iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44560

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Secure IoT based Emergency Communication System

Dr. Manishankar S[1], Chaya A[2], Likitha H K[3], Sinchana H S[4]
[1, 2, 3, 4]*Dept. of Information Science & Engineering, GSSS Institute OFEngineering & Technology for Women,* Mysuru, India

Abstract: ***The Internet of Things is the most recent & rapidly developing technology of our time. This paper proposed the idea of Hybrid-cellular Wireless sensor network architecture which uses a functioning cellular base station. A routing scheme is also proposed for the emergency scenario that systematically utilizes accessible devices. Wireless devices are taken into account in the proposed emergency communication architecture, which also supports WSN's self-organizing function. Within a few hours, this communication model may be put up in disaster-stricken communities. The proposed methodology can achieve the goal of establishing communication between trapped and rescue volunteers by providing emergency communication infrastructure. A control station serves as an accurate information system for rescue teams' mobility, organization, and coordination. To assure their legality, a secure communication environment with rigorous IP address registration is provided. This approach provides a solution to issues such as calamity recovery networks and trapped victim search and rescue operations***
Keywords: Hybrid-cellular-WSN, emergency communication architecture, disaster-hit area, rescue volunteers, control station, robust IP address registration, legitimacy, disaster recovery.

I. INTRODUCTION

In today's Information and Communications Technology (ICT) world, the Internet of Things is the newest & most rising trend (ICT). IoT applications include crisis response, army surveillance, medical, intelligent agriculture, and robotic systems, to name a few. The specification of IoT is substantially grounded on distributed and centralized communication architecture. Clients in the dispersed infrastructure extract data directly from deployed sensor devices, whereas sensor devices in the deployed area process information gathered via a concerned base station in the centralized infrastructure.

Multiple Wireless Sensor Networks collaborate to provide IoT connections to end-users. As a result, managing the identification of sensor devices in a secure environment is critical for these networks. Device-to-Device (D2D) security is a suitable option in these situations because WSN and IoT infrastructure development is time-consuming in most circumstances in the existing literature. D2D authenticating techniques for IoT are mostly utilized in a centralized manner. Legitimate sensor devices, on the other hand, rely on third parties, such as authentication servers, for their verification and network involvement in a centralized Device to the Device authentication system. Because all participating devices rely on a single point for authentication, this raises the risk of failure. In these networks, decentralized authentication overcomes the problem. Authentication of IoT networks connected as multi-WSNs is a new decentralized solution to solving the challenges associated with centralized authentication.

Because of its constant emergence, the interconnection of multi-WSNs poses several issues in terms of network security, design, longevity, and communication metrics. Data confidentiality and integrity are critical features of IoT networks because they ensure the network's validity. To provide a secure communication infrastructure, The topological structure and routing protocols are the primary focus of D2D authentication of IoT networks connecting multi-WSNs.

Currently available methods rely on centralized communication and peer-to-peer authentication via nodes, servers, or base stations. During this research, this article provides a decentralized solution to tackle the authentication issue in these networks, which is effective in terms of many authentication types.

II. LITERATURE SURVEY

1) Cyber-physical systems connected as part of the Internet of Things (IoT) are subject to a range of security vulnerabilities due to the infrastructure-less deployment of IoT devices. The integrity, authenticity, and privacy of data inside the deployed region are all ensured via device-to-device authentication of those networks. Different techniques for dealing with security challenges with CPS technology are suggested in the literature. They are, however, mostly reliant on centralized procedures or particular system installations with greater compute and transmission costs. To achieve Device - to - device authentication, the proposed strategy leverages the Hash-MAC-DSDV mutual approach, with the MAC addresses of specified devices being registered in the first phase and published in the second. Valid devices can use the suggested approach to unicast one-way hashing identification and change their routing table.

