A Systematic Approach to Prevent Threats Using IDS in IoT Based Devices

Vinod Kumar[1], Sachin Kumar Gupta[2,3,*], Abid Hussain[4], and Amit Sharma[4]

ARTICLE INFO

Article history:
Received: 24 July 2023
Revised: 29 August 2023
Accepted: 16 September 2023

Keywords:
ACAAS
Deep learning
Custom features
Intrusion detection system
Embedded systems
IoT security

ABSTRACT

Due to the enormous volume of data produced by the IoT, effective intrusion detection is necessary to protect confidential and sensitive information before an attack. This article presents a five-layered system for detecting intrusion in huge datasets. This work uses the construction of brand-new specialized features to increase the rate at which the machine model learns and decrease misperceptions while it is learning. We first examine the literature for the most important problems and difficulties. We also suggest a course of action using several important design principles for search strategy support tools in systematic literature reviews. The limitations of this study may include constrained testing scenarios that might not encompass the full spectrum of real-world IoT threats, potential challenges in accurately simulating all possible attack vectors, and the dependence on available machine learning algorithms which might not cover emerging threats comprehensively. Additionally, the study's outcomes might be influenced by the selected hardware and software configurations, potentially limiting the generalizability of the results across diverse IoT device types and environments.

1. INTRODUCTION

Technology in numerous areas of life has converted thanks to the Internet of Things (IoT). People and objects are continually connected through the Internet of Effects conception. Perception, network, and operation situations make up the three layers of the Internet of Effects armature. Security norms must be applied at every subcaste to guarantee the stability of the Internet of Effects [1]. Likewise, as technology advances, so do bed subsystems' vulnerabilities. As a result, bedded security must be considered while creating bedded systems. We'll be suitable to develop new online services and apps thanks to the Internet of Effects (IoT), a technological development that allows communication between humans and machines as well as between the two. Trust is essential when it comes to IoT products and services. To give effective security through social geste analysis and ethical operation of IoT technology, as well as to help system element damage from unacceptably high pitfalls, IoT security bias and networks need to be covered and delved into [2].

It has been established that the Web of Effects (IoT) fabrics include sins that make them vulnerable to several assaults. Pitfalls can arise from enterprises with availability, confidentiality, and other aspects of security. It's also possible to lose important data. Monitoring IoT bias and vulnerable coffers makes it possible to identify the attack types most likely to target affordable IoT bias [3]. Due to the massive amount of data that IoT devices generate, it is exceedingly difficult to identify dangers without trustworthy tools. Intrusion detection systems (IDS), which are defensive technologies that monitor the network activity of Internet of Things devices, may provide this level of protection. Network traffic may be examined by an IDS, also known as an intrusion detection system, to spot various security risks and exploited vulnerabilities [4].

IDS keeps track of traffic and reports its findings to administrators to let them know if anything is out of the ordinary. The intrusion detection system keeps an eye out for signs of penetration on the system's networks. The framework for interruption location inspects network infrastructure [5]. The security information and events management systems notify the administrator when they see unusual behavior [6]-[8]. When the security system detects suspicious behavior, it issues an alert. The network layer is one of the layers that make up the Internet of Things. This layer transmits information bundles between has and is built below the standard layers used for web communication. The network layer, a key component of the IoT architecture,

[1]*Department of Computer Science Engineering, Galgotias University, Greater Noida, U.P., India,*
[2]*Department of Electronics and Communication Engineering, Central University of Jammu, Samba-181143, Jammu (UT of J&K), India*
[3]*School of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, Katra-182320, Jammu (UT of J&K), India.*
[4]*School of Computer Applications, Career Point University, Kota, Rajasthan, India..*
**Corresponding author:* Sachin Kumar Gupta; E-mail: sachin.ece@cujammu.ac.in.

contains several components and is susceptible to a variety of security issues. Several security frameworks have been implemented to address these issues [9]-[11]. Figure 1 depicts the intended IoT environment for the IDS Framework.

