use encryption and authentication as means of protecting against possible attacks. Detection-based methods are used when prevention methods fail. The detection methods are -Signature detection (Figure 1)- This technique use known patterns for detecting malicious traffic; Anomaly detection (Figure 2) - These detection techniques are designed in such a way that they can detect abnormal behavior in the system; Hybrid methods combine one or more methods. Certain type of IDS is passive in that security breach will be detected by an IDS sensor and the event is logged and will be reported on the console. In an intrusion prevention system, known as reactive systems, the IDS sensor will respond to the malicious work either by resetting the connection or by recoding the firewall, to block the network traffic from the suspicious source. A worm is any malicious code that can replicate and spread on its own. A worm in the first step scans the given network for identifying any vulnerabilities. Then, the worm will exploit the weakness and finally attacks the network.

An attempt has been made, in the following paragraphs, to capture not only the different types of cyber-attacks but also the techniques used for implementing intruder detection in different domains. Also, future research directions are provided for interested academicians, practitioners, and researchers.

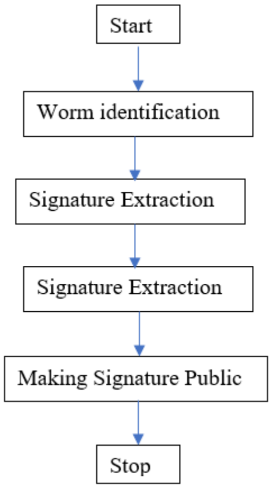

Figure 1, Signature detection process

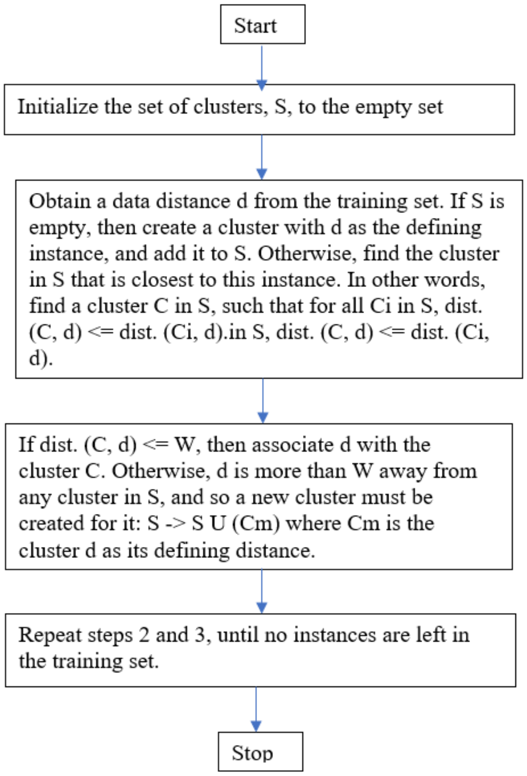
Start
Initialize the set of clusters, S, to the empty set
Obtain a data distance d from the training set. If S is empty, then create a cluster with d as the defining instance, and add it to S. Otherwise, find the cluster in S that is closest to this instance. In other words, find a cluster C in S, such that for all Ci in S, dist. (C, d) <= dist. (Ci, d).in S, dist. (C, d) <= dist. (Ci, d).
If dist. (C, d) <= W, then associate d with the cluster C. Otherwise, d is more than W away from any cluster in S, and so a new cluster must be created for it: S -> S U (Cm) where Cm is the cluster d as its defining distance.
Repeat steps 2 and 3, until no instances are left in the training set.
Stop

Figure 2 Anomaly Detection Algorithm

2 Literature Review

2.1. Smart Grids

Many researchers in the recent past have been working on protecting smart grids (Figure 3) by using wireless networks. Smart grids have been used for (i) power generation(ii) power transmission (ii) power distribution (iii) power utilization (iv) power monitoring and protection

Many researchers have proposed techniques for protecting smart grids. With the advent of Internet and ICT smart grids are becoming more efficient. Smart grids can be protected by (1) Protection (2) Detection and (3) Mitigation.

