Available online at
www.mdl.mazedan.com

MJCEA

www.mazedan.com

www.mazedan.com/mjcea

IN THE INTERNET OF THINGS ENVIRONMENT, UNAUTHORIZED IDENTIFICATION SYSTEMS

THAMRAJ NARENDRA GHORSAD*[1], SADIK KHAN[2], YOGESH K SHARMA[3], DYUTI BANERJEE[4]

MAZEDAN JOURNAL OF CIVIL ENGINEERING & ARCHITECTURE
e-ISSN:
Article id- MJCEA0103003
Vol.-1, Issue-3
Received: 19 Aug 2021
Revised: 17 Sep 2021
Accepted: 20 Sep 2021

Citation: Ghorsad, T. N., Khan, S., Sharma, Y. K, & Banerjee, D. (2021). In the Internet of Things Environment, Unauthorized Identification Systems. *Mazedan Journal of Civil Engineering & Architecture*, 1(3), 8-13.

Abstract

Over the past few decades, the use of the Internet of Things has become more and more prevalent in human life in terms of industrial development, so many cybercriminals are on the rise, and different ways of carrying out cyber-attacks are being explored. In this connection, many researchers have developed several IoT intrusion detection systems to prevent attacks on IoT and to provide strong security to the IoT system, based on such criteria as system search techniques, authentication strategy, and deployment. In this study, we have a comprehensive overview of contemporary IoT IDS and the techniques, deployment strategies, authentication strategies, and datasets commonly used to build IDS. We have discussed how the previously proposed system detects attacks and how IoT provides stronger security, as well as classified IoT attacks that have occurred so far. Discussions are underway to prevent such attacks in the future and to provide stronger security for the IoT.

Keywords: Internet of Things, Intrusion Detection, Network attack, Machine Learning.

1. INTRODUCTION

Recently Technological innovations and significant improvements in the internet, standards, and procedure architectures have made communication between various IoT-enabled devices called nodes, easier than it was previously. The nodes in the Internet of Things refer to everyday items such as light bulbs, power consumption meters, humidity sensors, temperature sensors, fire sensors, and CCTV cameras, as well as sophisticated items such as frequency symbols (RFID), parking sensing cameras, and a variety of other sensing devices in automobiles [4].

There square measure many utilizations and services by the IoT extending from basic foundation to health care, military, smart home, and agriculture services [5]. Furthermore, the domains protected by IoT services include, but are not limited to, power, retail, transportation, and production. The huge size of IoT networks introduces additional challenges, such as device administration, data longevity, telecommunications equipment, procedure, and safety and confidentiality. There is a wide look into addressing such updated IoT features [5]-[6]. The security and privacy guarantee simple user fulfillment, which is the commercial product of IoT frameworks. The approach that IoT employs enables developments such as decentralized computation and cloud computing, among others. The IoT devices build an outsized volume of knowledge of information thus at that moment typical ways for data assortment, process, and knowledge storage are going to be failing. during this context, we tend to square measure used additionally effective and suitable models to provide the Internet of Things nodes with outstanding method capability and expertise (devices). Among the most effective approaches for embedded device sophistication in IoT-connected nodes is called the machine learning approach. random forest, Decision tree, naive Bayes, Linear Classifiers, Artificial Neural Networks, Supervised Learning, and other machine learning techniques are utilized for intelligence. Such machine learning techniques can be used in a variety of situations, including threat identification, human-computer interaction, video processing, product identification and classification, medical services, automotive sectors, manufacturing units, verification, and so on.As per the detail given above before surveys, this text focuses on the following:

- Classifying varied styles of IoT IDS supported intrusion techniques, and preparation strategies.
- Describing a great effort to form higher IoT security IDS.
- Classification of Internet of Things attacks.
- The challenges of IoT IDS.