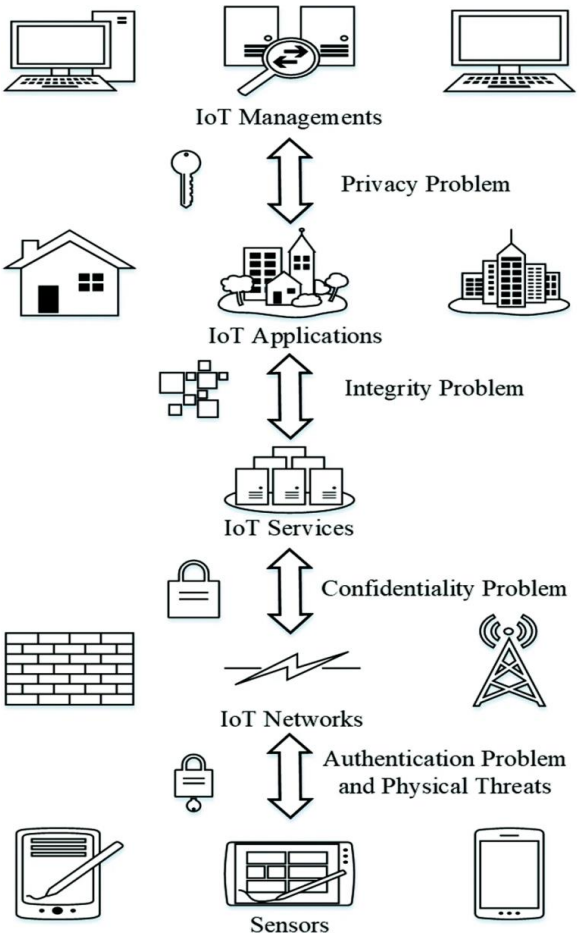

Fig. 1. Proposed IDS and IOT Framework Environment.

The discussion of the proposed IDS and IoT framework environment highlights the innovative approach presented in this study. The framework demonstrates the integration of intrusion detection systems (IDS) within the context of IoT, offering a systematic solution to address the growing security challenges in IoT-based devices. By combining well-established IDS techniques with the unique characteristics of IoT environments, the framework aims to enhance the overall security posture of IoT systems. The discussion delves into the effectiveness of the chosen IDS methods within this specific context, emphasizing their adaptability to the resource constraints and diverse communication protocols prevalent in IoT networks. Additionally, it addresses the feasibility of real-time monitoring and threat detection, discussing potential trade-offs between accuracy and computational efficiency. Furthermore, the discussion might explore the potential scalability of the proposed framework to accommodate an increasing number of IoT devices, as well as its potential integration with existing security measures. Overall, the discussion critically examines the strengths and limitations of the proposed IDS and IoT framework, shedding light on its significance within the broader landscape of IoT security.

New network behavior must be evaluated and modeled in terms of trustworthiness when making use of machine learning. Strategies for AI consider the best model for managing the gigantic and ceaseless measure of information given by IoT gadgets [12]. A method for dispersing understandings and expectations in light of top-to-bottom examination of information designs is called profound learning (DL). In IoT environments, a variety of DL techniques are utilized to identify abnormal behavior patterns. We can demonstrate a forecasting framework that is both successful and versatile concerning investigating and grouping unstable and unpredicted interruptions, which are intrinsic in unique assault methods. DL methods let us accomplish this. Lacking in the study are both the evaluation during prediction, of false-positive (FP) and false-negative (FN) rates, as well as the analysis of features' misperception-related characteristics during learning [8, 10].

The IoTID20 dataset is used by the suggested model to forecast intrusions. The approach reduces the possibility of misunderstanding during learning by producing a collection of fresh characteristics from a dataset to close the gaps in earlier studies. If misunderstandings were removed, the FN and FP rates would go down while the prediction's accuracy would rise [11, 13]. The IoTID20 Dataset is suggested in this research as a mechanism for identifying IoT device incursion in smart homes and medical settings. The prediction system recognizes the incursion and accomplishes the following goals using a deep learning method [14, 15].

- The dataset's data are encoded into a special format as part of the pre-processing procedure so that characteristics may be assessed further during prediction. Rows and columns that are unnecessary are also eliminated.
- To avoid misperceptions during feature evaluation, innovative custom features are derived from the clean dataset.
- By using the feature selection approach on the clean set, significant features for prediction are discovered. Prediction accuracy is evaluated using both the relevant feature set and the unique feature set. The three cutting-edge deep learning algorithms CNN, ANN, RNNBiLSTM, and BSP were used to classify the incursions. (Binary space partitioning) models. For a precise evaluation, the models combine the two deep learning algorithms.

1.1 Research Commitments

The following are the research commitments of the present study:

- Likelihood of further developing IDS models with a cleaned-up dataset.
- Develop a custom list of capabilities to stay away from misperceptions of information.

