Retraction

Retraction: A survey on intrusion detection system and prerequisite demands in IoT networks (J. Phys.: Conf. Ser. 1916 012179)

Published 23 February 2022

This article (and all articles in the proceedings volume relating to the same conference) has been retracted by IOP Publishing following an extensive investigation in line with the COPE guidelines. This investigation has uncovered evidence of systematic manipulation of the publication process and considerable citation manipulation.

IOP Publishing respectfully requests that readers consider all work within this volume potentially unreliable, as the volume has not been through a credible peer review process.

IOP Publishing regrets that our usual quality checks did not identify these issues before publication, and have since put additional measures in place to try to prevent these issues from reoccurring. IOP Publishing wishes to credit anonymous whistleblowers and the Problematic Paper Screener [1] for bringing some of the above issues to our attention, prompting us to investigate further.

[1] Cabanac G, Labbé C and Magazinov A 2021 arXiv:2107.06751v1
Retraction published: 23 February 2022
A survey on intrusion detection system and prerequisite demands in IoT networks

Parthiban Aravamudhan1 and T Kanimozhi1,
1Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai – 600062 Tamilnadu, India.
Email ID: parthiamudhan8454@gmail.com, drtkanimozhi@veltech.edu.in

Abstract. Over the past few years the development in the mobile industry and development of internet, network for all, 4G, 5G etc. enabled the ordinary people as well as the elite people to depend upon mobile networks for regular business developments, entertainment, medical and educational needs. Almost all areas of development depend on the so called improvement of the mobile network. As the advantages and flexibility increases, the consumers entering by new registration increase widely and service requirement of existing consumers increase massively. It is mandatory to provide high level of security and dual privacy protection to the users sharing the large set of information through the cloud. The massive crowd sensing is important for any kind of network security system to ensure the detection of any miscellaneous activity entering the network grid. The study is focused on gathering various literature evidences on demand for intrusion detection system, analyzing the pitfalls in current models and creating an idea that would be helpful for us to proceed further with the research on intrusion detection system implementations and innovating a novel methodology that improvise from the present system. The future enhancement and interpretations on solutions would be discussed too.

Keywords: intrusion detection system, network security, cloud security, internet of things, edge detection systems, deep learning, cloud computing.

1. INTRODUCTION
Protecting the network from miscellaneous activity is mandatory and that would save a huge data which may be hacked in suspicious activity. The important part of any system management is to protect it from network hazards and ensuring high level of security [1]. The large amount of confidential data, transaction data, activities and follow ups are uploaded to the network in current days through simple steps. Hence it has become flexible for end users to upload the data more frequently and through hassle free steps. Every time the user login to the particular network it enables the port open to accept all the inputs for a certain period of time frame. This key gap is enough for the hackers and third party users to enter and grab the most privileged information from the network grid. Intrusion detection systems are small tools or software that acts as a ingress guard in the network points to ignore the miscellaneous activity during heavy traffic. The IDS (Intrusion Detection System) provides dual stack security, ensure the authenticated entry to protect the network from Internet attacks. Firewall provides basic security to the system, to protect the grid from third party attacks. [2]

The design of IDS depends on the type of information, quality and weightage of the system. The
system follows certain rules and policies to find out and troubleshoot such online threats, malware attacks or any kind of intrusions and to safe guards both the edge computing devices and data.

1.1 Classification of Intrusion Detection System
Intrusion detection systems are broadly classified as follows:

1.1.1 Network based Intrusion Detection System (NIDS)
The NIDS models are intrusion detection system that is preprogrammed to be initiated at certain node of the internet to monitor and track all internet traffic that comes across the way on all subnets. In case of any miscellaneous activity in the network, an immediate alert will be sent to the administrator. A common example we can discuss is that firewall is being installed in all systems, where anonymous software is trying to crack the protection.

1.1.2 Host based Intrusion Detection System (HIDS)
The meaning of Host here any network connected system or device on IOT. The Host-IDS is able to run independently in host systems, that monitors the network activities, keep track the incoming and outgoing packets and alert the administrator in case of any miscellaneous activity held in the network grid. In some systems, the existing machine controls are getting changed within due to internet malfunctioning software entering the network. HIDS analyzes not only the traffic but also system calls, running process, file-system changes, inter-process communication and application logs. The anonymous software enables the machine to get updated automatically and change the control line etc. are example of host based intrusion detection systems in practice.