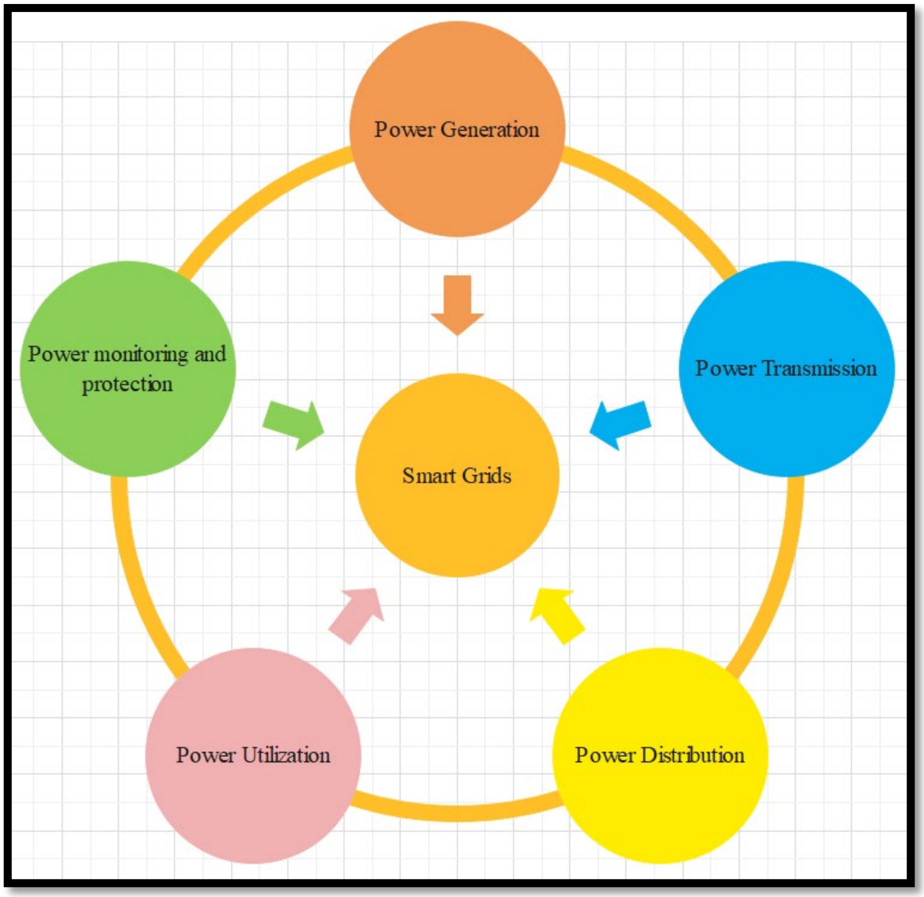

Figure 3. Elements of a Smart Grid

One of the techniques used for protecting cyber-physical smart grids is encrypted communication channels (Saxena et al. 2016). The most commonly used detection mechanism is a statistical-based method (Yan et al. 2017) and non-statistical based methods (Kurt et al. 2018). In these techniques, both space related and time related characteristics of the system are used for detecting cyber threats. Most cyber-physical smart grids are also provided with mitigation efforts for achieving a compromise between the system and the attacker to reduce the undesired impacts of cyber-attacks (Tan et al. 2019). Sequential optimization is normally used to achieve the objectives. Many of these techniques have assumed fixed behavior from different attackers. This is a very unrealistic assumption. Cyber-attacks do vary from attacker to attacker. One of the biggest challenges in designing a system against cyber-attacks is that the attacks vary continuously from time to time (Wang et al. 2018, Agarwal et al. 2018, Chastikova et al. 2017, Chen et al.2014, Desnitsky et al 2016, Floreano et al. 2015, Kotenko et al. 2016, Kotenko et al. 2018, Kuliev et al. 2017, Mac et al. 2016, Nojmol 2014, Perez 2018, Pshihov et al. 2018, Rogers 2015, Singh et al. 2017, Vatamaniuk et al. 2015, Yang et al. 2016).

2.2 Nuclear power plants

Physical protection of nuclear power plants (Fennelly 2016, Garcia 2005, Garcia 2007, Hochreiter 1997) serves as the first defense against physical intrusion. Detailed guidelines are defined by nuclear regulatory authorities. Host-based intruder detection systems (HIDS) are (Figure 4) increasingly used in nuclear power plants. HIDS consists of different types of sensors (e.g., microwave sensors, electric field sensors, infra-red sensors, etc.) for detecting intruders as well as isolating the system from the outside. Earlier intruder detection systems required human intervention. These systems are limited by the capability of human operators. With the advent of vision systems, many researchers have started solving intruder detection systems and have successfully demonstrated intruder detection, classification, and tracking. Many researchers have used both optical and thermal cameras for acquiring images for subsequent processing by intelligent intruder detection systems. This is because optical cameras have the difficulty in detecting intruders during night times and also when the intruder is not looking different from the background.

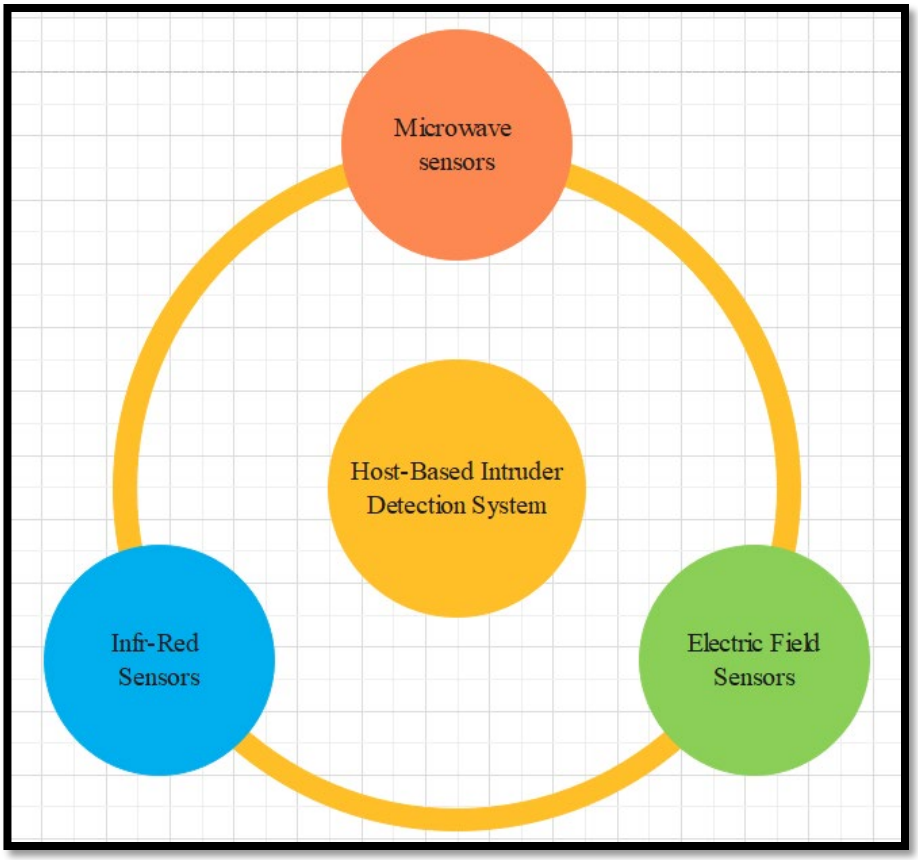

Figure 4. Sensors used in Host-based Intruder detection System

2.3 Camera system

Literature has reported using SAMSUNG SCO-2120R optical camera, in addition to a thermal camera. Literature has also reported using a network video server (Figure 5) fitted with an IP filtering function for joining a network. To overcome tangential distortion due to the manufacturing process, Zhang (2000) proposed a calibration algorithm. In his research work, 26 chessboard images are taken from different perspectives for Camera calibration. In his research, the camera calibration algorithm computes distortion coefficients using the chessboard images. Then these coefficients are used for correcting camera distortion using the OpenCV function (Bradski et al. 2008). Different cameras used in a camera system would help in providing the different views or perspectives of a 3D object. Thus, all the views would complement each other in identifying a 3D object. In a 3D object recognition system, the accuracy of object recognition is very important. Many researchers have been contributed for 3D object recognition. However, the robustness of the object recognition is not very robust and this is to be addressed for making the object recognition system very effective.

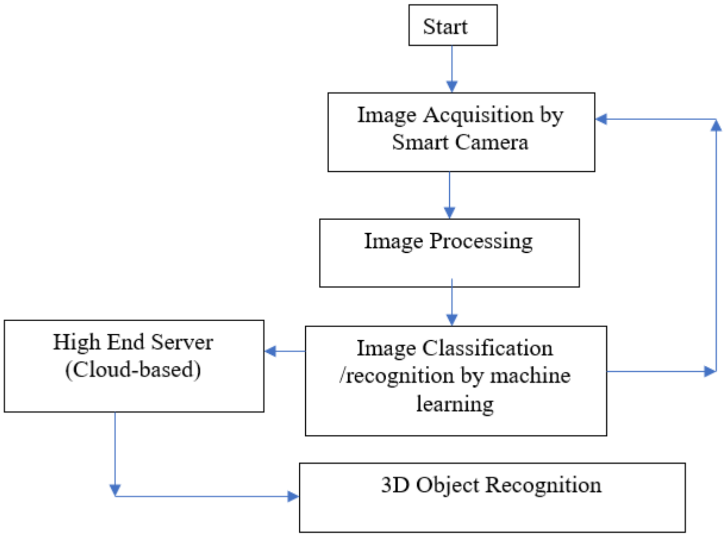
Start
Image Acquisition by Smart Camera
Image Processing
Image Classification /recognition by machine learning
High End Server (Cloud-based)
3D Object Recognition

Figure 5. Working principle of a Camera Network

2.4 Virtual Fence

It is an imaginary line that differentiates the system or protected area from its surroundings. This can be set up by using a spline curve. The controlling points of the spline curve are set up by using the coordinates given by the operator. The operator normally uses a GUI for feeding the coordinates.
The cubic spline function connecting two points (x_i, y_i) and (x_{i+1}, y_{i+1}) is given below.

$$P(x) = a_i(x - x_i)^3 + b_i(x - x_i)^2 + c_i(x - x_i) + d_i \qquad (1)$$

Intrusion detection is very much significant in the surveillance system. It is capable of identifying moving objects entering into the focus area defined by the virtual fence. The system is also capable of detecting moving objects in real-time.

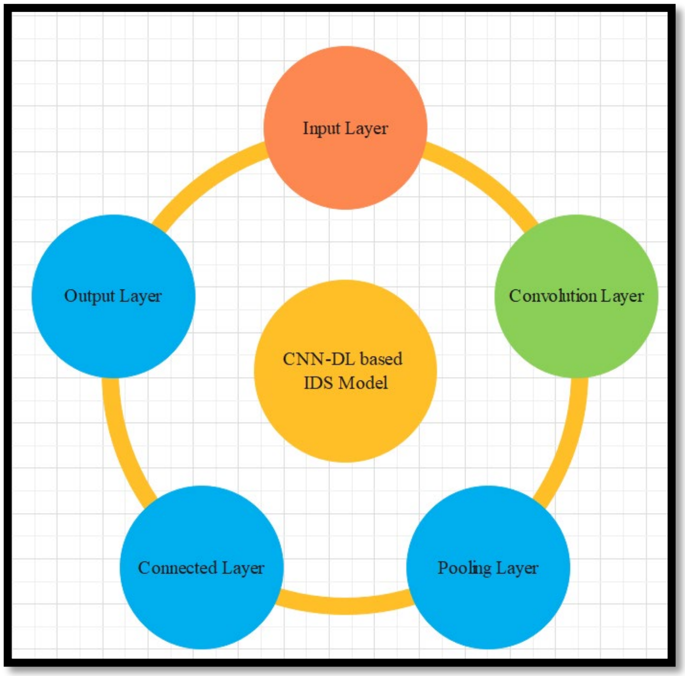

Figure 6 CNN-DL based Intruder detection model

During intruder detection, the moving object is classified as humans or animals. Le Cun et al. (2015) used deep learning for classifying moving objects. The Convolution Neural Network (CNN) (Figure 6) is also a type of deep learning algorithm. CNN does learn from the coefficients of the convolution filter uses relevant features for classifying images. Seung Hyun Kim et al. (2018) have proposed a CNN-based intruder detection algorithm for classifying moving objects. In their research work, they used six convolution layers. The detection algorithm extracts a feature that is unique for a given image. They used a training image database of ten categories of human intruders as well as animals. The training database consisted of 5000 images in each class. Thus, there were 50000 images. Most of the intruder detection is done using the OpenCV library and Caffe (Jia et al. 2014).

One researcher has implemented a virtual fence utilizing a graphical user interface. A virtual fence will differentiate areas under surveillance from external areas. One research work (Jia et al. 2014) has been reported to have identified the moving objects in the background by using a convolution neural network (CNN). The researcher also tried to classify moving objects like animals or intruders. The HIDS are normally designed in such a way that whenever an intruder is detected while crossing the virtual fence, an alarm is prompted. It was reported in one research work that a Virtual fence was implemented as a spline curve (Knott, G.D., 2012) having control points defined using a graphic user interface by an operator. In another research, deep learning was used for classifying moving objects. Deep learning (LeCun et al. 2015) was implemented using a computational model consisting of many layers. Particle filters are used for intruder behavior identification. A particle filter is a simulation-based technique. It uses Bayesian probability distribution. It gives good results not only for linear but also for non-linear environments.

One of the objectives of Intruder detection is to increase the accuracy of intruder identification. To address the limitations of HIDS, a researcher has proposed an intelligent intruder detection system that will improve the reliability and efficiency ID in nuclear power companies. This scheme makes use of two cameras and deep learning technologies for tracking intruder behavior detection.

2.5 Cross border intruder detection

Jagdish et al. (2016) have explored border intruder detection in hilly regions and dark environments. To protect from intruders, video surveillance systems are increasingly being used. This way researchers have demonstrated identifying suspicious activities. But these systems have certain limitations. Though the sensors used for intruder detection, along the border, work well they sometimes give false alarms to the security personnel. This may be due to the intrusion by wild animals or foliage. This shows that not only intruder detection is important but also intruder classification is equally important. Identifying human intruders is very difficult because of their dresses, sizes, and heights. Vittal et al. (2010) in their research used thermal cameras for intruder detection. These thermal cameras were connected to an image processing system. During operation, these thermal cameras are used to scan the border area and send images to the digital image processing system. By using the images, the system detects intruders. The system however has a limitation in that it cannot differentiate between animals and human intrusions. Barry et al. (2007) have used radar systems for intruder detection (Figure 7).

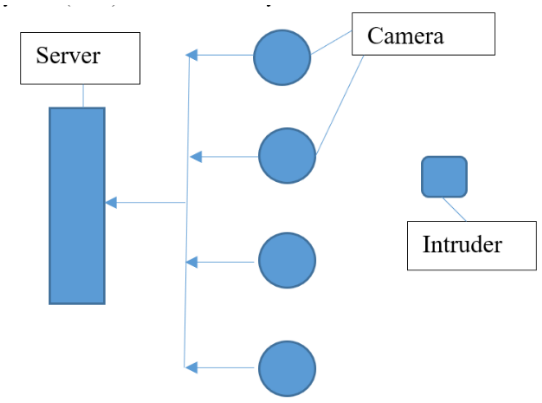

Figure 7 Working configuration of Intruder detection system

Literature shows that many researchers have started using Microsoft Kinect for human intruder detection as it is readily available and provides depth information about the human body (Bengalur et al. 2013, Pisharady et al. 2013, Raheja et al. 2011). Jagadish Lal Raheja et al. (2015) have used Microsoft Kinect, which uses an SDK, an infra-red camera for human intruder detection. They extracted skeletal images of humans during human intruder detection. This approach does not require any illumination. Also, the authors have claimed very high recognition rates (88.33%) in intruder detection. They have suggested that improved training would result in improved classification. They have also claimed that improved accuracies are obtained in the case of walking and bending.