Applying the significant feature selection algorithm to a dataset that is free of clutter. Using custom features to forecast attacks in large datasets. Verified the prediction accuracy using customized and significant feature sets.

1.2 Scope of Work

The scope of work involves an in-depth exploration of IoT security challenges and threats through comprehensive literature review, followed by the design and integration of an effective intrusion detection system (IDS). This systematic approach encompasses selecting suitable detection techniques, implementing them within IoT devices while considering resource constraints, and evaluating the system's performance, accuracy, and robustness against various attacks. The study also focuses on user interface design, alerts, documentation, and recommendations for future enhancements, ultimately aiming to provide a holistic solution for preventing threats using IDS in IoT-based devices [16]-[22].

The rest of the article is organized as below: section 2 presents the review of literature in the domain. Then, section 3 discussed the proposed methodology and performance evaluation. Finally, section 4 concluded the article with its future scope.

2. REVIEW OF LITERATURE

When a secure existent or business is denied access to services they would naturally anticipate, similar to the internet, dispatch, or network connectivity, it's known as a distributed denial of service (DDoS) assault. DDoS is an issue with resource overuse. Latha, S. S, and Goud, S. et. al. (2023) Securing IoT-enabled cyber-physical systems (CPS) poses challenges due to the inadequacy of conventional security measures from IT/OT systems [1]. This research proposes a two-level ensemble attack detection framework for industrial CPS, featuring decision trees and deep neural networks, demonstrating superiority over comparable methods using real data. Bertoli, G.D.C.; and Alves, P. J. L. et. al. (2023) Amid evolving digital transformation, securing vast networks is challenging due to networking reliance and security design complexities. Data-centric ML approaches like stacked-unsupervised federated learning prove effective, overcoming contextual limitations in network security, showing superior performance and adaptability across diverse data silos [2]. Alsharif, N.A.; and Mishra, S. et. al. (2023) Addressing IoT vulnerabilities, this research combines ML and blockchain to heighten security and privacy, yielding a 99.9% accurate intrusion detection system using Random Forest on simulated attack data. Blockchain enhances security via a tamper-proof decentralized communication system, guarding against cyber threats in IoT networks [3]. Analogous to a big crowd swarming a storefront, a DoS or DDoS assault prevents genuine consumers from entering and disrupts commerce. Lee et al. coffers are effects like memory, CPU time, bandwidth, train descriptors, and buffers. Easy information interchange between billions of individuals, systems, and objects has consequences. Real-world examples are abundant [7]. This study looks at the revolutionary IoT. The globe is impacted by our technology, energy, and purchases. The Internet of Things is a platform for the future, not a tactic or technique. Karl Steinbach, a German computer scientist, predicted that most industrial machines will have computers in a few decades in 1966. Due to global connectivity and an increase in internet-connected devices, the Internet of Things is limitless.

Bushwhackers bombard the vicious resource with a flurry of packets or a single sense packet, which can spark a chain response that depletes the resource's limited force (Junior and Kumar, 2021). A typical DDoS attack takes advantage of an excrescence in one computer system to transfigure it into the DDoS master. The assault master system locates other vulnerable systems and seizes control of them by infecting them with malware or guessing the dereliction word of a system or device that's constantly used to get beyond authentication walls. DDoS assaults passed frequently against every business between 2000 and 2004. The DDoS assault was first reported by Canada's Computer Incident Advisory Capability (CIAC) in the summer of 1999. For case, on April 4, 2013, the price of virtual currency was modified to beget a change with unstable pricing, making Tokyo- grounded Mt. Gox the target of the topmost DDoS assault on a coin exchange. The opponent also gave the dealers access to Fitri (2021) Alley Cat and Ross' error runners. Meanwhile, a fresh Spamhaus crusade has devastated nonprofits with locales in the UK and Switzerland. With 300 gigabits per second of data under trouble, this is one of the largest DDoS cyber-attacks ever (2022). In addition, Microsoft blazoned at the end of August 2022 that its Azure pall service had eased a distributed denial of service attack of 2.4 terabits per alternate — the company's largest DDoS attack to date and the alternate-largest DDoS attack ever recorded (2022).

2.1 Research Gap

An analysis of related exploratory theories and research revealed that the bulk of the study used benchmark datasets that rely on intrusion detection systems (IDS) for such DDoS assaults. The UNSW-NB15-based interruption discovery framework, the NSL-KDD evaluation study, and other similar projects may all benefit from this method of data gathering, which is in demand and underutilized in research based on the IoTID20 dataset. One of the most difficult problems, according to a related research, is that the benchmark datasets NSL-KDD and UNSW-NB15 are

unable to withstand the most current IoT-based assaults, which results in a poor prediction level.

2.2 Motivation

One of the important factors in making this work is also the maturity of trouble on host- and network-grounded intrusion discovery. As a result, the trouble was motivated to concentrate on inflow- and IoT- grounded intrusion discovery. The system used to gain pivotal data and include it in the vaticination also had an impact on the product of this work. Deep literacy approaches were proposed as a result of these issues since rule-grounded, data mining, and machine literacy systems are unfit to prognosticate unborn IoTID20 attack patterns and tend to misinterpret attacks.

3. PROPOSED METHODOLOGY AND PERFORMANCE EVALUATION

In this section, the proposed model and data extraction layer with data acquisition components are discussed.

3.1 Proposed Model

The innovative custom feature of the dataset, in addition to the standard features, is an essential component of the design of the system that provides an effective IDS and detects intrusions within the IoT context. The suggested model's five-layer design, which contains several elements for forecasting the assault, is in Figure 2.

3.2 Data Extraction Layer with Data Acquisition Component

Data Parser, Cleaner, and Field Encoder Components in the Pre-Processing Layer Construction Layer with Custom Constructor Components for Attributes Selection Layer with Components for Attributes Attack Recognizer Components in the Detection Layer.

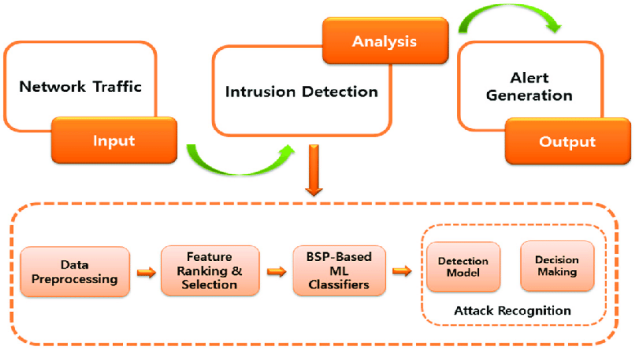

Fig. 2. Proposed model based on IDS to protect from DDoS Attack.

3.3 Performance Evaluation

The calculation time of the Bulk Synchronous Parallel (BSP) ML classifier depends on factors such as the complexity of the dataset, the chosen algorithm's computational demands, the parallel processing capabilities of the system, and the efficiency of data distribution and synchronization during the parallel execution. Generally, BSP classifiers divide computation into super steps with synchronization points, potentially reducing parallel efficiency due to synchronization overhead. The actual calculation time can vary significantly based on these considerations, making it essential to assess the specific characteristics of the classifier, the dataset, and the hardware setup to estimate its performance accurately.

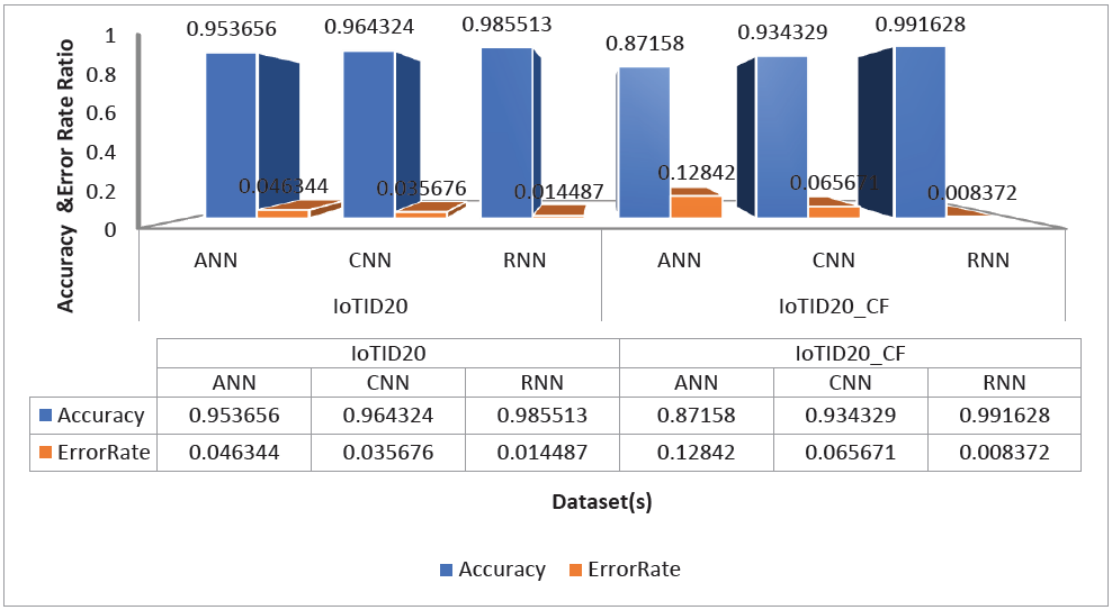

Fig. 3. Result analysis of the proposed model.

