Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

A Securable Reinforcement Learning IDS in IoT for Smart Homes using GKMF- OMDP

Gauri Kalnoor[1], Vijayalaxmi Kadrolli[2*], Varsha Bodade[3]

[1]Assistant Professor-Senior Scale, Dept. of CSE, Manipal Institute of Technology, India, gauri.kalnoor@manipal.edu
[2]Associate Professor, Dept. of Information Technology, Terna Engineering College, India, vijayalaxmikadroli@ternaengg.ac.in
[3]Professor, Dept of Information Technology, Terna Engineering College, India, varshabodade@ternaengg.ac.in

Recent advances in the Internet of Things (IoT) have made it a viable tool for creating intelligent settings. Any technology that relies on the Internet of Things (IoT) concept is seen as having serious security and privacy issues. The Internet of Things (IoT) needs a highly secure IDS paradigm in order to generate user confidence. Even though various IDS models have been developed, detecting the dynamic and uncertain attacks in a real environment is a challenging task. The work has developed a Reinforcement learning-based IDS using GKMF-OMDP in IoT for smart homes application. The developed GKMF-OMDP doesn't get trained up over any labeled datasets but in case learn by itself about the instances of the attacks and makes a robust decision to conquer them. The improvisation of the decision is done through the reward function to produce accurate attack detection. The approach selects an optimal policy using GKMF-FO by addressing the noisy observation that is caused due to uncertainty. Overall, the developed approach is capable of taking a countermeasure by identifying the occurrence and evolution of theattacks. Experimental analysis shows that compared with the existing methodologies the approach tends to obtain better accuracy, attack detection rate and avoids the false alarm rate of detecting the attack.

Keywords: Internet of things (IoT), smart homes, Intrusion detection system (IDS), security, reinforcement learning (RL), Uncertainty, Gaussian kernel membership function based optimized Markov decision process (GKMF- OMDP), Fuzzy optimization.

1. Introduction

Objects or "things" that can sense their surroundings, connect to one other and exchange data via the Internet are being referred to as the Internet of Things (IoT) [1, 2]. IoT networks are expected to link one trillion IP addresses or items to the Internet by 2022 [3]. There has been recent usage of the IoT paradigm in developing intelligent settings, including smart homes, with a variety of application domains and associated services[4]. It is the purpose of

constructing these smart houses to improve human well-being and productivity by addressing environmental issues [5].

Smart homes and IoT technologies work together to improve the efficiency of smart items. Denial-of-service (DoS) attacks and distributed denial-of-service (DDoS) attacks are two types of security threats that might affect IoT systems [6, 7]. An IoT network's IoT services and smart environment applications might suffer significant harm as a result of such assaults. It has become more important to secure IoT systems as a result of this. IDS (intrusion detection system) is a network-based security method for IoT systems [8]. There should be no limitations on the types of data packets that an IDS may examine or the types of answers it can create in real time, regardless of where the packets are in the IoT network or what protocol stack they're in [9, 10]. For an IDS to be effective in IoT-based smart settings, it must be able to analyse large volumes of data quickly and with minimum processing power. Traditional IDS may not be appropriate for IoT contexts because of this [11, 12]. In order to keep up with the ever-changing nature of IoT security, it is necessary to keep up with the most recent research on the security vulnerabilities of IoT systems and the development of related mitigation strategies. GKMF-OMDP has been used to create an IDS for smart homes that is based on reinforcement learning.

Furthermore, sections 2 and 3 exhibit similar studies, section 3 details the suggested technique and section 4 and section 5 examine findings and conclusions.

2. LITERATURE SURVEY

Manimurugan et al. [15] DBN technique was used to build an intrusion detection system model utilizing deep learning. The CICIDS 2017 dataset was used to test the performance of the IDS model. New method surpassed previous one in terms of accuracy, recallability, precision, F1 score, and detection rate. Contrarily, our model was too complex and took a lengthy time to detect attacks.

Md Arafatur Rahman et al. [16] A semi-distributed and distributed technique to feature extraction and selection has been shown. It developed a parallel machine-learning model based on a partitioned assault dataset in order to distribute the processing strain. However, intruders were able to take advantage of the centralized IDS's intrinsic trade-offs between accuracy and time performance, which led to the greatest detection accuracy and the best time performance.

