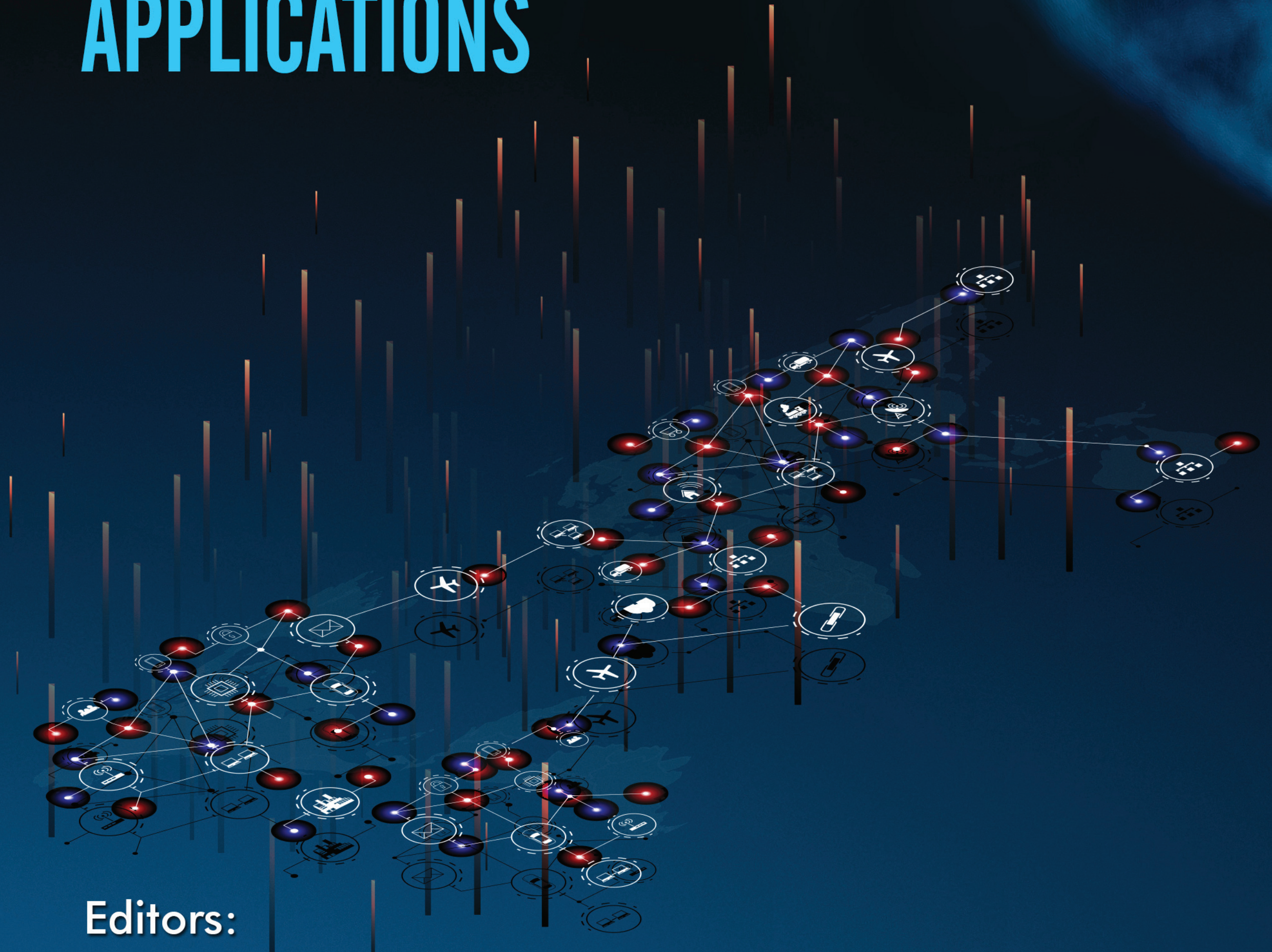
IOT-ENABLED SENSOR NETWORKS: ARCHITECTURE, METHODOLOGIES, SECURITY, AND FUTURISTIC APPLICATIONS



Editors:
Samayveer Singh
Manju
Aruna Malik
Pradeep Kumar Singh

Bentham Books

Advances in Computing Communications and Informatics

(Volume 6)

IoT-enabled Sensor Networks: Architecture, Methodologies, Security, and Futuristic Applications

Edited by

Samayveer Singh

Department of Computer Science and Engineering
Dr. B. R. Ambedkar National Institute of Technology
Jalandhar, Punjab, India

Manju

Department of Computer Science and Information Technology
Jaypee Institute of Information Technology
Noida, Uttar Pradesh, India

Aruna Malik
Department of Computer Science and Engineering
Dr. B. R. Ambedkar National Institute of Technology
Jalandhar, Punjab, India

&

Pradeep Kumar Singh
Jaypee University of Information Technology
Waknaghat, India

Advances in Computing Communications and Informatics

(Volume 6)

IoT-enabled Sensor Networks: Architecture, Methodologies, Security, and Futuristic Applications

Editors: Samayveer Singh, Manju, Aruna Malik and Pradeep Kumar Singh

ISSN (Online): 2737-5730

ISSN (Print): 2737-5722

ISBN (Online): 978-981-5049-48-0

ISBN (Print): 978-981-5049-49-7

ISBN (Paperback): 978-981-5049-50-3

© 2024, Bentham Books imprint.

Published by Bentham Science Publishers Pte. Ltd. Singapore. All Rights Reserved.

First published in 2024.

BENTHAM SCIENCE PUBLISHERS LTD.

End User License Agreement (for non-institutional, personal use)

This is an agreement between you and Bentham Science Publishers Ltd. Please read this License Agreement carefully before using the ebook/echapter/ejournal (**"Work"**). Your use of the Work constitutes your agreement to the terms and conditions set forth in this License Agreement. If you do not agree to these terms and conditions then you should not use the Work.

Bentham Science Publishers agrees to grant you a non-exclusive, non-transferable limited license to use the Work subject to and in accordance with the following terms and conditions. This License Agreement is for non-library, personal use only. For a library / institutional / multi user license in respect of the Work, please contact: permission@benthamscience.net.

Usage Rules:

1. All rights reserved: The Work is the subject of copyright and Bentham Science Publishers either owns the Work (and the copyright in it) or is licensed to distribute the Work. You shall not copy, reproduce, modify, remove, delete, augment, add to, publish, transmit, sell, resell, create derivative works from, or in any way exploit the Work or make the Work available for others to do any of the same, in any form or by any means, in whole or in part, in each case without the prior written permission of Bentham Science Publishers, unless stated otherwise in this License Agreement.
2. You may download a copy of the Work on one occasion to one personal computer (including tablet, laptop, desktop, or other such devices). You may make one back-up copy of the Work to avoid losing it.
3. The unauthorised use or distribution of copyrighted or other proprietary content is illegal and could subject you to liability for substantial money damages. You will be liable for any damage resulting from your misuse of the Work or any violation of this License Agreement, including any infringement by you of copyrights or proprietary rights.

Disclaimer:

Bentham Science Publishers does not guarantee that the information in the Work is error-free, or warrant that it will meet your requirements or that access to the Work will be uninterrupted or error-free. The Work is provided "as is" without warranty of any kind, either express or implied or statutory, including, without limitation, implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the results and performance of the Work is assumed by you. No responsibility is assumed by Bentham Science Publishers, its staff, editors and/or authors for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products instruction, advertisements or ideas contained in the Work.

Limitation of Liability:

In no event will Bentham Science Publishers, its staff, editors and/or authors, be liable for any damages, including, without limitation, special, incidental and/or consequential damages and/or damages for lost data and/or profits arising out of (whether directly or indirectly) the use or inability to use the Work. The entire liability of Bentham Science Publishers shall be limited to the amount actually paid by you for the Work.

General:

1. Any dispute or claim arising out of or in connection with this License Agreement or the Work (including non-contractual disputes or claims) will be governed by and construed in accordance with the laws of Singapore. Each party agrees that the courts of the state of Singapore shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this License Agreement or the Work (including non-contractual disputes or claims).
2. Your rights under this License Agreement will automatically terminate without notice and without the

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Pte. Ltd.
80 Robinson Road #02-00
Singapore 068898
Singapore
Email: subscriptions@benthamscience.net

CONTENTS

PREFACE

The Internet of Things (IoT) significantly broadens the use of information technology by fusing the physical and digital worlds. The third wave of the IT industry revolution is currently being led by futuristic device-based networking. When it comes to smart gadgets and embedded wireless technologies that use sensing devices, recent years have witnessed enormous growth. In the near future, it is expected that billions of devices need to be connected to the Internet directly or indirectly. The term “IoT”, which was first proposed by Kevin Ashton, a British technologist, in 1999, has the potential to impact everything in today's world, right from health care, smart cities, education, and industries.

As equipment becomes more digitalized and interconnected, networks between machines, people, and the Internet are formed. This results in the development of new ecosystems that allow for increased productivity, improved energy efficiency, and increased profitability. Sensors help to recognize the state of things, by which they gain the advantage of anticipating human needs based on the information collected per context. These sophisticated devices can make decisions on their own without human assistance in addition to gathering information from their surroundings.