2. IOT SECURITY APPROACH

The purpose of this paper is to give a review of the existing requirement for Safety measures, threats, and highly

[1]Department of Computer Science & Engineering, G H Raisoni University, Amravati, Maharashtra, India.
[2]Computer Science & Engineering Department, K. C.E. C. Jalgaon, Maharashtra 425002, India
[3]Vishwakarma Institute of Information Technology, Pune – 411048, Maharashtra (India)
[4]NIMS University Jaipur, Shobha Nagar, Jaipur, Rajasthan 303121
*Corresponding author email- rais.khan@ghru.edu.in

reliable solutions for IoT networks [1]. It suggests a strong security approach for IoT gateways based on ML and ANN [2]. The proposed approach effectively discovered the improper information in the IoT network after inputting some valid and invalid information for anomaly identification. Designed an android-based surveillance app for controlling and analyzing the campuses utilizing electronics and electrical equipment using IoT-enabled sophisticated services to improve cybersecurity and reduce resource utilization [3]. Another security solution relies on a unique credential approach to authenticating IoT nodes, and servers [7]. Several security mechanisms for cloud-based IoT have been offered. For ensuring a safe connection between the client and the cloud applications, the researcher presented a middleware cybersecurity approach for the cloud-based system [8].

3. MACHINE LEARNING APPROACH

This article investigates several areas of ML techniques that are applied in IoT cybersecurity. An artificial neural network [2] was suggested to evaluate the relevant feature and identify valid and incorrect information in the IoT network. The use of an ML technique to collect a massive volume of information from many sources while also ensuring data security [18]. In addition, a hybrid CNN/LSTM approach is utilized to identify DDoS attacks in IoT networks and to assess the trusted node using the DL approach [19]-[21]. Depending on edge computing, an SVM approach is employed to provide the distinction between native and modified data [20].

Recent Work of Ids in IoT

Table 1 Summary of related work of IDS in IoT

S N	Authors	Methods/Techniques Used	Security Threats	Limitation
1	Elvin Eziama et. al.	NB, DT, SVM, KNN, RF	Injection Attacks, Ballot Stuffing, Bad Mouthing	When two matrices are employed separately, efficiency suffers.
2	Size Hou et. al.	RBF, SVM	Code Mutation	All sorts of attacks are not detected by the system.
3	Monika Roopak et. al.	Convolution neural network and Multilayer Perceptron	DDoS	If the database is changed, the effectiveness of threat identification may be affected.
4	Janice Canedo et. al.	Artificial Neural Networks	Man in the Middle and (DoS)	To identify abnormalities in the IoT network, the System provides alternative input entries for legitimate and incorrect input.
5	Nathezhtha. T et. al.	RNN	Conventional	The overall probability of malicious node identification is minimal when an additional node is added to the IoT network.
6	M. Aldairi et. al.	Isolation Forest, SVM	Conventional	To identify malicious activity, the truthful user is necessary to recollect the pattern for weekend activities annotations.

Types Of Ids

Distributed Ids

IoT devices may be able to provide security to other IoT devices. Such distributed IDs are based on a large IoT ecosystem. All of these IoT devices interact with each other and control intrusion detection systems with the help of central servers.

Many deploy distributed architectures using IDS. In such an architecture, subsets are used to check other nodes. Distributed IDS is more advantageous than centralized IDS and is used for incident analysis, to identify the type of attack in the IoT ecosystem, and to prevent attacks. In addition to providing security through IoT devices by detecting IoT botnets in the network. Such data can be used by IoT Botnet to detect infected systems and remove infections from the system as well as help to prevent further spread. Distributed IDS have less control over resources.

Centralized Ids

In a centralized IDS system, intrusion detection systems are housed in boundary switches and designated devices. IoT equipment collects complete information from the network and sends it through a network boundary switch (Benkhelifaet al., 2018). As a result, packets in IDS IoT devices and networks are checked using a switch located in the border switch. However, it is difficult to identify whether the network packet passing through the border switch is inconsistent. Centralized IDS is used to monitor network traffic. This traffic is removed from the network using parameters such as packet capture, and Netflow. Network traffic can also be monitored using a computer-based network. A security mechanism can be introduced at an early stage to protect from external threats using more NIDS.

NIDS has some limitations such as limited ability to check complete data and data transferred across the network using high-speed communication [3]. Strong protection against both external and internal attacks can be provided by using different IDS in many network topologies.

Data in such networks include system calls, various APIs, log files, and data packets that are extracted from attacks in the network. Such data can be used as the main and useful source for classifying intrusive behaviors.

Hierarchical Ids

Hierarchical IDS is a type of network in which clusters of each network are created. Many sensor nodes are connected in a single cluster. Each cluster has a head that monitors each member node and analyzes the entire network.

Ids Validation Strategies

The IoT IDS model system needs to be developed to detect various attacks within IoT and provide security as well as determine their authentication. For the effective implementation of IDS, many researchers have used

various techniques such as theoretical, empirical, and hypothetical strategies in their models.

Following are the performance measuring parameter used in IDS.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$TPR(TruePositiveRate)/Recall/Sensitivity = \frac{TP}{TP + FN}$$

$$Specificity\ or\ True\ Negative\ Rate(TNR) = \frac{TN}{TN + FP}$$

$$Precision\ or\ positive\ predictive\ value\ (PPV) = \frac{TP}{TP + FP}$$

$$F1 - Score = \frac{(2 * Precision * Recall)}{(Precision + Recall)}$$

Table 2 Summary and comparative analysis of various IDS implementation approaches based on their position

Types of IDS System	Data source	Advantages	Disadvantages
Distributed IDS	API, audit file, Pattern Matching, log record, rule-based matching	○ HIDS can check end-to-end encrypted communications behavior. ○ There is no need for additional hardware. ○ Checks the host filesystem, system calls, and network activities for intrusion. ○ This system can reassemble packets ○ Looks at the entire item, not streams only	○ Delays in reporting attacks ○ used a large number of host services and resources ○ Each hot must-haveinstalled. ○ It can only be deployed on a machine that can analyze the attack.
Centralized IDS	○ SNMP ○ TCP/UDP/ICMP ○ MIB ○ Router NetFlow records	○ IoT devices can be overloaded. ○ Detects attacks by analyzing packets in the network. ○ Not required to install on each host. ○ Several hosts can be checked at identical times. ○ Capable of detecting a variety of protocols.	○ The invader can operate the IoT network, if some adjustments may be made to the central IDS system. ○ The difficulty is detecting assaults in encoded data. ○ Specialized equipment is necessary. ○ It is solely capable of detecting only attacks. ○ High-speed connectivity becomes harder to examine ○ High internal risk
Hierarchical		○ For compatibility, the network employs NIDS, HIDS, and wireless intrusion detection technologies. ○ Such an approach is excellent for creating Intrusion Detection in IoT environments that are huge and diverse.	○ High Complexity

Table 3 Security characteristics between personal computers and IoT

Characteristics	Personal Computer	IoTPlatform
Execution Platform Heterogeneity	Low	High
Malware family Variety	High	Low
Intrusion Detection Technique	Easy	Difficult
Internal Analysis	Easy	Very Difficult
Sandbox Execution	Easy	Difficult
Removing Malware	Medium	Very Difficult
Susceptibility Testing	Medium	Very Difficult

4. CLASSIFICATION OF IDS

Figure 3 depicts the cybersecurity aspects of a particular system, which is a collection of equipment linked to a PC and IoT malware. From inside and outside, applications linked with the IoT system can be attacked. An interior intruder may be a compromising node in the network, but an exterior invader is not. The categorization of potential threats that can occur on IoT applications is shown in Figure 1. It also depicts the many forms of attacks, as well as how they would influence the IoT network and what effect they will have.

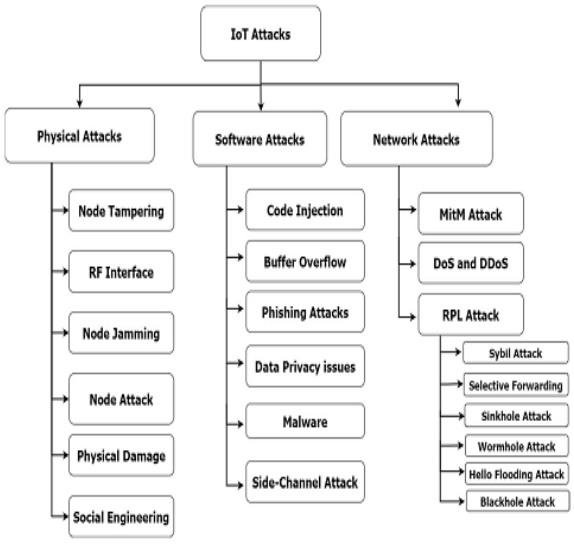

Figure 1Classification of IoT attack

5. APPLICATION OF ML IN IOT

Embedded System

The development of a cryptographic architecture of secure data transmission for an embedded platform based on the