Python 3.2 is used to implement the framework in Anaconda. Windows is powered by a 64-bit Intel Core i7-4600M CPU operating at 2.90 GHz, 16 GB of RAM, and an 8 GB GPU. The recommended model is demonstrated to perform better than others in terms of vaticination delicacy and error rates when the mileage of the model is estimated. The performance measures handed below are used to indicate how well the proposed model performs. Figure 3 displays the advised parameters for the bracket error rate and the vaticination delicacy rate. The suggested classifier, Double Space Partitioning (BSP), has a high delicacy rate of99.16 and a low error rate for the set IoTID20 CF, as seen in Figure 3.

3.4 Find Error Rate

To calculate the error rate for IDS detection using Artificial Neural Network (ANN), Convolutional Neural Network (CNN), and Recurrent Neural Network (RNN) algorithms, we may need the following information:

1. True Positives (TP): Number of actual attacks correctly detected by the algorithm.

2. False Positives (FP): Number of non-attacks incorrectly flagged as attacks.

3. True Negatives (TN): Number of non-attacks correctly identified as such.

4. False Negatives (FN): Number of actual attacks missed by the algorithm.

Error Rate formula: `(FP + FN) / (TP + TN + FP + FN)`

Need to gather the above data from your experiment or simulation to calculate the error rate accurately for each algorithm.

3.5 Comparative Analysis

This section includes a description and examples of the comparative study of the existing algorithms used on the IoTID20 dataset. To predict new assaults, the accuracy of the machine learning system must be increased because attack patterns are evolving [19]. The following illustrates how the comparative study compares the benchmark techniques used for IoTID20 with the suggested model BSP (Binary space partitioning) utilizing metrics for accuracy and error rate.

4. CONCLUSIONS AND FUTURE WORK

A new dataset that may be used to identify and study vulnerabilities in IoT bias was created using Intrusion Discovery Systems (IDS). Chancing flood tide attacks were the main thing of this disquisition. Virtual network analysis needed several twinkles to discover the anomaly, which may affect significant losses, therefore a system with limits was employed rather. The dataset will be enhanced in a posterior analysis to include attack timings, attack types (packet and proliferation), and the elaboration of recorded data attributes. This study also offers network-grounded DDoS discovery using supervised machine literacy. The highlights from the SNMP MIB dataset have been used in several extensively used AI calculations. The results demonstrate that the arbitrary timber (RF) algorithm identifies DDoS attacks with delicacy (99.94%). Also, Multilayer Perceptron's' (MLP) performance is frequently relatively strong and similar to RF. Protocol analysis, network business analysis, intrusion discovery, cyber-attack mitigation, and returning to normal are many of the intrusion discovery styles Snort may be used for. A larger dataset may be created by combining the information for business, attacks, and typical network exertion in the future.

REFERENCES

[1] Latha, S.S. Goud, K.M.S. Reddy, P.M.S.C. Reddy, P.S. and Arunet, P.B. 2023. Cyber-Attacks in IoT-enabled Cyber-Physical Systems. Proceeding of ICDSAC 2023 ITM Web of Conferences, 56, 06003. Coimbatore, Tamil nadu. 23-24 June, France: EDP Science – Web of Conferences

[2] Bertoli, G.d.C.; Alves, P.J.L.; Saotome, and Santos, A.L.D. 2023. Generalizing intrusion detection for heterogeneous networks: A stacked-unsupervised federated learning approach. Computers & Security 127: 103106.

[3] Alsharif, N. A.; Mishra, S.; and Alshehri, M. 2023. IDS in IoT using Machine Learning and Blockchain. Engineering, Technology & Applied Science Research 13(4): 11197–11203.

[4] Butpheng, C.; Yeh, K.H.; and Xiong, H. 2020. Security and privacy in IoT-cloud-based e-health systems—A comprehensive review, Symmetry 12 (7):1191-1223.