2) Scalability and security issues affect the developing Internet of Things (IoT). IoT devices, on the one side, are "weak" and require external assistance. In terms of scaling a large number of devices, edge computing presents a viable alternative to centralized cloud computing. The main point of this paper is to utilize a permissioned blockchain & an internal currency or coin system to link the edge cloud resource pool with each Internet of Things device account and resource use. Edge Chain employs a credit-based resource management system to limit the amount of resources that IoT devices may obtain from edge devices based on pre-defined criteria including precedence, application kinds, and previous behavior.

3) The current work examines a unique way of authentication in emergency response systems, in which a mobile user's biometric features are used to verify his or her identity. This study provides a design for such a system that authenticates individuals using both physiological and behavioral biometrics. Here, finger photo biometrics recognition is utilized in conjunction with a gesture. The Right Shift technique is used by an algorithm to match the bio-metric qualities of input with reloaded bio-metric features.

4) A method was proposed that combines the advantages of the Clustering methodology and the Compressive Sensing-based scheme. The optimal number of clusters, as well as the optimal Cluster Head (CH) distribution, were provided first. To address the "Hot Spot Problem" and reduce energy consumption caused by the rotation of Cluster Head tasks, the Backup Cluster Head (BCH) was assigned a third responsibility, as well as a method for rotating the roles of the Cluster Head and Backup Cluster Head.

5) Because of resource limits in IoT edge devices, implementing security features requires a substantial amount of computing power as well as a high hardware/software cost. The power-up states of built-in SRAM are used to build device fingerprints in this work, resulting in a low-cost authentication solution for IoT edge devices. Unclonable IDs obtained from on-chip SRAMs can be troublesome, thus the authors devised a unique ID matching method to circumvent this. This reduces the requirement for on-chip SRAM IDs to be more reliable. The protocol is implemented with a common microcontroller.

6) Existing IoT systems are vulnerable to single points of failure and malicious assaults, making it impossible to provide reliable services. Because of blockchain's versatility and security guarantees, the idea of merging blockchain with the Internet of Things (IoT) is gaining traction. This article developed a blockchain architecture with a credit-based consensus mechanism for IoT to address these issues. It also suggested the credit-based solid evidence (PoW) technique for IoT devices, which could improve transaction efficiency while also ensuring system security. In order to protect sensitive data confidentiality, a data authority management approach was developed to limit sensor data access.

7) There are several security techniques available, but the majority of them are computationally and communicationally intensive. It's challenging to install complex calculations on IoT items since they have limited resources and are often powered by batteries. The Datagram Transport Layer Security (DTLS) protocol has been created to operate in combination with the Node-to-node protocol to offer security. However, Datagram Transport Layer Security isn't well suited to multicasting, although it's a rather typical need in IoT setups. Although the DTLS protocol has been modified to work effectively in a multicast setting, it still uses a lot of communication and computes resources. The technique known as Segregated Ciphertext Policy Attribute-Based Encryption was suggested, with a focus on multicast demands and customization.

8) A new solution based on 5G technology and Cyber-Physical Systems are offered for emergency wireless communications in urban contexts (CPS). The design is divided into three levels, each of which defines and connects distinct feedback control rings using the CPS paradigm. The spectrum consumption is monitored at the physical level by CPS control loops, which analyze whether power signals are of acceptable quality. 5G virtualization technologies are used at the network level to handle network configuration and user management in a very dynamic fashion.

9) We show the universality of a cold-blooded cellular mobile ad hoc network (cellular MANET) for extending wireless content by establishing a fully working microblogging system for smartphones and tablets in a disaster area without modifying the current wireless infrastructure. The assumption is that participants connect via a Wi-Fi radio to form a scrambled cellular MANET, which then transfers data over bumps with sufficient cellular forwarding capacity. We proposed a tone-organizing, mobility-earthenware multi-path routing protocol to control data forwarding in the mongrel cellular MANET (MANET). We agree that it works in the constructed microblogging network by employing the Wireless Mesh Protocol (HWMP) as defined by the IEEE802.11 s standard.