1.1.3 Protocol based Intrusion Detection System (PIDS)
In the front-end server, an IDS protocol model is installed, that comprises of system or agent. The model is always interpreting the communication protocol to check between the user device and the server. Most of the systems monitor to secure web server through regular tracking of HTTP protocols.

1.1.4 Application Protocol based Intrusion Detection System (APIDS)
APIDS modules are normally configured within group of servers. They identify the intrusions by monitoring and formulating the communication on specific applications.

1.1.5 Hybrid based Intrusion Detection System (HIDS)
In some cases, the IDS modules are configured as one or more hybrid combination of intrusion detection systems. Study reveals that hybrid intrusion detection system is more robust in security comparing all other methods. The method is tending to be more secure because more than one method of the stacked security is configured together.

1.2 Detection methodologies

1.2.1 Signature based Intrusion Detection System (SIDS)
The concept of signature based IDS implementation approach monitors the specific frame of patterns to be followed in the network in common. The SIDS is also being implemented with the help of previously handled patterns or the miscellaneous activities related steps and instructions to be repeated again. The SIDS is quite similar like malware detection in massive mobile networks or IOT networks.

1.2.2 Anomaly based Intrusion Detection System (AIDS)
AIDS methods are enabled in many systems to provide protection grid that detect the unknown malwares as well as keep track on new malwares developing inside the network. In most of the current scenarios the anomaly based detection of intrusion elements is developed using suspicious detecting machine learning models. In case of any new suspicious activity in the network, the pre-trained
machine learning models create a trustworthy activity which detects and probe the root cause of the problem. They can be modeled or programmed according to the applications and configurations.

1.3 Familiar IDS Tools

*Supersonic Naval Ordnance Research Track (SNORT)* developed by Cisco Systems which is capable of performing real-time traffic analysis and packet logging on IP networks based on interruption discovery framework programming.

*Open Source HIDS Security (OSSEC)* is an excellent host-based interruption discovery framework that performs log analysis, integrity checking, windows registry monitoring, rootkit detection time-based alerting and active responses.

*Suricata* Network-based interruption discovery framework programming works at the application layer for more prominent deceivability.

*Zeek* is an open source software framework for network security monitoring.

*Sagan* is a log investigation instrument that can coordinate reports created on grunt information. So it is a HIDS with a touch of NIDS.

*Security Onion* is a network checking security device comprised of many components pulled in from other free devices which detects and prevents many exploits in the network.

*Advanced Intrusion Detection Environment (AIDE)* is a HIDS for checking the integrity of files for Unix, Linux, and Mac OS.

*Open Source WIPS-NG* Wireless NIDS and interruption anticipation framework from the producers of Aircrack-NG monitors all the 2.4 channels using multiple cards.

*Samhain* is an open-source multiplatform application for POSIX systems (Unix, Linux, MACOS, Cygwin / Windows), which integrates and maintains the log files.

*Fail to Ban* is an intrusion prevention software framework that protects computer servers from brute-force attacks. It is lightweight, host-based interruption identification programming framework for Unix, Linux, and Mac OS.

2. LITERATURE STUDY

[3] The research work proposed an intrusion detection system that decodes the packets and check every time it enters the network. It automatically detects the malwares or miscellaneous activity held. The IDS in this paper is implemented with alert system that produce sound in case of any suspicious activity held.

Conducted research work on intrusion detection and prevention system through deep learning algorithms. They utilized kddcup99 dataset for testing and training. The implementation is divided into two categories, one for intrusion detection system and another for intrusion prevention system. The proposed system uses MLP (Multi Layer Perceptron) for batch processing and achieved 91.4% accuracy in prediction.

Developed research work on novel triple intrusion detection system, in which the IDPS ensures secure connection with SDN-IOT in terms of failure analysis, accuracy, precision, delay, traffic crown sensing etc. They have used fuzzy based authentication system. They have concluded with further...
improvements needed with privacy preserving model with new authentication technologies.

[4] The proposed paper uses mutual authentication scheme that analyze outdoor resilience and indoor resilience that covers the attacks such as Relay attacks and MITM attacks, quantity attacks etc., They concluded that sophisticated protocols enable better security on IOT networks.

[5] They proposed a research paper with machine learning approach for cyber-attacks detection using Bayesian networks. The system focused on query based attack detection system. The conclusion of the paper provides that effectiveness of the signature based method need to be improved and robust authentication IDS are required.