Multi-wavelength laser scanning techniques are being used for the classification of materials with camouflage. The material may have multiple patterns embedded in the fabric (Kavitha et al. 2012). They used specimens consisting of leaf, black fabric, wood, PVC material, the bark of wood in testing their prototype. In the experimental setup, they had used a CCD camera, laser module, and optical system. Their experimentation results indicate that the prototype system is capable of discriminating camouflage materials at a distance of 6 meters. They had measured spectral response from camouflage materials. They measured slope values of spectral responses of different materials which served as discriminating features for classifying materials with camouflage.

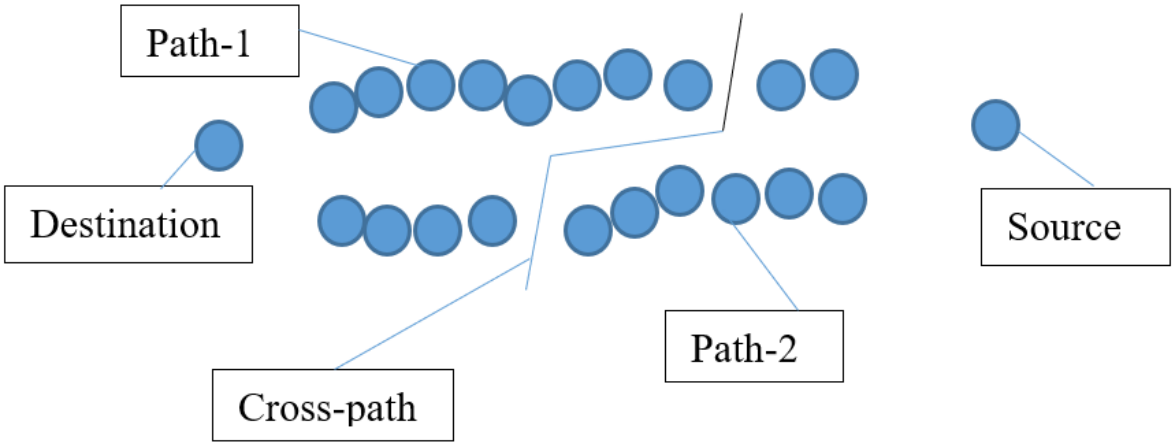

Figure 8 Vulnerabilities in a wireless network

Suvendu Kumar et al. (2016) have designed a barrier coverage algorithm by using microwave sensors and directional camera sensors, to identify the intruder. Here, microwave sensors are used for detecting the movement of an intruder (Figure 8). When the sensors are installed along the borderline, a vast amount of data will be generated and this cannot be handled by a traditional database platform. In this context, Big data analytics will become very useful. Big data would help in handling volume, variety, velocity, and value. A big data system is also capable of handling unstructured data generated by camera sensors. Here velocity means speed of data creation by camera sensors. Here, variety refers to the different format data coming from heterogeneous sensors. Here, value means useful information that can be extracted by data.

Many researchers have been working on barrier construction algorithm (Dean et al. 2008; Hoseini et al. 2012). The main limitation of these techniques is that they take more time for detecting intruders.

2.6 Big-Data-based architecture for Intruder detection.

The architecture consists of the following layers (Figure 9): Wireless network layer: The layer where sensors were deployed for data collection from barrier from time to time; Big data analytics and storage layer: Provides the support for performing processing, analysis of huge data as well as helping in the detection of intruders; Cloud layer: provides facility for storage for huge data with scalability and fault tolerance.

Researchers have claimed that this architecture achieves efficient results regarding analysis, storage, and also performance in intruder detection. The researchers have also studied the performance of a system using the CloudSim simulator. The researchers have also studied the effect on storage cost by using the number of servers ranging from

30-50. When the size of data, coming from camera sensors, increases, using a single server will take more data processing time. In such scenarios, it is advisable to go for the parallel processor. The size of the data may be as huge as 100GB. Researchers have used spark workstations fitted with the graphic processing unit. It is also observed that packet size will also influence the processing performance of data centers. Researchers have also studied throughput by having the number of servers. Researchers have also studied the %CPU utilization with data size and the number of data centers. It was observed that for a given data size, increasing the number of data centers will bring down the %CPU utilization, due to over distribution. Many researchers have worked on storage cost optimization. It is also observed that by using both CPU and GPU the processing time can be 18.6 faster compared to only the SPARK platform.