10) Wireless sensor networks (WSNs) are a critical technology for the Internet of Things (IoT). IoT enabled wireless sensor networks to have detector nodes and resource-constrained detector nodes utilized for group communication in the form of multicasting for message delivery rather than device-to-device communication. To preserve multicast group communication messages, it is necessary to build an effective key establishment and distribution mechanism that maintains the

communication's integrity while simultaneously ensuring authenticity and secrecy. This article describes two group key creation and distribution techniques for secure multicast group messaging across IoT detector nodes with constrained resources. The NS3 simulations are also used to evaluate the adoption of new protocols based on the three distinct performance factors: cost, charge, and packet loss.

11) Natural disasters strike many parts of the world on a regular basis, and the efficacy of rescue operations is vital to the survival of stranded victims. However, when a crisis strikes a region, the cellphone communication system usually goes down, making coordination among rescue volunteer squads extremely difficult. Many present crisis communication approaches, however, may be unsuccessful. We proposed a hybrid cellular-MANET architecture that uses operating cellular base stations when they are not broken down in this study. For this emergency script, we also propose a routing method that makes the most use of the devices' available communication and energy resources. The proposed emergency communication architecture takes device mobility into account and promotes MANET's self-organizing capability. This communication mechanism may be implemented in calamity hit areas within limited hours.

12) The use of IoT in disaster management is critical and potentially life-saving. The role of IoT in disaster management is discussed in this study. More specifically, it covers IoT-based disaster operations for several types of catastrophes, as well as a comparison of relevant market solutions. It shows how specific IoT applications, such as an early warning system for fire detection and earthquakes, are implemented, as well as certain strategies for discussing the operation, IoT architecture, and focusing the research on various disasters. This study might be a useful resource for stakeholders interested in using IoT technology to safeguard the structure of their smart cities, manage catastrophes, and decrease dangers.

13) This study examines the many authentication systems offered in the literature. It compares and examines the current authentication methods using a multi-criteria categorization, highlighting their benefits and shortcomings. In the form of tables, the most recent major breaches of privacy, counters, and techniques in VSNs and MSNs are described. In addition, there is a summary of suggestions for further study. Readers will have a better grasp of research trends in private information techniques for ad hoc social networks as a result of this survey.

14) We explore IoT data packets in this work, provide a range of IoT data emulsion circumstances, including privacy and sequestration, divide IoT operations into many disciplines, and give a complete assessment of the state-of-the-art of knowledge emulsion in important IoT operation disciplines. We use the demands of IoT data emulsion in particular as a metric to test and compare the performance of data emulsion methods. Based on the extensive examination, we summarize open research questions, highlight interesting future research areas, and identify research challenges.

15) An edge node approach is presented in this study to cope with the difficulties of jamming attacks in WSNs. In the deployed area of WSN, three edge nodes with different transmission frequencies within the same bandwidth are used. The jamming attack channel in the WSN broadcast medium may be detected thanks to the sender signal's varying transmission frequencies and Round-Trip Time (RTT). If one of the transmission channels is jammed by an attacker, the other two edge nodes test media serviceability by sending data from the same deployed WSNs. Furthermore, due to high-frequency interference in nearby channels, the RTT of the surrounding channel is interrupted from its intended length of time, suggesting a network jamming assault.