[6] Research work on mobile ad-hoc network based smart IDS is evaluated for MANER-Security. They have utilized artificial neural network (ANN) for data packets classification. They stated that classification plays a major criteria in intrusion detection. Boat classifier is developed here. The system is efficient in rare attacks, Dos and probing problems are discussed [7].

[8] Their study is on home level intrusion detection system, using Wifi-Enabled IOT devices. They implemented a RSSI (Received signal strength indicator) based identification router that incorporate with a detection algorithm and visualize the whole home security through IOT. The idea of IOT security with RSSI gives apt results for them, that they concluded proposed design optimizes accurate detection.

[9] Proposed study and implementation on IDS in edge routed networks that blend with Dos attack analysis, edge network intrusion detection, edge node cloud security etc., SDMMF single-layered Min-max fair allocation scheme is used. The concluded paper states that they have given efficient solution for multi-layer resource allocation problem [10].

[11] Their study is focused on challenges and imbalances within the supervised ML algorithms, real-Time interfaces and NFV - Network Function Virtualization which creates a new working paradigm. Moreover ML requires more cloud security protocol for frequently changing cloud environment.

[12] The study conducted to learn about the challenges in intrusion detection system in-terms of performance, privacy preserving authentications and energy consumptions over the network etc. This paper also discussed about the limitations of the deep information gathering, the challenges in IDS systems, research overlaps and obstacles etc.

3. ARCHITECTURE OF IDSS IN IOT NETWORKS

Intrusion detection support system architecture model contains the knowledge base or the database that contains numerous information formulated into a certain form to read and process in the network easily. An intrusion detection system of IOT network operated in two different nodes. (1) as standalone system and (2) as collaborative system.

3.1 Standalone Intrusion Detection Support System (SIDSS)

SIDSS depends on the traffic patterns and enable the continuous tracking of data within the network. The SIDSS doesn’t need any information on the behavior of the user and domains. The IDSS is designed with efficient algorithms that learn the behavior of the network and data entering the network. It filters the users accordingly and isolate the pattern of attack generated.

3.2 Collaborative Intrusion Detection Support System (CIDSS)

In IDSS on IOT applications, the collaborative based approach is being divided into three categories. Centralized CIDS consists of mechanism that was placed in the central portion of the network. The advantage of placing the CCIDS is to keep an eye on all data coming from every side. The central
monitor keeps the data for further analysis. Each monitor connected with the CCIDS that grab the information from the local network traffic.

3.2.1 De-Centralized Intrusion Detection Support System (DCIDSS)

De-Centralized IDSS are network that follows the hierarchical topology that contains the monitoring point of self-routed multiple monitors. The data coverage become narrow, hence incase of back-tracing the miscellaneous behavior become quite easier comparing with the centralized scheme. The control and monitoring of the hierarchical data within the network reduces the unnecessary usage of network spaces.

Distributed CIDSS is the concept of distributing the tasks over the network to the all monitors and hence all the monitors also act as a central IDSS. Mostly these kind of DCIDSS uses peer-peer kind of architecture so that the communication between the monitors follows certain clarity and tasks are equally distributed.

3.3 Internet of things

The great role of internet of things is to provide wide coverage on connectivity of devices that provide flexible connectivity with users and cyber world. It connects and communicates with different applications and enables the internet to act as a medium for transferring data with hassle free services. Because of growth in internet of things in current scenario, the device is able to connect with small applications to complex applications, to provide connectivity between home appliances [13], IoT operations, general connectivity, etc., Data collection act as the important factor in growth of IoT in figure 1.

![Figure 1. Architecture of IDSS in IOT Networks](image)

The data can be primary data and secondary data. The data are collected from sensors, camera, signal generators, text, video, etc., The data collection phase are designed to act [14] with node communications, constraints about the distance of the node, connecting priority nodes etc., the protocols are designed in such a way to provide efficient IoT connectivity strategies in figure 2.

![Figure 2. Architecture of IOT networks](image)
The increased demand on IOT access is the major factor for need for robust IDS in massive internet networks. The Strength of IOTs network depends on the effective data read and feature extraction capabilities [15]. So many third party cloud service vendors available in current epoch make the cloud weighted and crowded. This kind of IDSS is mandatory at the edge computing of the Cloud services. The importance of IDSS is reflected at the IOT gateway frameworks.

3.3.1 Limited Resources
The IOT systems have limited resources that contain constrained process of data, limited storage, and levels of accessibility.