[5] Mohamed, K.S. 2019. The Era of Internet of Things Towards a Small World. Switzerland: Springer Cham.

[6] Kobusińska, A.; Leung, C.; Hsu, C.H.; Raghavendra, S.; and Chang, V. 2018. Emerging trends, issues and challenges in Internet of Things, Big data and cloud computing. Future Generation computer systems 87(1): 416-419.

[7] Sharma, G.; and Kalra, S. 2018. Identity based secure authentication scheme based on quantum key distribution for cloud computing. Peer-to-Peer Networking and applications 11(2): 220-234.

[8] Kumar, V.; Pathak, V.; Badal, N.; Pandey, P.S.; Mishra, R.; and Gupta, S.K. 2022. Complex Entropy based Encryption and Decryption Technique for Securing Medical Images. Multimedia Tools and Applications 81: 37441-37459.

[9] Gaud, D.; Jain, A.; and Sharma, A. 2018. Using an IoT Gateway to Connect the Future "Things" For Worldwide Smart City. IJARSE 7(2): 279-287.

[10] Pandey, P.S. Kumar, V. and Wario, R. 2022. Homomorphic Encryption of Neural Networks. Proceeding of 4th International Conference, MIND. Bhopal, India, 19-20 January. Switzerland: Springer Nature.

[11] Vincent, A. Gupta, A. LiRShaw, C. and Akhya1ni, S. 2019. Data acquisition and visual analytic tool-set for paediatric sleep data. Proceedings of the 13th EAI International Conference on Pervasive Computing Technologies for Healthcare - PervasiveHealth'19, Trento, Italy, 20-23 May, Italy: ACM

[12] Chunka, C.; Banerjee, S.; and Gupta, S.K. 2023. A secure

communication using multifactor authentication and key agreement techniques in internet of medical things for COVID-19 patients. Concurrency and Computation: Practice and Experience 35(7): 01-22.

[13] Kumar, V.; Badal, N.; and Mishra, R. 2021. Elderly fall detection using IoT and image processing. Journal of Discrete Mathematical Sciences and Cryptography 24(3): 681-695.

[14] Rashid, A.; Gupta, S.K.; Khanam, Z.; Rashid, M.; Sultan, S. A.; and AlGhamdi, A.S. 2022. A Novel Approach for Securing Data against Adversary Attacks in UAV Embedded HetNet using Identity Based Authentication Scheme. IET Intelligent Transport Systems: 1-19.

[15] Bhagat, V.; Kumar, S.; Gupta, S.K.; and Chaube, M.K. 2022. Lightweight Cryptographic Algorithms Based on Different Model Architectures: A Systematic Review and Futuristic Applications. Concurrency and Computation: Practice and Experience 35(1): 01-27.

[16] Gupta, A.; and Gupta, S.K. 2022. Flying through the Secure Fog: A Complete Study on UAV-Fog in Heterogeneous Networks. International Journal of Communication Systems 35(13): 1-41.

[17] Kumar, S.; Chaube, M.K.; Nenavath, S.N.; Gupta, S.K.; and Tetarave, S.K. 2022. Privacy Preservation and Security Challenges: A New Frontier Multimodal Machine Learning Research. International Journal of Sensor Networks 39(4): 227-245.

[18] Saxena, P.; Pathak, V.; and Kumar, V. 2013. Algorithm for Animal Diet Formulation. Animal Nutrition and Feed Technology 13(1): 139-146.

[19] Kumar, V. Badal, N. and Mishra, R. 2021. Body Sensor Networks Architecture and security issues in Healthcare application. Proceeding of ICCRDA, Roorkee, India, 24 october. IOP Conf. Series: Materials Science and Engineering

[20] Khan, A.; Gupta, S.; and Gupta, S. K.. 2023. UAV-Enabled Disaster Management: Applications, Open Issues, and Challenges. GMSARN International Journal 18: 44-53.

[21] Mondal, S.; Shafi, M.; Gupta, S.; and Gupta, S.K. 2022. Blockchain based Secure Architecture for Electronic Healthcare Record Management. GMSARN International Journal 16 (4): 413-426.

[22] Kumar, S.; Kumar, S.; Chaube, M.K.; Gupta, S.K.; and Saket, R.K. 2023. Role of Mathematical Modelling and Learning Techniques for Privacy Preservation. GMSARN International Journal 17(1): 96-110.