Table I. Comparision Table

Md Jubayes al Mahnwd & Ujjaval Guin	2020	Low-Cost authentication Edge device	Using a secure hash function, this research focused on a low method for authenticating edge devices in an IoT network.
Borja Bordel Sánchez, Ramón Alcarria	2020	5G technology and Cyber-physical system	5G virtualization technologies are used to handle network configuration and user management in a dynamic manner.
K.Kartheeban , J. Hemalatha	2020	two group key establishment and distribution protocols	This study offers two methods for establishing and distributing groups In the Internet of Things, keys enable secure cluster interactions between resource-constrained sensor networks.
Muhammad Adil, Mohammed Amin Almaiah	2020	edge node scheme	In the deployed region of WSN, three edge nodes with distinct transmission frequencies in the same bandwidth are employed.
Kaljot Sharma, Darpan Anand	2021	An early-warning system for the detection of calamities	This paper discusses the critical importance of IoT in disaster management.
Muhammad Adil, Mian Ahmad Jan	2021	Hash-MAC-DSDV protocol	The validity of participating devices is assured by constantly broadcasting their information about authentication in localized and open chains Furthermore, real devices in the local chain use one-way Hash MAC authentication, which compares Hash MAC to their MAC address database to verify the offered information.
Chenyu Zheng & Lijun Chen	2014	Hybrid cellular mobile & Hoc network	In hybrid cellular-MANET, the HMANET Protocol beats the HWMP Protocol in terms of adaptability to role shift and mobility.
Srividya R & Ramesh B	2015	Physical and behavioral biometric	The proposed person with a similar physical palm/finger size forge pattern.

III. METHODOLOGY

Fig 1 shows the system architecture of the proposed project. System architecture consists of Base Station, cluster head and sensor devices.

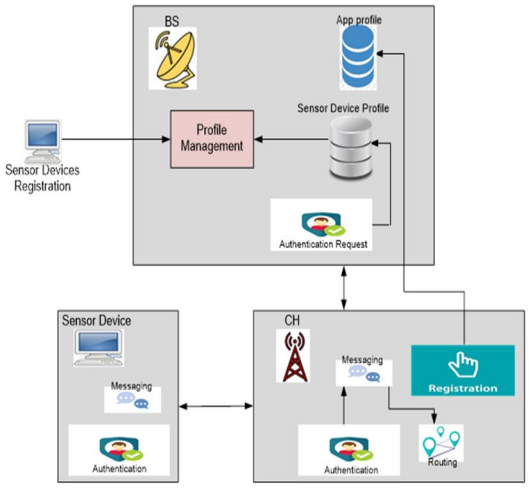


Fig 1 : System Architecture

A. Base Station(BS)

Base Station will add the user profile , registers cluster head and sensor devices. Base station can also view all the registered CH .

B. Cluster Head(CH)

First cluster head should register itself by providing all the details such as user name, password, Base Station IP Address and port number, then registration request will be sent to the Base Station, BS will authenticate and send registration successful to only authorized CH , CH can also view all the registered sensor devices.

C. Sensor Devices

Devices registers itself by providing user name and password , registration request will be sent to the Base Station , BS will authenticate and send registration successful to only authorized users. Device should connect to any of the nearest cluster head to communicate with other devices, all the available CH information will be displayed to the user.