3.3.2 Multi-Level attacks
The intrusion detection system undergoes multiple levels of attacks attempting the specific vulnerable attack protection. Even though such dangers have been examined in different spaces, for example, portable, existing recognition frameworks for IoT exclusively center around the recognition of individual dangers skeptic of likely connections between them. We accept the dynamic idea of the IoT frameworks makes the test.

3.3.3 Device Protection
In order to safeguard detection systems from vulnerable attacks, the device need to be protected using in-built IOT protection modules.

3.3.4 Data collection
All examinations depend on the train data available with us. The collection of accurate dataset becomes tough nowadays. We accept further examination into committed honeypots for IoT frameworks is required and will be critical in encouraging careful assessment of future interruption discovery draws near.

4 ANALYSIS OF CURRENT IDS APPROACHES

4.1 Placement
In spite of so many concurrent occurrences of computing platforms, to place the IDSS module within the network is a challenging task. The limitations of own host computer enable the limited data reading capability of the network. To provide a robust dual stacked protection, it is important for IDSS systems to associate with the massive IOT networks. Strong malware detection and prevention system [16], combined with system call protection, firewall protection need to be considered.

4.2 Detection Time-Frame
The IOT systems are dynamic in nature. Hence in the fast moving dynamic IOT data packets, keeping an IDSS that provide security as well as detect an attack is to be given limited time frame. Responding to such attacks dynamically within the given time frame needs highly efficient approaches that detect and treat the miscellaneous threats. [17].

4.3 Detection Engine
It is required to implement smart detection engines that have strong analyzing capacity with respect to the input malfunctions. They have to treat the malwares as well as to respond the attacks in time. The processing time and analysis epochs need to be controlled programmatically. Software like MATLAB Python are used for developing such robust algorithms in IDSS modules. Regression algorithms, self-organized mappings are suggested models for pattern prediction and fast analysis of complex network inputs. The IOT data are massive and in future the establishment and advancement need to be fulfilled the potential needs of the network [18].
4.4 Architecture modeling
As discussed in Sec III., Standalone or collaborative architecture is chosen based on the crowd capability of the network devices. With respect to the edge router the architecture may be collaborative or distributive. Most of the literature suggests that collaborative approach suits the increasing demands on IDSS in IOT networks.

4.5 Attack Types
The IDSS implementation also considers the type of attack that frequently hit the edge computing devices. The analysis can be made through studying the pattern of highlighted attack history. As discussed in Sec I-B the attacks would be anomaly attacks or signature based authentication attacks.

4.6 Detection Performance
The detection performance of any installed IDSS modules are determined by the success rate of accurate detection of malware attacks, prediction and prevention of such vulnerabilities in the IOT networks. The effectiveness of the attack prediction depends on the fundamental attributes of the IDS. The approach performance is measured through the False positive rate and True positive rate. The accuracy, precision and recall are the parameters that impact the performance measure of the IDSS implemented approaches Figure 3.

![Figure 3](image)

**Figure 3.** Analysis of Current IDS approaches

4.7 Scalability
In terms of increasing demand for IDSS in all networks, in order to address the raising problem of all devices, significant scalability of IDSS systems is required in table 1. The future implementations are suggested to focus on improving the scalability factor of the IDSS in IOT networks. Massive IOT systems need adaptive and predictable IDSS modules in the network. Machine learning approach with incorporated in each IDSS module enable the future IDSS platforms with more robust undoubtedly.