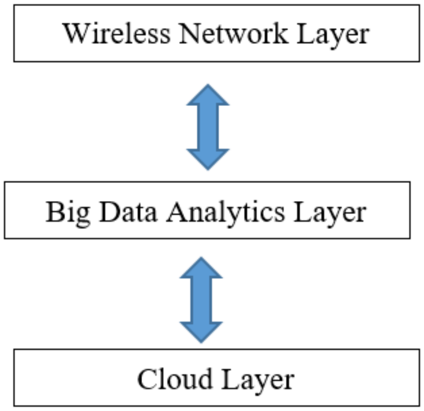

Figure 9. Big Data-based IDS architecture

Thus, it is seen how Big data analytics help in the processing of huge data coming from camera sensors. It is also seen that Big data analytics is responsible for processing and analyzing the data for detecting intruders. Researchers have developed schemes for detecting intruders with increased accuracy. Thus, it minimizes the occurrence of false alarms. It is also observed that the Intruder data is stored in the cloud for future reference. It is also shown how 24X7 border surveillance is made possible by using camera sensors and Big data analytics. The minimum classification accuracy of intruder detection and animal is reported is 90% and 72% respectively, when related to AlexNet (Krizhevsky et al. 2012). The minimum classification accuracy of intruder detection and animal is reported is 93% and 80% respectively, when compared to Google Net (Szegedy et al. 2015).

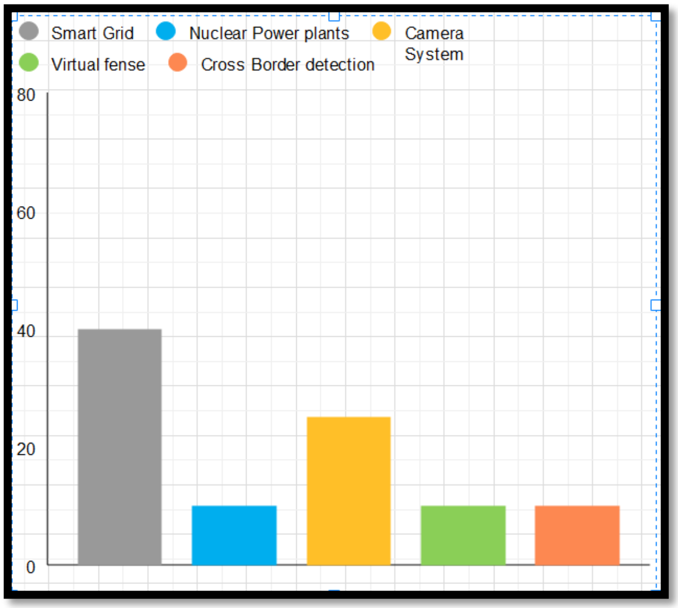

Figure 10. The relative progress of research in different domains about intruder detection

3 Conclusion

With the advent of Industry 4.0, many types of equipment used in manufacturing and other domains are being transformed into cyber-physical systems. These cyber-physical systems are highly vulnerable to cyber-attacks. As they are exposed through the internet. Thus, they require protection from cyber-attacks. Many researchers have been working on intrusion detection techniques for protecting these cyber-physical systems. The types of cyber-attacks are unique to each domain. Hence, an attempt is made in this research work to portray the different cyber protection schemes implemented in (i) Smart Grids (ii) Nuclear Power Plants (iii) Cross Border Intruder detection. Figure 10 shows the research progress in different domains about intruder detection. As can be seen from figure 10, much work has been done in the area of smart grids. Much work remains to be done in other areas. With the advent of Big-data analytics and cloud-based wireless sensor networks, data capture, data storage, analysis, and decision making have become more efficient. Researchers have claimed that this architecture achieves efficient results regarding analysis, storage, and also performance in intruder detection. The researchers have also studied the performance of the system using the CloudSim simulator. The researchers have also studied the effect on storage cost by using the number of servers ranging from 30-50. One of the objectives of Intruder detection is to increase the accuracy of intruder identification. To address the limitations of HIDS, a researcher has proposed an intelligent intruder detection system that will improve the reliability and efficiency of IDS in nuclear companies. This scheme make use of two cameras and deep learning technologies for tracking intruder behavior detection. When the size of data, coming from camera sensors, increases, using a single server will take more data processing time. In such scenarios, it is advisable to go for the parallel processor. The size of the data may be as huge as 100GB. Researchers have used spark workstations fitted with the graphic processing unit.

Most cyber-physical smart grids are also provided with mitigation efforts for achieving a compromise between the system and the attacker to reduce the undesired impacts of cyber-attacks Sequential optimization is normally used to achieve the objectives. Many of these techniques have assumed fixed behavior from different attackers. This is a very unrealistic assumption. Cyber-attacks do vary from attacker to attacker. One of the biggest challenges in designing a system against cyber-attacks is that the attacks vary continuously from time to time. Though many researchers have been working, over the years, in designing effective intruder detection algorithms, much work needs to be done in enhancing the security level offered by intruder detection schemes. Also, it is observed that there is a need to improve the detection accuracy, detection speed, and robustness of the detection algorithms. Also, there is a need for further reduction in the costs of hardware such as thermal camera and Vision camera to make the intruder detection system more economical. This would enable the Intruder detection schemes to be used in other domains as well. As of today, Intruder detection systems are being used only in few domains. There is a wide scope for implementing intruder detection systems in aerospace, shipbuilding, construction, hospitals, agriculture, textiles, banking, and other non-manufacturing industries as well. There is a wide scope for using a heterogenous swarm of cyber-physical systems for both intruder detection as well as monitoring the intruders. There is also a wide scope of using robotic swarms for monitoring and detecting intruders. The trend is intellectualization and integration with multiple sensors to enhance the overall security of the cyber-physical system.