internet of things [13] is a new study in this domain. To offer an embedded system-based data protection approach for employee identification. To verify the information of persons in India, Aadhar checking is used for employee identification [9]. To create a structured way for authority, the guidance of an advantage, starting with a device Safety design that efficiently checks communication utilization and architecture resources. The strategy is built on integrated equipment/software, and software access control principles, as well as the mitigation of threats posed by hidden defects in embedded systems and standards [11].

Smart Homes

This category includes common household appliances such as refrigeration systems, television sets, and lamps that have been designed and can communicate with the authorized person via the Internet, allowing better monitoring and management of electronics devices as well as better energy consumption [17]. To create a more secure home automation system that utilizes various IoT gadgets such as motion or posture detectors, cloud servers, and object recognition, among others. The authenticated person can control the system [3].

Transportation

IoT infrastructure is evolving at a rapid pace, and innovative functionalities are being developed to better everyday life [17]. Determining the IoT's role in transportation is crucial, but what will these developments look like? Where do you think it would be a better strategy for everyone to look for people? We're only now seeing the intersection of IoT and transportation. They can be on a small scale, such as vehicle-to-person communications. To identify the flowing structure in the use of ML techniques in transportation, and to examine the integration and, analysis in each of the transportation classes [17].

Health-care System

IoT and ML techniques have been utilized in the medical industry to obtain the patient history such as health improvements, routines, everyday activities, sleeping patterns, and nutrition [22], as well as to protect the medical or healthcare applications from external threats [24]. In reality, a variety of IoT-based frameworks have been created to track a patient's medical issues. Depending on the inter-IoT approach [23], present a system that makes it easier for patients and doctors to engage.

Security and Surveillance Systems

Across the street, CCTV security cameras can capture the video contributions. Security systems can detect suspicious activity or predict risky situations using continuous visual object recognition.

6. CHALLENGES OF ML IN IOT

Selection of Algorithm, Methods, and Techniques

The machine learning model is implemented using several distinct algorithms and techniques. Despite the concept that computations can be performed within any normal circumstances, several guidelines can be followed to determine which approaches and algorithms should be employed. As a result, while an effective approach and selection of algorithms and techniques are critical elements in the ML approach in IoT, wrong selection results in incorrect outcomes and wastes time, money, and effort.

Selection of Databases

If you enter incorrect data into the ML model, the model gives incorrect results. The proper dataset selection depends on various factors like quality, size, and preparation among others. It is critical to have a tactical separation from predispositions and select material that is completely representative of an instance.

Data Preprocessing:

Data processing involves a variety of procedures, including processing, cleaning, and preparation. Datasets can have missing values, so processing data is a difficult undertaking. To expose attributes and value approaches, investigations are needed, and strategies such as element scalability must be used to prevent particular highlighting from overpowering the entire model.

Data Labeling:

The data processing techniques utilized in Machine Learning are basic and quite effective. Choosing a good algorithm/technique is a very challenging task. It might be a lengthy and arduous task that involves numerous unsuitable actions. Data labeling is required in supervised machine learning. Systems must be capable of understanding data that appears on a screen, what is said in a voice recording, and what is written in a book, among other things. Machine learning may be improved by data labeling, and Intelligence proceeds to advance.

Security concerns:

The vast volume of information created is extremely versatile, but it also raises considerable security risks. Approximately half of the IoT-enabled organizations believe security to be the most significant barrier to IoT implementation. It is really easy to see why, given that over 67 percent of IoT-enabled devices are buying, and how personal information might be at home. These concerns, together with the usual risks associated with shifting visitor data to the cloud server, explain why users are seeking guarantees about the confidentiality of sensitive data.

7. CHALLENGE OF INTERNET OF THINGS IDS ON INTRUSION DETECTION

The most difficult challenge in IDS is detecting a data theft attempt utilizing several tactics. Apart from establishing strategies for new signatures to assess the stealing capability. To enhance the safety of the IoT network in IDS, additional study is required. This is because technology is always changing, and hackers can manipulate data by adopting equivalent approaches when assaulting and entering. As a result, conventional and established methods are still ineffective.

8. CONCLUSION

We give a brief outline of detection and prevention methodologies, remedies, and technological limits in the IoT network in this study. Several academics have developed intrusion detection systems to detect assaults

on IoT platforms, but identifying diverse intrusions in IoT network systems can be difficult. We presented existing study findings and explored ways to increase the functionality of IoT. By examining traditional and existing intrusion detection systems, we were able to identify upcoming problems and investigation areas. We found four critical parameters that are required for constructing a robust IoT IDS using heterogeneous technologies during this research.Firstly, it will issue a false warning if the volume of data in the network is excessive. Second, IoT networks should be scrutinized for unusual activity. Third, create a mechanism to protect against zero-day assaults. Fourth, construct self-contained IDSs using machine learning and deep learning approaches. In conclusion, all we can say is that this review could be quite useful to security experts.

REFERENCES

[1] Fatima Hussain Syed Ali Hassan Rasheed Hussain Ekram Hossain, "Machine Learning for Resource Management in Cellular and IoT Networks: Potentials, Current Solutions, and Open Challenges" ArXiv 2019.

[2] J. Cañedo and A. Skjellum, "Using machine learning to secure IoT systems," 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, 2016, pp. 219-222.DOI: 10.1109/PST.2016.7906930

[3] R. Sarmah, M. Bhuyan, and M. H. Bhuyan, "SURE-H: A Secure IoT Enabled Smart Home System," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 59-63. DOI: 10.1109/WF-IoT.2019.8767229

[4] Hussain, Fatima, Internet of Things; Building Blocks and Business Models, Springer, 2017.

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, Fourth quarter 2015. DOI: 10.1109/COMST.2015.2444095.

[6] Mohamad Noor, Mardiana& Hassan, Wan. (2018). Current research on the Internet of Things (IoT) security: A survey. Computer Networks.148. 10.1016/j.comnet.2018.11.025.

[7] T. Shah and S. Venkatesan, "Authentication of IoT Device and IoT Server Using Secure Vaults," 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, 2018, pp. 819-824. DOI: 10.1109/TrustCom/BigDataSE.2018.00117

[8] H. Garg and M. Dave, "Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-6. DOI: 10.1109/IoT-SIU.2019.8777334

[9] A. Joshy and M. J. Jalaja, "Design and implementation of an IoT-based secure biometric authentication system," 2017 IEEE International Conference on Signal Processing, Informatics, Communication, and Energy Systems (SPICES), Kollam, 2017, pp. 1-13. DOI: 10.1109/SPICES.2017.8091360

[10] M. Singh, A. Singh, and S. Kim, "Blockchain: A game-changer for securing IoT data," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 51-55. DOI: 10.1109/WF-IoT.2018.8355182

[11] F. Siddiqui, M. Hagan and S. Sezer, "Embedded policing and policy enforcement approach for future secure IoT technologies," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-10.DOI: 10.1049/cp.2018.0010

[12] J. Han, Y. Jeon, and J. Kim, "Security Considerations for the secure and trustworthy smart home system in the IoT environment," 2015 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2015, pp. 1116-1118.doi: 10.1109/ICTC.2015.7354752

[13] P. Peniak and M. Franeková, "Extended Model of Secure Communication for Embedded Systems with IoT and MQTT," 2018 International Conference on Applied Electronics (AE), Pilsen, 2018, pp. 1-4. DOI: 10.23919/AE.2018.8501434

[14] J. Shahapure, A. Shinde, Y. Madwanna, V. Sontakke, and P. P. Laturkar, "IoT Based System for Passenger Service in Railways with Secure ICN Architecture," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, 2018, pp. 819-821. DOI: 10.1109/ICOEI.2018.8553938