| S1.no | Research Title                                | Author                  | Year | Algorithm implemented                              | Drawbacks                                                                 |
|-------|-----------------------------------------------|-------------------------|------|---------------------------------------------------|--------------------------------------------------------------------------|
| 1     | Machine Learning Techniques for Cyber Attacks Detection | Rafał Kozik and Michał Choraś | 2014 | (LESG) Length based Signature generation Algorithm | The client can just sign archives on that specific PC, the security of the private key relies completely upon the security of the PC |
| No | Title                                                                 | Authors                                                                                   | Year | Model/Method                                                                 | Comments                                                                                                      |
|----|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------|------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| 2  | Feasibility of supervised learning for cloud security                | Bh, Deval & Salman, Tara & Samaka, Mohammed & Erbad, Aiman & Jain, Raj                   | 2016 | Logistic Regression                                                          | High reliance on a handling the presentation of your data                                                  |
| 3  | An Adaptive and Robust Device-Free Intrusion Detection Using Ubiquitous WiFi | Yue Jin, Z. Tian, Zhenyuan Zhang                                                         | 2018 | Non-Parametric statistical method                                             | Less efficient comparing with Parametric models.                                                            |
| 4  | Optimization-Oriented Resource Allocation Management for Vehicular Fog Computing | Fuhong Lin, Yutong Zhou and Giovanni Pau                                                | 2018 | Region Based Trust aware Model                                                | Disparate, distributed and disconnected nodes are carrying sensitive messages.                               |
| 5  | Key Free authentication protocol                                      | Zhigang Huang, Lei Zhang, Xinyu Meng and Kim-Kwang Raymond Choo                         | 2019 | AES                                                                          | It uses too simple algebraic structure. Every block is always encrypted in the same way                   |
| 6  | An adaptive intrusion detection and prevention system for Internet of Things | Sheikh Tahir Bakhsh, Saleh Alghamdi, Rayan A Alsemirani and Syed Raheel Hassan           | 2019 | Self-schedule and self-distributive MAC scheduling                           | Less effective on energy efficiency                                                                       |
| 7  | Intrusion detection and prevention in AdHoc networks                 | M-Islaabudeen, M.K. Kavithaa Devi                                                         | 2020 | ANN                                                                          | Prunes to over fitting and more computation time.                                                          |
| 8  | Intrusion Detection system in IoT networks                            | Mohammad Dawood Momand, DrVikas Thada, and Mr. Utpal Shrivastava                         | 2020 | Light Weight PCA                                                             | Accuracy is poor for data which is not standardized                                                        |
| 9  | Intrusion detection and prevention system                             | Akhil Krishna AshikLal M.A., Athul Joe Mathewkutty, Dhanya Sarah Jacob and M. Hari       | 2020 | Neural Network Learning                                                      | Uncertain behaviour of neuron selection and hidden layers                                                 |
5 DISCUSSIONS

It is evident from the literature reviews above that the demand in intrusion detection support system is quite increasing with respect to the increased population of users approaching IOT networks. To safeguard the user and the edge computing devices, efficient intrusion detection, prediction and analysis system is mandatory in near future. Reviews of convey us the basic idea on intrusion detection systems, the prediction models using neural networks and the results which were discussed. Stated the privacy preserving key authentication protocols and the need for improvised dual stack security in demand. Explains the machine learning impacts on implementing the strong security wall on intrusion detection systems. Allocations of space and system connectivity needs were discussed. Analysis of IDS in cloud security is another important factor that needs to be taken care of during the installation of IDS.

6 CHALLENGES AND FUTURE DIRECTIONS

• Guaranteeing a successful deployment of network.
• Dealing with the high volume of alarms.
• Comprehension and researching cautions.
• Realizing how to react to dangers

As a major aspect of this examination, we have played out a careful survey of existing endeavors to address one of the basic parts of IoT security i.e., interruption recognition. In past areas, we have introduced an exhaustive record of the best in class inside this space and a careful similar examination of individual methodologies. In this segment, we feature significant future examination bearings which require further examination and endeavors to improve generally speaking security of an IoT framework.

7 CONCLUSION

Emerging growth of Internet of things and increased demand of users for flexibility, a number of unauthorized applications take control of the device like computers, mobile devices and many smart connectivity enabled devices. The need for intrusion detection and support system and the challenges in existing implementations are discussed. The need for providing dual stack security enabled authentication protocols are highly required in edge computing devices and centralized IDSS become more compulsive things in IoT environment. The study reveals the challenges in developing an efficient IDSS and discussed in depth about the approaches that need to be improved. It is clear from the study that there is a need for robust IDSS modules in dynamically changing environments of massive internet of things. It provides evidence that random attacks and unauthorized third party entry would be highly controlled. Keeping such valuable points, further research work improved by implementing adjustable IDSS frameworks, to safeguard the IoT networks from dynamically challenging changes and attacks.

REFERENCES

[1] Sheikh Tahir Bakhsh, Saleh Alghamdi, Rayan A Asemmeari and Syed Raheel Hassan, An adaptive intrusion detection and prevention system for Internet of Things SAGE open access journal in Soft Computing in Intrusion Detection System, published Volume : 15 Issue : 11 published Year 2019.
[2] Akhil Krishna, Dhanya Sarah Jacob, Ashik Lal M A, Hari M and Athul Joe Mathewkutty Research on Intrusion Detection & Prevention model Using Deep Learning, International Conference on Electronics and Sustainable Communication Systems (ICESC), ISBN: 978-1-7281-4108-4, published Year 2020.