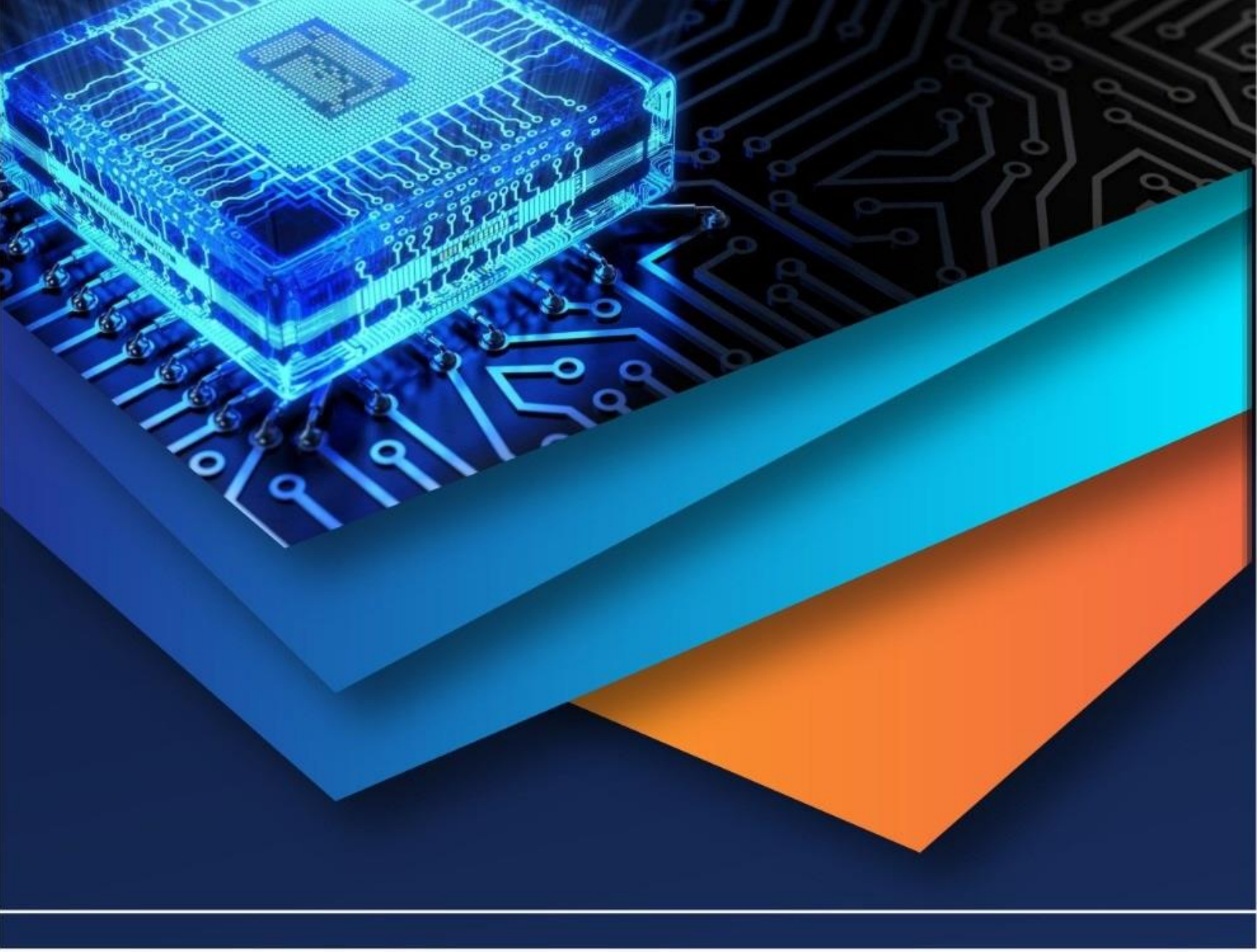
Author	Year	Approach	Description
Himanshu Verma, Naveen Chauhan	2015	Hybrid cellular-MANET architecture	In disaster-stricken areas, a hybrid cellular mobile ad hoc network (hybrid cellular MANET) can provide a solution for emergency communication systems.
Mohammed El-hajj, Maroun Chamoun	2017	IoT authentication protocols using multiple criteria,	This study examines the many authentication systems offered in the literature. It compares and analyses existing authentication systems using a multi-criteria categorization, highlighting their benefits and drawbacks.
Quan Wang & Pengfei Yang	2018	Energy efficiency and life span of WSN	The EECSR algorithm can effectively save energy and extend the network lifetime.
Subho Shankar, Somanath Tripathy	2018	Secure Multicast in an IoT environment and fewer resources	Authors have proposed an S-CPABE technique based on CPABE, aimed specifically toward multicast demands and tailored to the IoT context.
Junqin Huang & Singh Kang	2019	Credit-based proof of work	This paper implements the system on a Raspberry Pi and ran a case study factory, resulting in the conclusion that the PoW technique and data access control are secure and efficient in IoT.
Wenxiu Ding & Xuyang Jing	2019	Data fusion	This paper is based on the need for IoT data fusion as a metric to assess and compare the results of current data fusion methods approaches. Based on the extensive survey, also outlines open research questions, highlights interesting future research areas, and identifies research challenges.
Jianyu Wang & Austin Hester	2019	EdgeChain Prototype Environment Setup, Blockchain Transactions	The authors discussed the EdgeChain framework's architecture and prototype, which is a unique Edge-IoT framework based on blockchain and smart contracts.