Sushil Kumar Singh et al. [17] Utilizing Blockchain and Software-Defined Networking (SDN) protocols, a distributed environment for CPS communication was constructed using deep learning-based IoT-oriented infrastructure. Using a deep learning-based cloud at the application layer of the infrastructure, communication latency and centralization concerns were addressed. The Smart City's applications, such as smart industry and transportation, were supported by high-performance computer resources that were made accessible at a reasonable cost. Attackers who were difficult to detect or control functioned effectively with this tactic.

Sana Ullah et al. [18] A supervised machine learning-based support vector machine (SVM) was used to identify an attacker who was trying to sabotage the IoT network by injecting superfluous data. The results of the simulations demonstrated that the SVM-based classifier worked adequately in terms of classification accuracy and detection time when assisted by a

combination of two or three complex characteristics. Despite the fact that it worked successfully, the strategy was not resistant to a variety of assaults.

3. PROPOSED REINFORCEMENT LEARNING BASED IDS IN IoT FOR SMART HOMES

Fault-tolerance and reliability are two areas where intrusion detection has shown to be a reliable answer for modern- day information security challenges. When it comes to securing data, it is assumed that no matter how many IDS have been established, attackers would ultimately find a way around them. There must be methods that allow detection systems to respond immediately when a continuous intrusion is detected so that defensive countermeasuresmay be launched in a timely manner to deter, frustrate, or completely block the attacker's ultimate goals. There must be methods that allow detection systems to respond immediately when a continuous intrusion is detected so that defensive countermeasures may be launched in a timely manner to deter, frustrate, or completely block the attacker'sultimate goals [19]. GDMF-OMDP has been created for IDS in smart homes based on the Internet of Things (IoT). GDMF- OMDP has been created for IDS in smart homes based on the Internet of Things (IoT).

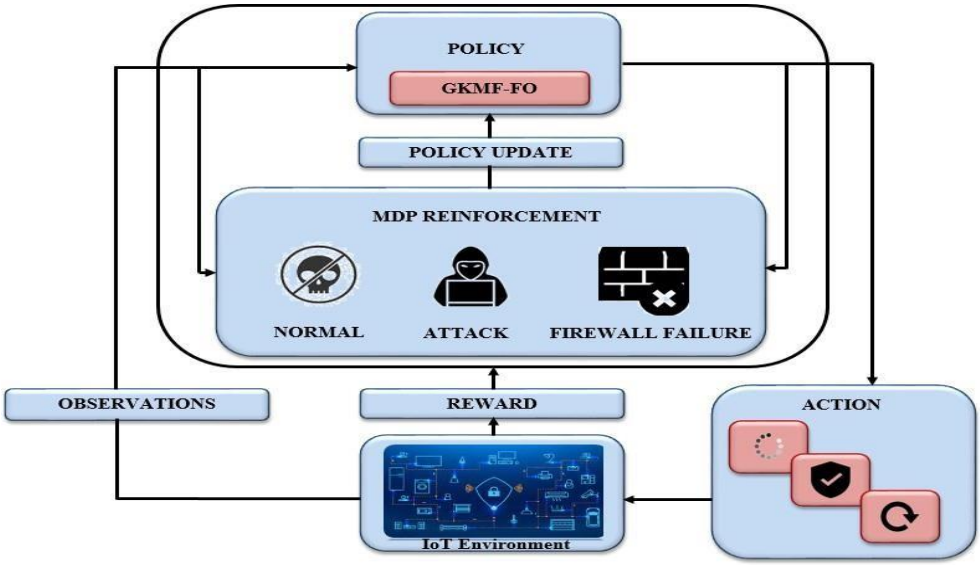


Figure1: Proposed Reinforcement learning IDS in IoT for smart homes

3.1. GKMF-OMDP Approach for IDS

Initially, the environments are categorized into three states: "Normally operating (S1)", “Attack (S 2)”, “Failure of N A security firewalls (S 3)". Consider the respective actions performed over each state labeled as: "Wait (□1)”, F W “Defend (□2)”, “Reset (□3)"as illustrated in figure 2. Let □ is the probability of transition for state-action pair (□S□), i.e.