[3] Amir Ali and Muhammad Murtaza Yousaf, Research entitled Novel three-tier Intrusion Detection and Prevention System in Software Defined Network, in IEEE Open-Access Volume : 8, ISSN: 2169-3536, Year 2020.

[4] Zhigang Huang ; Lei Zhang ; Xinyu Meng ; Kim-Kwang Raymond Choo, Key-Free Authentication Protocol Against Subverted Indoor Smart Devices for Smart Home, IEEE Internet of Things journal, Volume: 7, Issue: 2, ISSN: 2327-4662, published Year 2019.

[5] Rafal Kozik & Michall Choras, Machine Learning Techniques for Cyber Attacks Detection, Advances in Intelligent Systems and Computing book series Springer International Published Volume: 233, ISBN: 978-3-319-01621-4, published Year 2014.

[6] M Islabudeen and MK Kavitha Devi A Smart Approach for Intrusion Detection and Prevention System in Mobile Ad-hoc Networks Against Security Attacks, Wireless Personal Communications Springer International published Year 2020.

[7] Nadia Chaabouni, Mohamed Mosbah, Akka Zemmari, Cyrille Sauvignac and Parvez Faruki, Network Intrusion Detection for IoT Security Based on Learning Techniques, in IEEE Communication Surveys, Volume: 21, Issue: 3, ISSN: 1553-877X, Published Year 2019.

[8] Yue Jin, Zengshan Tian, Mu Zhou, Ze Li and Zhenyuan Zhang. A Whole-Home Level Intrusion Detection System using WiFi-enabled IoT International Wireless Communications & Mobile Computing Conference (IWCMC), ISS: 2376-6506, Published Year 2018.

[9] Fuhong Lin, Yutong Zhou, Xingsuo An, Ilsun You, Fair Resource Allocation in an Intrusion Detection System: Ensuring the Security of Internet of Things Devices, IEEE conference on Consumer Electronics Computing Magazine, Volume: 7, Issue: 6, ISSN: 2162-2248, publishedYear 2018.

[10] Mohammad Saeid Mahdavinejad, Mohammadreza Reyvan, Mohammadamin Barekatain Peyman Adibi, Payam Barnaghi, Amit P Sheth Machine learning for internet of things data analysis; a survey Digital Communications and Networks Science Direct, Volume:4, Issue 3, Pages: 161-175, published Year 2018.

[11] PrakashDuraisamy, XiaohuiYuan, ElSaba,A. and Sumithra Palanisamy, Contrast enhancement and assessment of OCT images, Proceedings of International Conference on Informatics, Electronics & Vision (ICIEV), 2012 Date: 18-19 May 2012 pp.91-95(Location : Dhaka, Print ISBN: 978-1-4673-1153-3,INSPEC Accession Number: 13058449, Digital Object Identifier :10.1109/ICIEV.2012.6317381)

[12] Sumithra M. G., Thumashkodi, K. and Helan Jenifer Archana, A. A New Speaker Recognition System with Combined Feature Extraction Techniques , Journal of Computer Science, Vol. 7, Issue 4, pp.459-465, 2011. (With impact factor SNIP of 0.162 and SJR 0.034).

[13] Balasaraswathi, M., Srinivasan, K., Udayakumar, L., Sivasakthivelan, S. and Sumithra, M.G., 2020. Big data analytic of contexts and cascading tourism for smart city. Materials Today: Proceedings.

[14] Sivakumar, P., Boopathi, C.S., Sumithra, M.G., Singh, M., Malhotra, J. and Grover, A., 2020. Ultra-high capacity long-haul PDM-16-QAM-based WDM-FSO transmission system using coherent detection and digital signal processing. Optical and Quantum Electronics, 52(11), pp.1-18.

[15] Jinug Seok, Moonseok Choi, Jimyung Kim and Jonsung Park A Comparative Study on Performance of Open Source IDS/IPS Snort and Suricata, Journal of the Korea Society of Digital Industry and Information Management, published Year 2016.

[16] Yakuta Tayyebi and D. S. Bhilare Cloud Security through Intrusion Detection System (IDS): Review of Existing Solutions, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 4, Issue 6, published Year 2015.
[17] J. Smith, Machine Learning With Matlab: Supervised Learning and Regression CreateSpace Independent Publishing Platform, published Year 2017. (FiZic-Format).