To meet the security-related challenges of today's industries, there is a need for designing and developing a heterogenous swarm of cyber-physical systems, for comprehensively understanding the state of the given system. Also, there is a wide scope for introducing the evolutionary features inherent in the biological systems. Thus, interested researchers may use an artificial intelligence-based heterogeneous swarm of cyber-physical systems, for addressing or addressing the security problems of industries. Many use cases will have to be demonstrated by researchers regarding crisis management and monitoring industrial premises by using robotics swarms.

Acknowledgment: The author would like to express his sincere thanks to the management of Pandit Deendayal Energy University (PDEU), for providing the necessary infrastructure and timely support.

References

Agarwal, P., Gupta, A., Verma, G., Verma, H., Sharma, A., Banarwal, S., Wireless Monitoring and Indoor Navigation of a Mobile Robot Using RFID. In Nature Inspired Computing, 83-90. Springer, Singapore, 2018.

Barry, A.S., Mazel, D.S., The Secure Perimeter Awareness Network (SPAN) at John F. Kennedy International Airport, Security Technology, 41st Annual IEEE International Carnahan Conference on. IEEE. 2007.

Bradski, G., Kaehler, A., Learning OpenCV: Comput. Vision with the Open CV Library. O'Reilly Media, Sebastopol, CA, USA., 2008.

Chastikova, V, Zherlitsyn, S., The research of the Gray Wolf Optimizer (GWO) algorithm, Scientific works of KubSTU, vol. 16, pp. 136-142, 2016.

Chastikova, V., Malykhina, M., Zherlitsyn, S., Volya, Y., Comparative analysis of some swarm intelligence algorithms with detection of network attacks using neural network methods, Scientific journal of KubSAU, vol. 129, pp. 106-115, 2017.

Chen, Z., Jia, X., Riedel, A., Zhang, M., A bioinspired swimming robot, 2014 IEEE International Conference on Robotics and Automation (ICRA), Hong Kong, pp. 2564-2564, 2014.

Dean J, Ghemawat S., MapReduce: simplified data processing on large clusters., Communications ACM, pp. 107–13, 2008.

Desnitsky, V., Chechulin, A., Kotenko, I., Levshun, D., Kolomeec, M., Combined Design Technique for Secure Embedded Devices Exemplified by a Perimeter Protection System, SPIIRAS Proceedings, vol. 48, pp. 5-31, 2016.

Fennelly, L., 2016. Effective Physical Security. Butterworth-Heinemann, Amsterdam.,2008.

Floreano D., Wood R. J., Science, technology and the future of small autonomous drones. Nature, vol. 521, pp. 460-466, 2015.

Garcia, M.L., Design and Evaluation of Physical Protection Systems, Butterworth-Heinemann, Amsterdam.,2007.

Garcia, M.L., Vulnerability assessment of physical protection systems, Butterworth-Heinemann, Amsterdam.,2005.

Hochreiter, S., Schmidhuber, J., Long short-term memory. Neural Computing, vol. 9, no.8, pp.1735–1780, 1997.

Hoseini, S.M., Dehghan, M., Pedram, H. 2012. Full angle coverage in visual sensor networks. In: 2nd International e Conference on Computer and Knowledge Engineering (ICCKE), pp. 260–265, 2012.

Jagdish Lal Raheja, Swati Deora, Ankit Chaudhary, Cross border intruder detection in hilly terrain in dark environment, Optik, vol. 127, no. 2, pp. 535-538, 2016.

Jia, Y., Steelhammer, E., Donahue, J., et al., 2014. Caffe: An open-source convolutional architecture for fast feature embedding. In: Proceedings of the 22nd ACM International Conference on Multimedia, pp. 675-678, 2014.

Kavitha Venkataraayan, Sreten Askraba, Kamal E. Alameh, Clifton L. Smith, 2012, Multi-wavelength laser sensor for intruder detection and discrimination, Optics and Lasers in Engineering, vol. 50, no. 2, pp.176-181, 2012.

Knott, G.D., Interpolating Cubic Splines. Springer Science & Business Media, DE. Krizhevsky, A., Sutskever, I., Hinton, G. E., ImageNet classification with deep convolutional neural networks. In: Advances in Neural Information Processing Systems, pp.1097-1105, 2012.

Kotenko, I., Levshun, D., Chechulin, A. Event correlation in the integrated cyber-physical security system, 2016 XIX
IEEE International Conference on Soft Computing and Measurements (SCM-2016), IEEE, St. Petersburg, Russia, 484-486. 2016.

Kotenko, I., Saenko, I., Kushnerevich, A. (2018) Architecture of the Parallel Big Data Processing System for Security Monitoring of Internet of Things Networks, SPIIRAS Proceedings, vol. 4, no. 59, pp. 5-30, 2018.

Krizhevsky, A., Sutskever, I., Hinton, G. E., ImageNet classification with deep convolutional neural networks. In: Advances in Neural Information Processing Systems, pp. 1097-1105, 2012.