D□S□ □□ S R and a reward function □□S, □□ is allotted for correct state-action pair and respective discount factor □ □□0,1□. A policy □ maps for each period t □ N is assigned and

a state-action history up to time

t□S0 , □0 , S1, □1, S2 , □2 ,.... St □t □ how likely it is that a certain activity will occur (□S,A) is the first step [20]. In

general, policy is influenced by the course of events in the past. It is provided for a strategy that maximizes thediscounted anticipated benefit over an infinite horizon □□□ , P□, where

Where, St represents the state at time period t , □t illustrates the action chosen at time tthat follows the probability distribution of □□ St □t □ □ □ . The vector p0 □ □ □ starting probability distribution across the collection of states. A simple assumption is made for the purpose of brevity and without sacrificing generality.

□s □ □ all states s and that the rewards are non-negative. It is assumed that the set of states and the set of actions are finite.

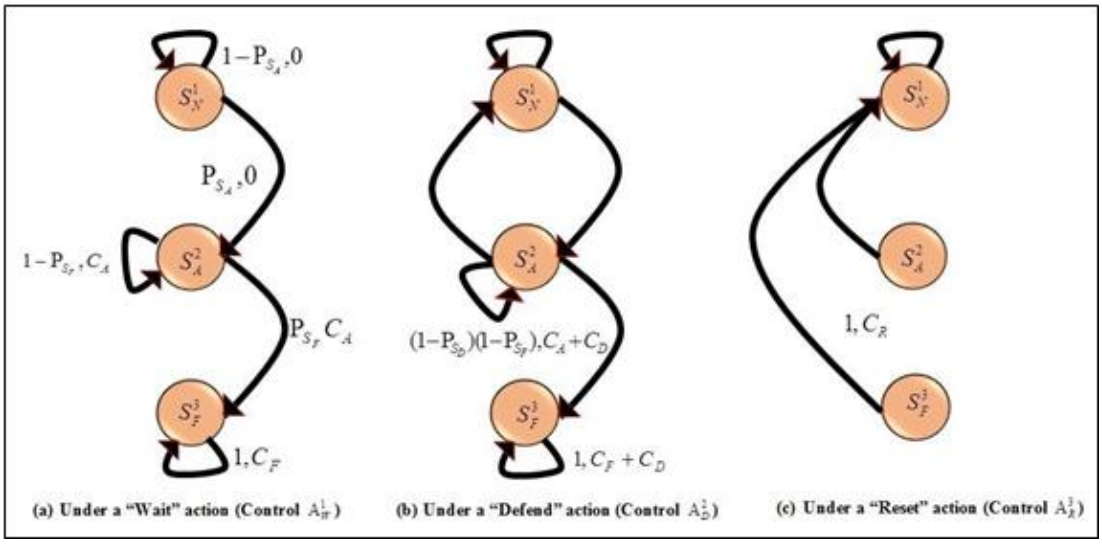


Figure2: GKMF-OMDP Architecture

"The intrusion detection system is built based on the transition among the states and the respective action outputs that will explicate whether the environment is normal or abnormal. Initially, under the "wait" action (control □1), there S are self-transitions in state 1 that represents a secure environment, which illustrates the normal execution of the N process. However, when there is a transition from state S1 to S 2 occur to per-stage probability □ , then their start N

to begin the intrusion attempt. Thereafter, self-transitions in state S 2 is represented to be under attack; eventually, a transition from state S 2 to S 3 occur with per-stage probability □ , This signifies the beginning of an ongoing F SF A S security firewall. The price of the changeover, starting at the state level 1 is cost-free, whereas for the transition N beginning at state S 2 and S 3 , there exists a cost of C and C . These same probabilities or cost parameters apply

A F A F

under the "defend" action (control □2), but with two differences as compared to wait: Firstly, the possible transition from state S 2 back to S1 (occurring with per-stage probability □) represents the successful disruption of the

N □ F

A

intrusion attempt via reducing the intrusion cost; secondly, the cost of disruption CD is incurred in addition to the transition cost under control □1 . Finally, under the “reset” action (control □3), a transition back to state 1 R SN occurs with probability one, incurring a cost of CR , regardless of where you are in the decision-making process”.

3.1.1. Optimal policy for decision making

The optimal policy is mandatory that seeks to obtain the best Intrusion detection system. However, statistical mistakes during the transition period owing to noise that occurs unpredictably result in a poor level of detection efficiency. As a result, it is a rough estimate of the actual problem's transition probability. Small changes in the problem parameters might have a very negative impact on the optimum strategy and result in suboptimal results for the nominal parameters. The study has designed a fuzzy optimization based on the Gaussian kernel membership function to produce a better policy.

The aim is to find a policy that would maximize the worst-case expected reward over the choices of P in the uncertainty setU , i.e.

Data is first mapped into each control, with the goal of minimizing the average cost per stage if there are several stages. As a last thought, think about the possible uncertainty sets that may arise throughout the movement of data. The uncertainty is objective uncertainty, epistemic uncertainty, etc.

Now, based on the uncertainty, an optimal policy is selected based on the fuzzy set, which splits the complex decision- making into a hierarchical tree structure. Now, the pairwise fuzzy comparison matrix is formulated for the uncertainty and the original data with the help of Gaussian kernel membership functions that is:

Where, □i is the central value and standard deviation, □ which should be greater than 0 □□ □ 0□ . The

membership value will be more accurate if the SD value is less. A membership metric is derived for each value

entered into the system. A pairwise comparison matrix is created based on the membership function. □M □. Now, the consistency of the matrix is checked, which helps to prioritize the uncertainty decisions by comparing them with the original data. A special condition is formulated to c ombine the u ncertainty that is

if M ik □ M kj □ M ij priority vector[□ 1,□ ,2...□

n]T(7)

Where, i, j, k □ 1,2,...n , □ denotes the fuzzy multiplication and □ represents the fuzzy equal to.

Various local priorities obtained at a different level of decision hierarchy are converted into composite global priorities using the weighted sum method. If there are i uncertainties, then the global priority is computed as:

N Mi □ □□ j M ij j□1(8)

Where, □j is the weight criterion of the j , M ij represents the alternative evaluation of and it states that higher the value of Mi the more referred the uncertainty.

Mi against the criterion j, Once the optimal policy is obtained, then the mapping is done

M : □S1 , S 2 , S 3 □→□□1 , □2 , □3 □

i N A F N A F (9)

The mapping with the state and action provides various single-stage decision i.e.

M d □ Mi □xd □ (10)

Now, based upon the decision made, the reward function is allotted to the model if the attack has avoided by computing the cost for each state-action pair i.e.

Initially, average cost per stage for "Wait upon attack (□ W)" is evaluated using:

Finally, the average cost per stage for "reset upon attack (□ W)" is computed using:

□S CR

□ W □ A

□1□ □ □

S A (13)

Based on the outcome of the cost, the model is rewarded and the attacks have been detected and defended

4. RESULTS AND DISCUSSION

In order to evaluate the suggested Reinforcement Learning model for IDS, several performance indicators are used, and the proposed work is then compared to the current approaches. The proposed work is performed in the working platform of python v3.7.

4.1. Performance Analysis

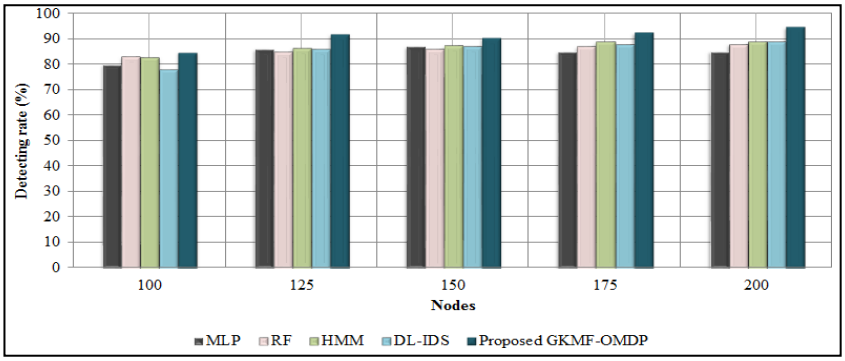
The proposed GKMF-OMDP is analyzed over the network nodes from 100 to 200 with a step size of 25 based on the performance metrics, such as Accuracy, Detection Rate, False Alarm Rate, Throughput, and Goodput, and evaluated with the existing methodologies, such as multi-layer perceptron (MLP), Random Forest (RF), Hidden Markov Model (HMM) and deep learning-based Intrusion detection system (DL-IDS). The tabular evaluation of accuracy is illustrated in table 1 and the graphical analysis of the remaining metrics is represented in Figures 3-4.

Table1: Evaluation of Proposed GKMF-OMDP based on accuracy metrics

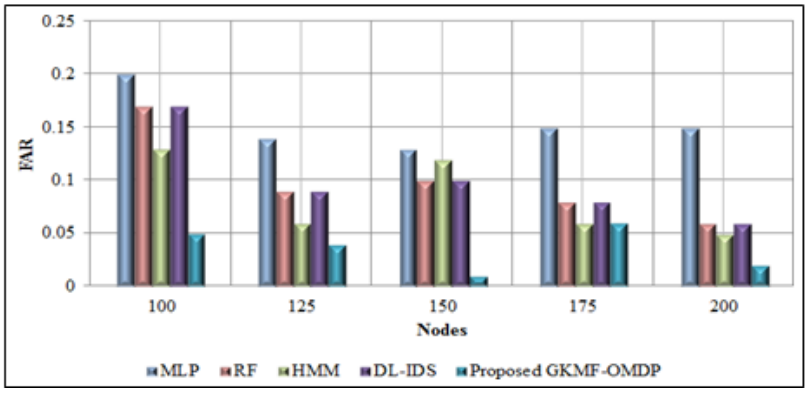
Techniques/Nodes	100	125	150	175	200
MLP	83.66	77.46	87.31	88.69	83.22
RF	84.34	81.08	82.45	83.56	84.75
HMM	83.65	82.3	83.99	84.75	84.98
DL-IDS	84.76	83.52	90.95	90.16	88.93
Proposed GKMF-OMDP	87.26	85.84	93.91	94.62	90.1

Table1 illustrates the accuracy achieved by the proposed method to detect the malicious function and then existing techniques are also evaluated. The high accuracy of a model illustrates a highly efficient model with a lowpossibility of errors. According to that, the proposed technique tends to obtain an accuracy of a maximum of 94.62%for a node of 175, Rather than achieving an accuracy level of 83.56 percent to 90.16 percent, current approaches tend to obtain an accuracy level of 83.56 percent to 90.16 percent. It has been shown that the suggested techniquehas a superior metric value for detecting the assault and is more efficient than the current ways .

The higher accuracy of the proposed framework tends to achieve a better Detection Rate (DR) and avoids the False Alarm Rate (FAR). The graphical analysis is illustrated in figure 3



a

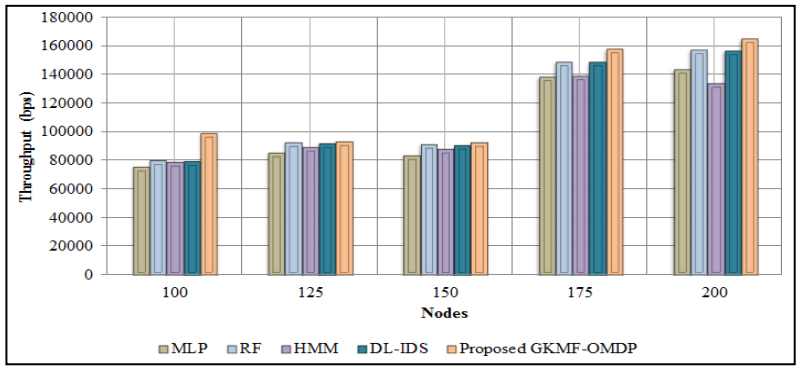


b

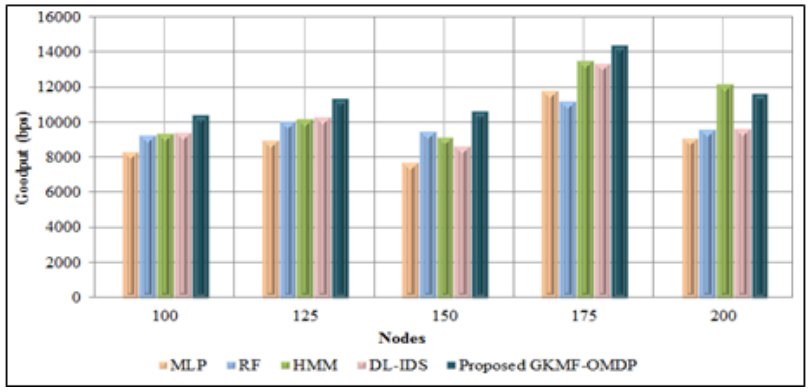
Figure3: Graphical analysis of proposed GKMF-OMDP based on (a) DR (b) FAR

The above figure demonstrates the detecting rate and False alarm rate of the proposed work. Figure 3(a) represents the detecting rate that represents the ratio of correctly detected attacks by a total number of attacks. The higher percentage of DR represents that the model tends to be more secure. According to that, the proposed approach achieves a maximum DR of 94.85% for the maximum node of 200, whereas the existing methods achieve a DR ranging between 85.25%-89.16%, which states an insecure model as compared to the proposed approach. Figure3(b) illustrates the FAR that indicates the attacks that are missed and classified as normal. A low value of FAR makea good model, regarding that the proposed method achieves a FAR value of 0.02 for the maximum network node of 200. After the proposed HMM, RF and DL-IDS achieve a better FAR ranging between 0.05 -0.06 and the MLP model achieves a FAR of 0.15, which is considered to be a worse model.

The observation of secure data is computed using throughput and goodput. Throughput is the number of data delivered per second and goodput is the number of useful data delivered per second. Both the metrics should be high to sustain a secure model. The graphical analysis of throughput and goodput for the proposed approach is represented in figure 4.



a



b

Figure4: Graphical analysis of proposed GKMF-OMDP based on (a) Throughput (b) Goodput

According to the definition, the proposed GKMC-OMDP performs to be more secure by

obtaining a better throughput as well as good throughput as stated in Figures 4(a) and 4(b). The proposed approach achieves a throughput of 165709.13 bps for the maximum network node of 200, whereas the existing approaches achieve a throughput value ranging between 134568.90-157978.75 bps for the network node of 200, which is comparatively lower in data delivery and slow execution than the proposed approach. In terms of good throughput, the proposed approach maintains the security level and also avoids unnecessary information by obtaining a value of 11707.34 bps for the network node of 200 and leads the existing approach with a wide difference value.

5. CONCLUSION

The paper proposes a Reinforcement Learning based IDS in IoT for smart homes. The proposed approach prevents the attack by not only detecting it but also by identifying its occurrence and evolution without any delay. The work performs better under various uncertainties that are caused randomly or under various dynamic situations of the attacks. The work has developed a GKMF-OMDP reinforcement learning to get rid of several real-time attacks and to detect them accurately without any data labels and user interface. The developed model itself gets trained on the IDS by improvising its decision against the attacks with the help of rewards. The work has performed an optimal policy selection for accurate decision-making by using Gaussian kernel membership function-based fuzzy optimization. The proposed IDS technique avoids the False alarm rate (FAR) and performs more reliably under various circumstances for detecting an attack. Experimental analysis declared that the model tends to obtain an accuracy of 94.62% and an attack detection rate of 94.85%. In addition to that, the proposed model reduces the false alarm rate by obtaining a FAR of 0.02. Thus, the proposed model tends to perform well as compared to the existing state-of-the-art method.