IV. CONCLUSION

This study presents a hybrid cellular-WSN-based emergency communication infrastructure for disaster-affected regions that may be utilized by both trapped survivors and rescue personnel in this project. In the event that if all other communication networks are unavailable, this suggested system includes an emergency communication infrastructure. For message delivery in this location, we also developed a mobility-aware, self-organized reactive routing scenario. The proposed solution covers both issues, namely the disaster recovery network and the search-and-rescue- and - rescue operation for people stuck in buildings.

REFERENCES

[1] Muhammad Adil “Hash-MAC-DSDV: Mutual Authentication for Intelligent IoT-Based Cyber-Physical Systems” IEEE JOURNAL OF INTERNET OF THINGS , July 2021..
[2] Jianli Pan & Jianyu Wang ” EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts” IEEE INTERNET OF THINGS JOURNAL, VOL. 6, NO. 3, JUNE 2019..
[3] Srividya.R and Ramesh.B,” Design of Biometric Authentication Technique for MANET Based Emergency Response System” IEEE, 2015.
[4] Quan Wang & Deyu Lin, “An Energy-Efficient Compressive Sensing-Based Clustering Routing Protocol for WSNs“ .IEEE Sensor Journal ,2018.
[5] Md Jubayer al Mahmod and Ujjwal Guin.” A Robust, Low-Cost and Secure Authentication Scheme for IoT Applications” Cryptography 2020,
[6] Junqin Huang,Linghe Kong,” A Robust, Low-Cost and Secure Authentication Scheme for IoT Applications” IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 15, NO. 6, JUNE 2019
[7] Subho Shankar Basu and Somanath Tripathy,” Securing Multicast Group Communication in IoT-Enabled Systems” IETE TECHNICAL REVIEW, 2018.
[8] Borja Bordel Sánchez, Ramón AlcarriaRozi ,” Managing Wireless Communications for Emergency Situations in Urban Environments through Cyber-Physical Systems and 5G Technologies” Electronics 2020,.
[9] Chenyu Zheng & Lijun Chen” Hybrid Cellular-MANETs in Practice: A Microblogging System for Smart Devices in Disaster Areas” IEEE 2014.
[10] K.Kartheeban ”Secure Multicast Group Communications for IoT Applications using WSN” Proceedings of the Third International Conference on Smart Systems and Inventive Technology (ICSSIT 2020) .
[11] Himanshu Verma & Naveen Chauhan” MANET Based Emergency Communication System for Natural Disasters“ International Conference on Computing, Communication and Automation (ICCCA2015).
[12] Kaljot Sharma & Darpan Anand ” A Disaster Management Framework Using Internet of Things-Based Interconnected Devices” Hindawi Mathematical Problems in Engineering, 2021..
[13] Mohammed El-hajj & Maroun Chamoun,” Analysis of Authentication Techniques in Internet of Things (IoT)” IEEE Conference Paper October 2017 .
[14] Wenxiu Ding1 & Xuyang Jing,” A Survey on Data Fusion in Internet of Things: Towards Secure and Privacy-Preserving Fusion” Information Fusion, 2019.
[15] Muhammad Adil, Mohammed Amin Almaiah ,” An Anonymous Channel Categorization Scheme of Edge Nodes to Detect Jamming Attacks in Wireless Sensor Networks” MDPI Journal , Sensors 2020
[16]



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY