INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research

International Journal of Mobile Network Design and Innovation

ISSN online: 1744-2850 - ISSN print: 1744-2869
https://www.inderscience.com/ijmndi

Effective anomaly detection in hybrid wireless IoT environment through machine learning model: a survey

V. Shanmuganathan, Suresh Annamalai

DOI: 10.1504/IJMNDI.2022.10053097

Article History:
Received: 29 June 2022
Accepted: 22 September 2022
Published online: 03 September 2023

Effective anomaly detection in hybrid wireless IoT environment through machine learning model: a survey

V. Shanmuganathan and Suresh Annamalai*

Department of Networking and Communications,
School of Computing,
College of Engineering and Technology,
SRM Institute of Science and Technology,
SRM Nagar, Kattankulathur,
Chengalpattu – 603203, Chennai, Tamil Nadu, India
Email: sv8468@srmist.edu.in
Email: suresha2@srmist.edu.in
*Corresponding author

Abstract: Wireless hybrid environment has seamlessly integrated inside all smart homes and in smart environments. Assaults and Anomalies are probably going to happen in open platform of IoT frameworks and which can result easily by sending fake alarms and the inability to appropriately identify basic occasions. To address that, IoT frameworks must be outfitted with peculiarity recognition preparing notwithstanding the necessary occasion identification capacity. This is a key component that empowers unwavering quality and productivity in IoT. An effective assault and oddity ready framework are a lot of important in IoT based climate, since these are power starving gadgets and convey extremely delicate information's. A proficient K-nearest neighbour (KNN) and Random Forest algorithm-based sensor information inconsistency recognition is anticipated in an edge gadget in this paper. The sensor hardware failure and software failures are identified in the IoT based environment and effective identification was achieved through KNN and Random Forest algorithm.

Keywords: anomaly detection; wireless IoT environment; KNN; K-nearest neighbour algorithm; Random Forest algorithm (RF); machine learning; IoT; Internet of Things.

Reference to this paper should be made as follows: Shanmuganathan, V. and Annamalai, S. (2023) 'Effective anomaly detection in hybrid wireless IoT environment through machine learning model: a survey', *Int. J. Mobile Network Design and Innovation*, Vol. 10, No. 4, pp.175–181.

Biographical notes: V. Shanmuganathan, ME, PhD, (pursuing) A Full-Time Research Scholar in the Department of Networking and Communications, School of Computing at SRM Institute of Science & Technology, Kattankulathur, Chengalpattu District, Tamil Nadu, India. He has completed his Master of Engineering in the field of Computer Science and Engineering and having a decade of experience in the field of Teaching. His area of specialisations are internet of things, networking, wireless sensor networks and wireless networks.

Suresh Annamalai, PhD, working as an Associate Professor in the Department of the NWC, School of Computing, SRM IST, Kattankulathur, Tamil Nadu, India. He has been serving more than two decades of experience in the field of teaching and his areas of specialisations are data mining, artificial intelligence, image processing and IoT. He has published eight patents and 100+ technical papers in the international journals. He has published 11 books as authored/edited and 17 book chapters published. He served as an Editor/Reviewer for the reputed publishers.

1 Introduction

Nowadays, Internet of Things (IoT) are becoming more Sophisticated. The IoT Environment has gone through wide range of progress in different fields. Anomaly detection in IoT Environment has gone through various Stages in many areas. IoT has entered into many heterogeneous objects such as sensors in cars, sensors in heavy vehicles, Ultra HD Cameras, Drones, etc., where these objects are

able to interact with each other and make communication by themselves on internet protocols.

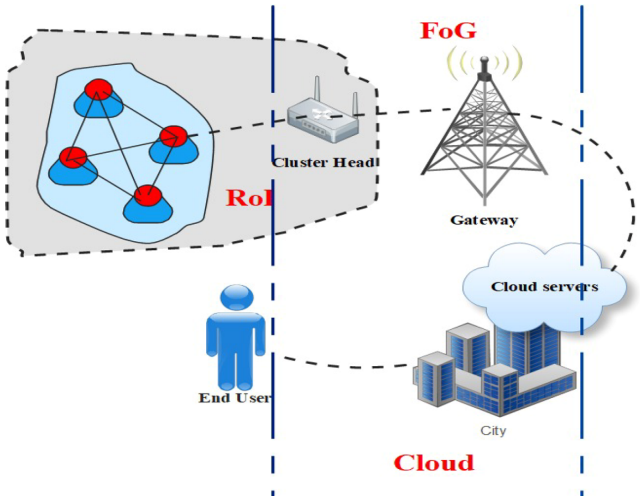
For the above-mentioned reasons, the detection of anomalies is becoming essential in wireless IoT environment and in a larger portion it is still under investigation process in machine learning models. Smart city, smart transportation, precision agriculture and healthcare are the major application domains in IoT technologies. Since IoT is meant for Sophistication and it is capable for providing relevant information and performance of a particular activity and it shows reliability and efficiency as well.