Kuliev, E., Sheglov, S., Pantelyuk, E., Kulieva, N., Adaptive algorithm of the pack of grey wolves for solving design objectives, Izvestiya SFedU, Engineering Sciences, vol. 7, pp. 28-38, 2017.

Kurt M, Yılmaz Y, Wang X., Distributed quickest detection of cyber-attacks in smart grid. IEEE Trans Inf Forensics Security, vol. 13, no. 8, pp., 2018.2015–30.

LeCun, Y., Bengio, Y., Hinton, G., Deep learning, Nature, vol. 521, pp. 436–444, 2015.

Mac, T.T., Copot, C., Tran, D.T., De Keyser, R., Heuristic approaches in robot path planning: a survey, Robotics and Autonomous Systems, vol. 86, pp. 13-28, 2016.

Nojmol, I., How can Access Control Systems Improve Security and Reduce Costs? Public Sector Estates Management, pp.1-5, 2014.

Perez, J. A., Deligianni, F., Ravi, D., Yang, G. Z., Artificial Intelligence and Robotics. arXiv preprint arXiv:1803.10813., 2018.

Pisharady, P.K.R., Saerbeck, M, Robust gesture detection and recognition using dynamic time warping and multi-class probability estimates, in Computational Intelligence for Multimedia, Signal, and Vision Processing (CIMSIVP), 2013 IEEE Symposium on. IEEE., 2013.

Pshihov, V, Medvedev, M., Group motion control of mobile robots in an uncertain environment using unstable modes, SPIIRAS Proceedings, vol. 5, no. 60, pp. 39-63, 2018.

Raheja, J.L., Manasa, M.B.L., Chaudhary, A., Raheja, S., Abhivyakti: hand gesture recognition using orientation histogram in different light conditions, Proceedings of the 5th Indian International Conference on Artificial Intelligence, India, pp.1687–1698, 2011.

Rogers, C., Google Sees Self-Driving Cars on Road within Five Years, Wall Street Journal, 2015.

Saxena N, Choi B, Lu R., Authentication and authorization scheme for various user roles and devices in Smart Grid. IEEE Transactions on Information Forensics and Securities, vol. 11, no. 5, pp. 907–21, 2016.

Seung Hyun Kim, Su Chang Lim, Do Yeon Kim, Intelligent intrusion detection system featuring a virtual fence, active intruder detection, classification, tracking, and action recognition, Annals of Nuclear Energy, vol. 112, pp. 845-855, 2018.

Singh, N., Singh, S. B., Hybrid algorithm of particle swarm optimization and Grey Wolf optimizer for improving convergence performance, Journal of Applied Mathematics, vol.2017.

Suvendu Kumar Mohapatra, Prasan Kumar Sahoo, Shih-Lin Wu, Big data analytic architecture for intruder detection in heterogeneous wireless sensor networks, Journal of Network and Computer Applications, vol. 66, pp. 236-249, 2016.

Szegedy, C., Liu, W., Jia, Y. P., et al., Going deeper with convolutions, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 1-9, 2015.

Tan O, Gomez-VilardebJ, Gunduz D. Privacy-cost trade-offs in demand-side management with storage. IEEE Transactions on Information Forensics and Securities, vol. 23, no, 6, pp. 1458–69, 2017.

Vatamaniuk, I.V., Panina, G.U., Ronzhin, A.L., Simulation of the path of the robot systems with the reconfiguration of the spatial position of the swarm, Robotics and Technical Cybernetics, vol. 3, no. 8, pp. 52-57, 2015.

Vittal, K.P. et al., Computer controlled Intrusion-detector and automatic firing unit for border security, in: Computer and Network Technology (ICCNT), Second International Conference on. IEEE, 2010.

Yan J., He H., Zhong X., et al., Q-learning-based vulnerability analysis of Smart grid against sequential topology attacks, IEEE Transactions on Information Forensics and Securities, vol.12, no. 1, pp. 200–210, 2017.

Yang, L., Qi, J., Song, D., Xiao, J., Han, J., Xia, Y., Survey of Robot 3D Path Planning Algorithms, Journal of Control Science and Engineering, 2016.

Zhang, Z., A flexible new technique for camera calibration. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, no. 11, pp. 1330–1334, 2000.

Biography

Dr. M. B. Kiran is an Associate Professor in the Department of Mechanical Engineering, School of Technology, Pandit Deendayal Petroleum University, Gandhinagar, Gujarat, INDIA. He earned his graduation (B.E.) from the University of Mysore in 1987. He did his post-graduation (M.E.) in Production Engineering from P.S.G. College of Technology (1991) and Doctoral degree (Ph.D.), in Surface Metrology from Indian Institute of Technology (I.I.T.), Madras in 1997. He has Industry/Research/Teaching experience of 25 years. He has published technical papers in many reputed national/international journals and conferences. He is a member of the Project management Institute (P.M.I.), U.S.A. He is a certified project manager (P.M.P.) from P.M.I. He has completed many mission-critical projects. He has conducted many training programs for working executives.