[15] M. Hagan, F. Siddiqui, S. Sezer, B. Kang, and K. McLaughlin, "Enforcing Policy-Based Security Models for Embedded SoCs within the Internet of Things," 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan, 2018, pp. 1-8.DOI: 10.1109/DESEC.2018.8625140

[16] M. Son and H. Kim, "Blockchain-based secure firmware management system in IoT environment," 2019 21st International Conference on Advanced Communication Technology (ICACT), Pyeong Chang Kwangwoon_Do, Korea (South), 2019, pp. 142-146.DOI: 10.23919/ICACT.2019.8701959

[17] Fotios Zantalis, Grigorios Koulouras, Sotiris Karabetsos and Dionisis Kandris, "A Review of Machine Learning and IoT in Smart Transportation", Future Internet 2019, 11, 94; doi:10.3390/fi11040094.

[18] A. Roukounaki, S. Efremidis, J. Soldatos, J. Neises, T. Walloschke, and N. Kefalakis, "Scalable and Configurable End-to-End Collection and Analysis of IoT Security Data: Towards End-to-End Security in IoT Systems," 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 2019, pp. 1-6.DOI: 10.1109/GIOTS.2019.8766407.

[19] M. Roopak, G. Yun Tian and J. Chambers, "Deep Learning Models for Cyber Security in IoT

Networks," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2019, pp. 0452-0457. DOI: 10.1109/CCWC.2019.8666588

[20] S. Hou and X. Huang, "Use of Machine Learning in Detecting Network Security of Edge Computing System," 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA), Suzhou, China, 2019, pp. 252-256.DOI: 10.1109/ICBDA.2019.8713237.

[21] E. Eziama, L. M. S. Jaimes, A. James, K. S. Nwizege, A. Baldor, and K. Tepe, "Machine learning-based recommendation trust model for machine-to-machine communication," 2018 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), Louisville, KY, USA, 2018, pp. 1-6.DOI: 10.1109/ISSPIT.2018.8705147

[22] F. Ahamed and F. Farid, "Applying Internet of Things and Machine-Learning for Personalized Healthcare: Issues and Challenges," 2018 International Conference on Machine Learning and Data Engineering (iCMLDE), Sydney, Australia, 2018, pp. 19-21. DOI: 10.1109/iCMLDE.2018.00014

[23] P. Pace et al., "INTER-Health: An Interoperable IoT Solution for Active and Assisted Living Healthcare Services," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 81-86. DOI: 10.1109/WF-IoT.2019.8767332

[24] A. K. Alharam and W. El-madany, "Complexity of Cyber Security Architecture for IoT Healthcare Industry: A Comparative Study," 2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Prague, 2017, pp. 246-250. DOI: 10.1109/FiCloudW.2017.100

[25] T. Nathezhtha and V. Yaidehi, "Cloud Insider Attack Detection Using Machine Learning," 2018 International Conference on Recent Trends in Advanced Computing (ICRTAC), Chennai, India, 2018, pp. 60-65. DOI: 10.1109/ICRTAC.2018.8679338.

[26] M. Aldairi, L. Karimi and J. Joshi, "A Trust Aware Unsupervised Learning Approach for Insider Threat Detection," 2019 IEEE 20th International Conference on Information Reuse and Integration for Data Science (IRI), Los Angeles, CA, USA, 2019, pp. 89-98. DOI: 10.1109/IRI.2019.00027

AUTHORS PROFILE

Thamraj Narendra Ghorsad

Ph.D. Scholar, Computer Science & Engineering Department, G. H. Raisoni University Amravati. M.Tech in Computer Science & Engineering, Radharaman Engineering College, R.G.P.V., Bhopal (M.P). B.E. in Computer Science & Engineering, Anuradha Engineering College, Chikhali, Dist- Buldhana, SGBAU, Amravati.

Area of Interest in Network Security, Internet of Things, Machine Learning.

Dr. Rais Abdul Hamid Khan

Professor, Computer Science & Engineering Department, G. H. Raisoni University Amravati Research Area: OS, MDS, ML, CN

Experience: 19 Years.