References

1. Kelton AP da Costa, João P. Papa, Celso O. Lisboa, Roberto Munoz and Victor Hugo C. de Albuquerque, “Internet of things: A survey on machine learning-based intrusion detection approaches”, Computer Networks, vol. 151, pp. 147-157, 2019.
2. Venkatraman S and Surendiran B, “Adaptive hybrid intrusion detection system for crowd sourced multimedia internet of things systems”, Multimedia Tools and Applications, vol. 79, no. 5, pp. 3993-4010, 2020.
3. Venkatraman Subbarayalu, Surendiran B and Arun Raj Kumar P, “Hybrid network intrusion detection system for smart environments based on internet of things”, The Computer Journal, vol. 62, no. 12, pp. 1822-1839, 2019.
4. Mariusz Gajewski, Jordi Mongay Batalla, George Mastorakis and Constandinos X. Mavromoustakis, “A distributed IDS architecture model for Smart Home systems”, Cluster Computing, vol. 22, no. 1, pp. 1739- 1749, 2019.
5. Mohamed Amine Ferrag, Leandros Maglaras, Ahmed Ahmim, Makhlouf Derdour and Helge Janicke, “Rdtids: Rules and decision tree-based intrusion detection system for internet-of-things networks”, Future Internet, vol. 12, no. 3, pp. 1-14, 2020.
6. Man Zhou, Lansheng Han, Hongwei Lu and Cai Fu, “Intrusion detection system for iot heterogeneous perceptual network”, Mobile Networks and Applications, 2020, doi.org/10.1007/s11036-019-01483-5.
7. Vikash Kumar, Ayan Kumar Das and Ditipriya Sinha, “UIDS: a unified intrusion detection

system for IoT environment", Evolutionary Intelligence, vol. 14, pp. 47-59, 2019.

8. Daming Li, Zhiming Cai, Lianbing Deng, Xiang Yao and Harry Haoxiang Wang, "Information security model of block chain based on intrusion sensing in the IoT environment", Cluster Computing, vol. 22, no. 1, pp. 451-468, 2019.
9. Yahya Al-Hadhrami and Farookh Khadeer Hussain, "Real time dataset generation framework for intrusion detection systems in IoT", Future Generation Computer Systems, vol. 108, pp. 414-423, 2020.
10. Yan Naung Soe, Yaokai Feng, Paulus Insap Santosa, Rudy Hartanto and Kouichi Sakurai, "Towards a lightweight detection system for cyber-attacks in the IoT environment using corresponding features", Electronics, vol. 9, no. 1, pp. 144, 2020.
11. Shuai Jiang, Juan Zhao and Xiaolong Xu, "SLGBM: An intrusion detection mechanism for wireless sensor networks in smart environments", IEEE Access, vol. 8, pp. 169548-169558, 2020.
12. Wenjuan Li, Steven Tug, Weizhi Meng and Yu Wang, "Designing collaborative blockchained signature- based intrusion detection in IoT environments", Future Generation Computer Systems, vol. 96, pp. 481- 489, 2019.
13. Geethapriya Thamilarasu and Shiven Chawla, "Towards deep-learning-driven intrusion detection for the internet of things", Sensors, vol. 19, no. 9, pp. 1977, 2019.
14. Ying Zhang, Peisong Li and Xinheng Wang, "Intrusion detection for IoT based on improved genetic algorithm and deep belief network", IEEE Access, vol. 7, pp. 31711-31722, 2019.
15. Manimurugan S, Saad Al-Mutairi, Majed Mohammed Aborokbah, Naveen Chilamkurti, Subramaniam Ganesan and Rizwan Patan, "Effective attack detection in internet of medical things smart environment using a deep belief neural network", IEEE Access, vol. 8, pp. 77396-77404, 2020.
16. Md Arafatur Rahman, Taufiq Asyharia A, Leong L.S, Satrya G.B, Hai Tao M, Zolkipli M.F, "Scalable machine learning-based intrusion detection system for iot-enabled smart cities", Sustainable Cities and Society, vol. pp. 1-43, 2020.
17. Singh, Sushil Kumar, Young-Sik Jeong and Jong Hyuk Park, "A deep learning-based IoT-oriented infrastructure for secure smart city", Sustainable Cities and Society, vol. 60, pp. 1-22, 2020
18. Sana Ullah Jan, Saeed Ahmed, Vladimir Shakhov and Insoo Koo, "Toward a lightweight intrusion detection system for the internet of things", IEEE Access, vol. 7, pp. 42450-42471, 2019.
19. Kalnoor, G., Gowrishankar, S. "IoT-based smart environment using intelligent intrusion detection system", Soft Comput 25, 11573–11588 (2021). https://doi.org/10.1007/s00500-021-06028-1.
20. Kalnoor, G., Gowrishankar, S. A model for intrusion detection system using hidden Markov and variational Bayesian model for IoT based wireless sensor network. Int. j. inf. tecnol. 14, 2021–2033 (2022). https://doi.org/10.1007/s41870-021-00748-1.