2 Wireless IoT Environment

IoT is a panoramic term which embraces the gathering to wirelessly connected devices that surround us. It is applicable not only for smartphones and tablets, but for millions and millions of devices and machines across the world. In Pourhabibia et al. (2020), a new twist on traditional products which were previously not connected to the internet. IoT in Hybrid environment is completely a new technology paradigm futured as a global network of entire machines and devices and it is capable of interacting with each other which represents various applications and advanced technical aspects. IoT remote organisations climate present exceptional difficulties and also for existing security systems are insufficient. In conventional IoT remote organisations, traffic and calculation are ordinarily checked and examined for abnormalities at different passages (Tsogbaatar et al., 2021). Be that as it may, customary installed security instruments in the actual layer like firewall and IDS are not, at this point enough to get the cutting-edge Internet and as an outcome of the boundless worries over grid access control and programming check, which is somewhat costly as far as the organisation's memory and energy utilisation.

In the recent researches, Machine learning for Anomaly detection has Random Forest algorithm and KNN algorithm has been extracted for features from network traffic data and finding of unlicensedhybrid environment IoT devices (Garg et al., 2019). They fostered an AI pipeline that performs information assortment, highlight determination and order for IoT DDoS recognition utilising various types of classifiers including irregular woodland, K-nearest neighbours (KNN), SVM, choice trees and neural organisations. Their outcomes showed that irregular woodland, K-closest neighbours and neural net classifiers were extremely powerful and effectively distinguished assault traffic with an exactness higher than 0.999. IoT gadgets conduct, we remove discriminate highlights from the data components in our rush hour gridlock information assortment (Su, 2011). A model of the ordinary conduct of the gadget can be made by the unaided profound learning calculation (auto encoder) on the worker. When we get the model, we then, at that point consolidate kind IoT gadgets with security obscure gadgets to get the assessment traffic information to assess our model. By inconsistency recognition methods, we recognise designs that don't adjust to anticipated ordinary conduct in the test information. After a few cycles, we will get a good performing model with the most elevated precision (Garg et al., 2019). This technique can be constantly applied to the information stream of new gadgets for ID and whitelisting.

Figure 1 IoT system reference topology (see online version for colours)



The significant impediment is identified with the availability amongst the registering cloud assets in the centre organisation and the gadgets at the edge. Figure 1 says that, ultimately end user is going to deal with the performance (Yahyaoui et al., 2021). On the one side, interchanges between IoT applications in the cloud and their connected item is accomplished through internet. The coordination permits the improvement of assets and the decrease of the executive's cost. IoT itself considered as an incorporated arrangement of subsystems for noticing various targets and various areas. Promotions comprises in the recognisable proof of what can keep a framework from achieving its predefined capacities like hubs disappointments, blunders, breakdowns and security assaults. EDS rather concerns the recognisable proof of occasions of interest and is distinguished in the determinations of an IoT reconnaissance framework, similar to the discovery of fire, flood and unapproved individual interruption (Cauteruccio et al., 2020). Peculiarity put together methodologies are by and large based with respect to AI calculations. They are utilised to identify oddities and pernicious exercises after a preparation stage to develop a model that recognises typical from strange information. Albeit these methodologies can identify new assaults, they have the burden of creating false encouraging points in a higher rate as opposed to govern based methodologies. Notoriety frameworks for the most part depend on screen

hubs to manage and assess their neighbour exercises. Trust esteems are influenced to every hub (Moustafa et al., 2018). They are determined by the hub noticed conduct like information collection and directing. At the point when a trust esteem is under an obvious limit, the related hub is considered malignant. Each approach has its key qualities and downsides (Kumar and Dutta, 2016). Accordingly, half breed approaches joining the past referenced methodologies were embraced to amplify the detection rate (DR), limit the false positive rate (FPR) and safeguard energy utilisation.

2.1 Current reviews

Various studies and surveys are being supported out in the field of IoT security in terms of reliability and efficiency for anomalies in IoT based environment. Moreover, the studies and surveys are still in the existence but not focusing on the various applications of machine learning techniques for IoT security. Table 1 recapitulates with the other surveys based on hybrid wireless IoT environment which compares the contribution of each survey related to IoT Security based on the terms of reliability and efficiency.

Table 1 Survey based on the comparison of IoT security in terms of reliability and efficiency

References No.	*Architecture of IoT*	*Protocols of IoT*	*Threats in IoT*	*Various Models in IoT ML*	*Securities in IoT*
Attarian and Hashemi (2021)	✓	✓	✓	×	×
Alraja et al. (2020)	×	×	✓	×	×
Wang and Cai (2020)	×	×	✓	×	×
Abduvaliyev et al. (2013)	×	×	×	×	×
Butun et al. (2013)	×	×	✓	×	×
Mishra et al. (2004)	×	×	✓	×	×
Anantvalee and Wu (2007)	×	×	✓	×	×
Kumar and Dutta (2016)	×	✓	✓	×	×
Granjal et al. (2015)	×	✓	✓	×	×
Zarpelao et al. (2017)	×	×	✓	×	×
Xiao et al. (2018)	×	×	✓	×	×
Buczak and Guven (2015)	×	×	✓	×	×
This survey	✓	✓	✓	✓	✓

In this paper (Attarian and Hashemi, 2021), the authors have clearly explained about the Classifications Wireless sensor Networks completely based on the deployment model of IDS Agent. In Alraja et al. (2020), said about cloud-based environment and they classified about cloud based IDs which affects availability based on IoT networks, confidentiality and integrity. In addition to that they described about hypervisor based IDs, host based IDS (HIDS), network based IDS (NIDS), and distributed IDS. In this paper (Wang and Cai, 2020), a similar scenario as a survey has been carried out about the classifications of Wireless sensor networks based on IDS detection type.

3 Anomaly detection approaches

Anomaly detection approaches has many classifications like clustering based, deep learning based, knowledge based and etc. In this classification based approach, K-nearest neighbour algorithm plays a vital role for detecting anomalies in a network that's where the below Figure 2 says in an ordered manner of classifications. Apart from other detection approach, classification-based approach is mainly used for reliability and efficiency in IoT (Himeur et al., 2021). An efficient attack is always a handy one in detection approach. One-class inconsistency strategies become really fascinating when there is an irregularity between the quantities of typical and assault perceptions, where those of ordinary occurrences are significantly more prominent than those of assault or uncommon occasions which is the idea of organisation traffic. They are likewise huge in case examples are delegated ordinary or assault with no assault types, like DoS and DDoS, being distinguished (Aljuhani, 2021). On the other hand, multi-class oddity strategies are more significant in case there is a harmony between the classes of typical and assault perceptions, and, additionally, best for perceiving assault types.

Therefore, Figure 3 says that learning strategies where they are using our information from just a solitary class to fabricate a typical for perceiving information from that class and dismissing the rest, have gotten really engaging (Benkhelifa et al., 2018). An important classification-based approach is applied for anomaly detection systems are support vector machine and K-nearest neighbour and as well as artificial neural network. A KNN instrument characterises every perception doled out to the class name by figuring the most elevated certainty between the *k* information focuses closest the question information point (Xiao et al., 2018). A KNN based NADS makes a typical organisation profile and treats any deviation from it as an assault. It is an amazing for anomaly detection systems in light of the fact that it doesn't request adjusting boundaries

in the preparation stage. The KNN strategy was utilised to plan a trustworthy NIDS (DIDS) in view of the weirdness and disconnection proportions of its potential capacities which could successfully distinguish network assaults.

Figure 2 Taxonomy of anomaly detection approaches (see online version for colours)

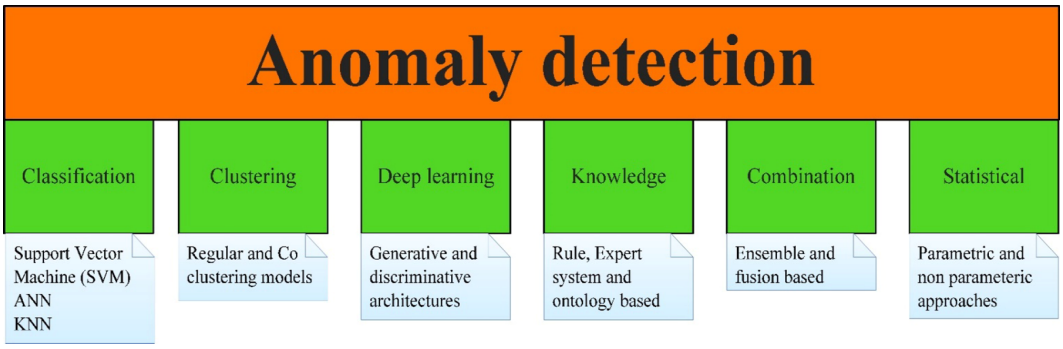
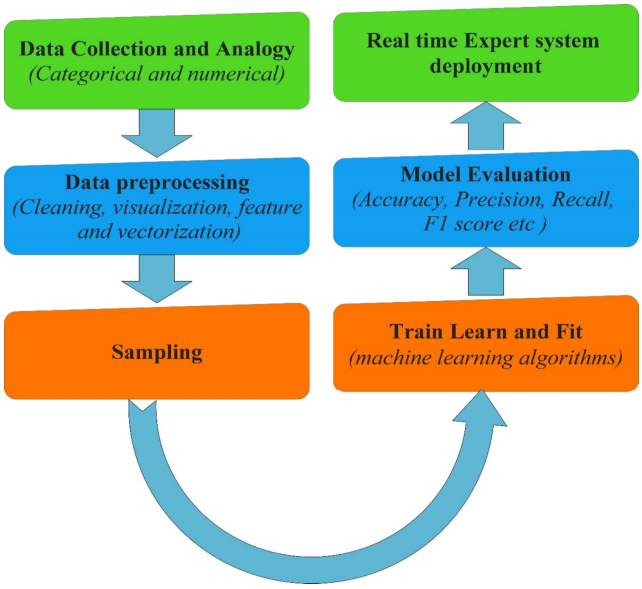


Figure 3 Testing for anomaly detection in IoT (see online version for colours)



All things considered, KNN are frequently tedious and require tremendous measures of capacity to group high velocity network traffic. In addition to that order procedures, for example, a choice tree, relapse models and fluffy rationale have likewise been applied to plan inconsistency recognition frameworks (Buczak and Guven, 2015). In any case, generally speaking, characterisation put together IDSs depend intensely with respect to the expectation that every classifier must be changed independently and consistently devour a greater number of assets than factual procedures (Anantvalee and Wu, 2007). At last, if these strategies don't effectively fabricate ordinary examples, they are not fit for identifying new assaults. Note that most order methods have been assessed utilising old datasets, especially the KDD99 dataset, and their terrible showings will unquestionably be more awful on more up to date datasets.

3.1 K-nearest neighbour algorithm

To begin with KNN, which is efficient and tremendous measures of capacity to reduce group high velocity network traffic. Trust and notoriety frameworks are predominantly utilised for checking task in wireless sensor networks and hybrid IoT frameworks. Generally, they depend on screen hubs or guard dogs that are utilised to direct and assess their neighbour practices (Iqbal et al., 2020). Confidence esteems are determined for the hub's dependent on their noticed exercises, and afterward choice for information collection or directing is taken dependent on this assessment. On top of IoT oversight framework, an administration layer contains the important modules that grant to screen the IoT hubs and network, compute and update the best sending plan of handling segments.

In addition to that, IoT Applications endorsers get warnings and alarms for occasions of interest and abnormalities. We set up a test customer IoT organisation and gather just favourable IoT gadgets traffic to track down the ordinary conduct (Ahmad and Alsmadi, 2021). These sensors in the IoT framework records the source Macintosh address, address of IP, source port, customer IPaddress and other fundamental data sent from wireless communication of associated gadgets, and afterward send it to a focal worker. Given a bunch of approved gadgets and a bunch of traffic information, the worker makes a finger impression for every gadget contains the exceptional recognisable data (Aversano et al., 2021). In view of area information on IoT gadgets conduct, we remove discriminative highlights from the data components in our rush hour gridlock information assortment. A model of the ordinary conduct of the gadget can be made by the unaided profound learning calculation (auto encoder) on the worker. When we get the model, we then, at that point consolidate amiable IoT gadgets having a security obscure gadget to get the test traffic information to assess our model. By oddity recognition methods, we can able to distinguish designs that don't adjust to anticipated typical conduct in the test information. After a few emphases, we can get the best performing model with the most elevated exactness (Mishra et al., 2004). This is a kind of technique which can be consistently applied to the source of information stream of new gadgets for recognisable proof.

Furthermore, Figure 4 states that, self-organised based K-nearest neighbour algorithm has one normal

characterisation conspire dependent on the utilisation of distance measures is that of the k-closest neighbour. The KNN method expects that the whole inspecting set remembers the information for the set, yet in addition the ideal order for everything (Wang et al., 2020). At the point when a characterisation is to be made for another thing, its distance to everything in the testing set should be processed. Hands down the *k* nearest passages in the examining set are thought about further. Identification of the closest neighbour is performed by the *k*-closest neighbour (KNN) calculation. As a rule, KNN is utilised as an order procedure, where a test information perception is arranged to a class in case it is nearer to the closest neighbour in that class. In this examination, KNN is utilised as a semi-managed learning strategy, where KNN is simply used to distinguish the closest neighbour in the reference BMUs (Bhuiyan and Billah, 2021). The distance of the test information perception to the centroid of the distinguished neighbour is determined. In this investigation this distance is called KNN distance. It is utilised as the well-being pointer.

In peculiarity location, Figure 5 mentions that the strategy is first applied to the sound preparing information to get the example of the worth from the well-being pointer of the solid framework (Butun et al., 2013). A percentile of the example is then chosen as the peculiarity limit.

Figure 4 KNN observation for new data point (see online version for colours)

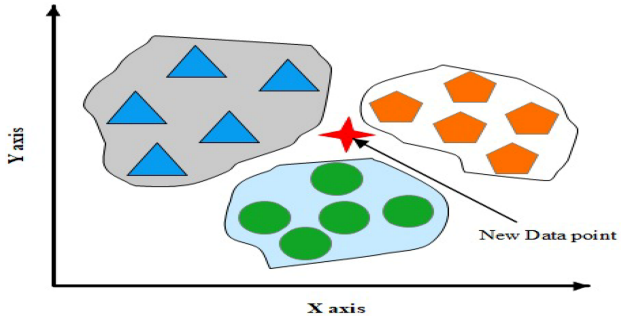
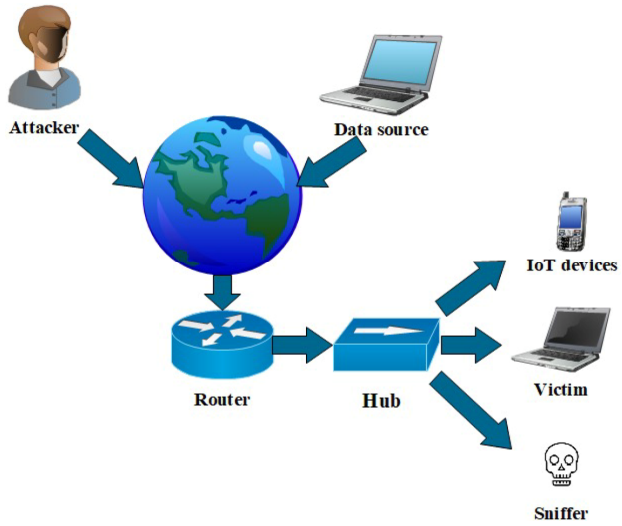


Figure 5 Experimental network topology (see online version for colours)



3.2 Random Forest algorithm

It's a popular machine learning algorithm which is an essential tool in supervised learning technique which can be used for both Classification and regression problems in machine learning (Modi et al., 2013). Moreover, its completely based on ensemble learning, which is a process of joining numerous classifiers to resolve a complex problem and to improve the performance of the model. Since it has some certain advantages when compared to other algorithms by taking less training time and predicting the output with the highest amount of accuracy even in the large datasets which can run efficiently in a network to find the anomalies (Granjal et al., 2015). An effective random forest Classifier is used to improve the performance of anomaly detection in IoT network.

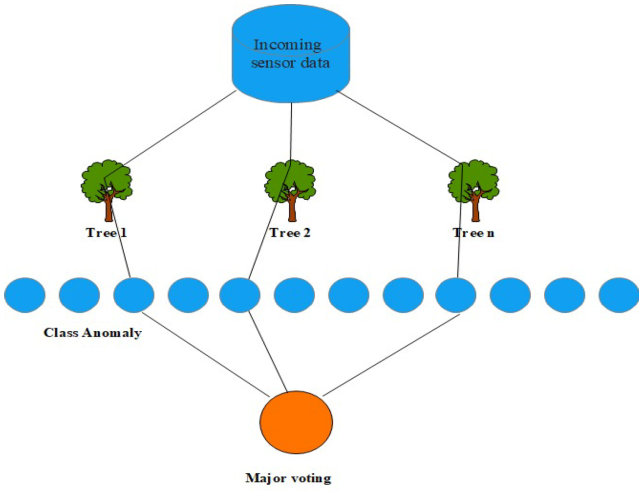
Irregularity recognition, otherwise called anomaly discovery, is perhaps the most broadly concentrated among various exploration and application regions. Indeed, the conversation of exception identification in informational collections can be followed back to the 18th century when Bernoulli scrutinised the act of erasing the anomalies (Xu et al., 2020). The issue of discovering peculiarities is regularly depicted as the issue of discovering designs in information that don't adjust to anticipated conduct or of discovering information objects with practices that are altogether different from assumption (Mishra et al., 2018). Peculiarities are normally connected with security dangers, monetary misrepresentation, clinical disappointment, framework disappointments, and so forth Perhaps the most broadly relevant regions for oddity discovery are distinguishing interruptions which requires online location. Random Forest calculation is a piece of tree-based order calculations and perhaps the best AI models, this calculation depends on the gatherings of choice trees.

The principal idea of this calculation is to shape the precision of the choice tree, to accomplish this objective picks the arbitrary subspaces of the highlights and construct various trees for the arbitrariness and this methodology sum up and further develop the characterisation then to foresee a specific class totals the votes of tree and the class with the most votes is the expectation result (Zarpelao et al., 2017). Since this calculation utilises numerous choice trees decrease the overfitting and it needn't bother with any component scaling and furthermore could perceive the non-linearities highlights and highlight cooperation likewise it upholds twofold, multiclass characterisation and relapses both straight out and constant highlights. The preparation of each tree doing independently, so should be possible in equal and furthermore joining the expectations of each tree decreases the change of the forecasts furthermore, working on the forecasts on the test information.

In Figure 6 states that Random Forest classifier calculation takes a few boundaries however the quantity of trees has significant job for making a model and influence the precision of the model, at the other hand the exactness for interruption identification is basic particularly for significant places so in this examination we attempting to

track down the quantity of trees that with the exception of the precision likewise considering the handling time and memory devouring. The proposed techniques for abnormality identification were exposed to assessment expecting to determine whether the time periods where inconsistencies happened were appropriately perceived (Garg et al., 2019). Plus, it is additionally assessed if the ID of the peculiarities gave reliable discovery, without arrangement blunders. As the name suggests, the irregular backwoods calculation makes the woodland with numerous choice trees. It is a regulated characterisation calculation. It is an appealing classifier because of the great execution speed. Numerous choice trees outfit together to frame an irregular timberland, and it predicts by averaging the forecasts of every part tree. It for the most part has much preferred prescient precision over a solitary choice tree. As a general rule, the more trees in the woodland the stronger the backwoods look.

Figure 6 Illustration of Random Forest classifier (see online version for colours)



Both K-nearest neighbour and Random Forest algorithm based on sensor data considered as one of the important detections in anomalies in a network. Through this we can get reliability and reliable communication through regression and classification problems in machine learning. It's a technique to provide solutions for complex problems in a network (Abduvaliyev et al., 2013). RF is portrayed as an outfit based nonlinear measurable packing strategy. RF produces homogeneous subsets of auxiliary indicators, known as relapse trees, in an arbitrary way and utilisations the benefits of utilising the normal consequences of every blend. From the outset, it requires a few quantities of factors from all indicator factors. The individual relapse tree is created from 66% of the bootstrapped test preparing information.

4 Challenges

Even though we couldn't recognise many attacks in the variants of existence, it's still a common defence in IoT based environment. On the other side some serious threats have been facing in the variants of existence in IoT based environment, where these challenges can be explored through different efficient attacks for anomalies. In addition to that, to detect and improve the reliability and efficiency, certain methodologies are facing with big encounters for their effective design is a daunting task is the upcoming challenges in hybrid IoT environment facing in reality. Though we are keenly concentrating on improving reliability and efficiency as a challenge, definitely we have to keep an eye on trustworthy and energy efficiency as well for the betterment of sophisticated hybrid IoT environment.

5 Conclusion

An effective efficient attack K-nearest neighbour and Random Forest algorithm sensor data has been proposed to improve the reliability and efficiency of Anomaly detection in IoT network. These two attacks are much needed for the IoT based environment, where they can carry Sensitive information without any delay with reliable sources which carries an effective identification has been achieved through K-nearest neighbour and Random Forest algorithm. Additionally, the proposed algorithm sensor data has been outperformed with respect to reliability and efficiency which holds a good solution for IoT based environment in future.

References

Abduvaliyev, A., Pathan, A.S.K., Zhou, J., Roman, R. and Wong, W.C. (2013) 'On the vital areas of intrusion detection systems in wireless sensor networks', *IEEE Commun. Surv. Tutor*, Vol. 15, pp.1223–1237.

Ahmad, R. and Alsmadi, I. (2021) 'Machine learning approaches to IoT security: a systematic literature review', *Internet of Things*, Vol. 14, June, p.100365.

Aljuhani, A. (2021) 'Machine learning approaches for combating distributed denial of service attacks in modern networking environments', *IEE Access*, Vol. 9, March, pp.42236–42264.

Alraja, M.N., Barhamgi, H., Rattrout, A. and Barhamgi, M. (2020) 'An integrated framework for privacy protection in IoT applied to smart healthcare', *Computers and Electrical Engineering*, Vol. 91, May, p.107060.

Anantvalee, T. and Wu, J. (2007) 'A survey on intrusion detection in mobile ad hoc networks', *Wireless Network Security*, Berlin, Germany, Springer, pp.159–180.

Attarian, R. and Hashemi, S. (2021) 'An anonymity communication protocol for security and privacy of clients in IoT-based mobile health transactions', *Computer Networks*, Vol. 190, May, p.107976.

Aversano, L., Bernardi, M.L., Cimitile, M. and Pecori, R. (2021) 'A systematic review on deep learning approaches for IoT security', *Computer Science Review*, Vol. 40, May, p.100389.

Benkhelifa, E., Welsh, T. and Hamouda, W. (2018) 'A critical review of practices and challenges in intrusion detection systems for IoT: toward universal and resilient systems', *IEEE Commun. Surv. Tutor*, Vol. 20, pp.3496–3509.

Bhuiyan, M.N. and Billah, M.M. (2021) 'Internet of things (IoT): a review of its enabling technologies in healthcare applications, standards protocols, security and market opportunities', *IEEE Internet of Things Journal*, Vol. 8, No. 13, July, pp.10474–10498.

Buczak, A.L. and Guven, E. (2015) 'A survey of data mining and machine learning methods for cyber security intrusion detection', *IEEE Commun. Surv. Tutor*, Vol. 18, pp.1153–1176.

Butun, I., Morgera, S.D. and Sankar, R. (2013) 'A survey of intrusion detection systems in wireless sensor networks', *IEEE Commun. Surv. Tutor*, Vol. 16, pp.266–282.

Cauteruccio, F., Cinelli, L., Corradini, E. and Terracina, G. (2020) 'A framework for anomaly detection and classification in multiple IoT scenarios', *Future Generation Computer Systems*, Vol. 114, August, pp.322–335.

Garg, S., Kaur, K., Batra, S., Kaddoum, G., Kumar, N. and Boukerche, A. (2019) 'A multi-stage anomaly detection scheme for augmenting the security in IoT-enabled applications', *Future Generation Computer Systems*, Vol. 104, September, pp.105–118.

Garg, S., Kaur, K., Kumar, N. and Rodrigues, J.J.P.C. (2019) 'Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in SDN: a social multimedia perspective', *IEEE Transactions on Multimedia*, Vol. 21, No. 3, March, pp.566–578.

Garg, S., Kaur, K., Kumar, N., Kaddoum, G., Zomaya, A.Y. and Ranjan, R. (2019) 'A hybrid deep learning based model for anomaly detection in cloud datacentre networks', *IEE Transaction on Network and Service Management* [online], July, Available in Online: DOI: 10.1109/ TNSM.2019.2927886

Granjal, J., Monteiro, E. and Silva, J.S. (2015) 'Security for the internet of things: a survey of existing protocols and open research issues', *IEEE Commun. Surv. Tutor*, Vol. 17, pp.1294–1312.

Himeur, Y., Ghanem, K., Alsalemi, A., Bensaali, F. and Amira, A. (2021) 'Artificial intelligence-based anomaly detection of energy consumption in buildings – a review current trends and new perspectives', *Applied Energy*, Vol. 287, April, p.116601.

Iqbal, W., Abbas, H., Daneshmand , M., Rauf, B. and Bangash, Y.A. (2020) 'An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security', *IEEE Internet Of Things Journal*, Vol. 7, No. 10, October, pp.10250–10276.

Kumar, S. and Dutta, K. (2016) 'Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges', *Secur. Commun. Netw.*, Vol. 9, pp.2484–2556.

Mishra, A., Nadkarni, K. and Patcha, A. (2004) 'Intrusion detection in wireless ad hoc networks', *IEEE Wirel. Common*, Vol. 11, pp.48–60.

Mishra, P., Varadharajan, V., Tupakula, U. and Pilli, E.S. (2018) 'A detailed investigation and analysis of using machine learning techniques for intrusion detection', *IEEE Commun. Surv. Tutor*, Vol. 21, pp.686–728.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A. and Rajarajan, M. (2013) 'A survey of intrusion detection techniques in cloud', *J. Netw. Comput. Appl.*, Vol. 36, pp.42–57.

Moustafa, N., Hua, J. and Slayb, J. (2018) 'A holistic review of network anomaly detection systems – a comprehensive survey', *Journal of Network and Computer Applications*, Vol. 128, December, pp.33–55.

Pourhabibia, T., Ongb, K-L., Kama, B.H. and Booa, Y.L. (2020) 'Fraud detection – a systematic literature review of graph-based anomaly detection approaches', *Decision Support Systems*, Vol. 133, June, p.113303.

Su, M-Y. (2011) 'Real-time anomaly detection systems for denial-of-service attacks by weighted k-nearest-neighbor classifiers', *Expert systems with Applications*, Vol. 38, pp.3492–3498.

Tsogbaatar, E., Bhuyan, M.H., Taenaka, Y., Fall, D., Gonchigsumlaa, K., Elmroth, E. and Kadobayashi, Y. (2021) 'DeL-IoT A deep ensemble learning approach to uncover anomalies in IoT', *Internet of Things*, Vol. 14, June, p.100391.

Wang, X. and Cai, S. (2020) 'Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud', *Future Generation Computer Systems*, Vol. 112, May, pp.320–329.

Wang, Z., Luo, N. and Zhou, P. (2020) 'Guard health: blockchain empowered secure data management and graph convolutional network enabled anomaly detection in smart healthcare', *J. Parallel Distributed Computing*, Vol. 142, April, pp.1–12.

Xiao, L., Wan, X., Lu, X., Zhang, Y. and Wu, D. (2018) *IoT Security Techniques based on Machine Learning*, arXiv, arXiv:1801.06275.

Xu, R., Cheng, Y., Liu, Z., Xie, Y. and Yang, Y. (2020) 'Improved long short-term memory based anomaly detection with concept drift adaptive method for supporting IoT services', *Future Generation Computer Systems*, Vol. 112, May, pp.228–242.

Yahyaoui, A., Abdellatif, T., Yangui, S. and Attia, R. (2021) 'READ-IoT: reliable event and anomaly detection framework for the internet of things', *IEE Access*, Vol. 9, February, pp.24168–24186.

Zarpelao, B.B., Miani, R.S., Kawakani, C.T. and de Alvarenga, S.C. (2017) 'A survey of intrusion detection in Internet of Things', *J. Netw. Comput. Appl.*, Vol. 84, pp.25–37.