We can turn on the lights in our homes from a desk in an office miles away. The built-in cameras and sensors embedded in our refrigerator let us easily keep tabs on what is present on the shelves, and when an item is close to expiration. When we get home, the thermostat has already adjusted the temperature so that it’s lukewarm or brisk, depending on our preference. These are merely a few of the millions of Internet of Things (IoT) frameworks in use these days. IoT has redefined the way we interact, communicate, and go about our daily work. From homes to maintenance to cities, the IoT ecosystem of devices is making our world smarter and more efficient. In this guide, we'll discuss everything you need to know about IoT, a world where more and more things are connected.

Chapters 1 and 2 of this book discuss in-depth the challenges, applications, and recent advances in the field of IoT. Chapters 3 to 5 have discussed various approaches to IoT implementation in different niches, along with an analysis of IoT-enabled wireless sensor networks. Chapters 6 and 9 provide information about recent technologies to mitigate security issues in IoT networks.

Samayveer Singh
Department of Computer Science and Engineering
Dr. B. R. Ambedkar National Institute of Technology
Jalandhar, Punjab, India

Manju
Department of Computer Science and Information Technology
Jaypee Institute of Information Technology
Noida, Uttar Pradesh, India

Aruna Malik
Department of Computer Science and Engineering
Dr. B. R. Ambedkar National Institute of Technology
Jalandhar, Punjab, India

&

Pradeep Kumar Singh
Jaypee University of Information Technology
Waknaghat, India

List of Contributors

Aatif Jamshed ABES Engineering College, Ghaziabad, U.P., India

Ajay K. Sharma Department of Computer Science and Engineering, National Institute of Technology Jalandhar, Jalandhar, Punjab, India

Aman Jatain Department of Computer Science and Engineering, Amity University, Haryana, India

Amit Garg IIMT Engineering College, Meerut, Uttar Pradesh, India
Department of Computer Science, Manipal University, Jaipur, India

Anshu Kumar Dwivedi Buddha Institute of Technology, Gorakhpur, U.P., India

Ankur Rastogi Jain University, Bengaluru, Karnataka, India

Ankur Department of Computer Science and Engineering, National Institute of Technology Jalandhar, Jalandhar, Punjab, India

Aruna Malik Department of Computer Science and Engineering, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India

Arvind Dagur Galgotias University, Greater Noida, U.P., India

Ashish Kumar ITS Engineering College, Greater Noida, Uttar Pradesh, India

Deepti Singh Department of Computer Science and Engineering, Netaji Subhas Institute of Technology (NSIT), Delhi, India

Manju Department of Computer Science and Information Technology, Jaypee Institute of Information Technology, Noida, Uttar Pradesh, India

Pawan Singh Mehra Delhi Technological University, New Delhi, India

Priyanshi Pandey Department of Computer Science and Information Technology, Jaypee Institute of Information Technology, Noida, Uttar Pradesh, India

Suman Pandey Department of Computer Science and Engineering, Kamla Nehru Institute of Technology (KNIT), Sultanpur, India

Sarika Chaudhary Manav Rachna International Institute of Research and Studies (MRIIRS), Faridabad, Mohali, India

Samayveer Singh Department of Computer Science and Engineering, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India

Saurabh Singhal Department of Computer Science and Engineering, Apex Institute of Technology, Chandigarh University, Chandigarh, India

Ved Prakash Department of Computer Science and Engineering, Kamla Nehru Institute of Technology (KNIT), Sultanpur, India

Vikas Verma iNurture, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India

CHAPTER 1

Internet-of-Things-Enabled Sensor Networks: Vision Challenges and Smart Applications

Aatif Jamshed[1], **Anshu Kumar Dwivedi**[2], **Pawan Singh Mehra**[3,*] and **Arvind Dagur**[4]

[1] *ABES Engineering College, Ghaziabad, U.P., India*

[2] *Buddha Institute of Technology, Gorakhpur, U.P., India*

[3] *Delhi Technological University, New Delhi, India*

[4] *Galgotias University, Greater Noida, U.P., India*

Abstract: Internet-of-Things is the future of connectivity that has turned the physical world into smart objects. The practical feature of Internet-of-Things is to combine all objects, rendering them dependent on a shared infrastructure, in such a manner that humans can regulate them as well as monitor their status. Internet-of-Things is a physical object network that is embedded with hardware, software, sensors, and networking to allow objects to share data with the connected devices. This chapter details the Internet of Things, vision challenges, and various intelligent applications in sensor-enabled networks. The wide-scale application of the Internet would significantly affect how computers and objects engage in real-life scenarios. This chapter aims to highlight the perspective of some novel technologies and innovative implementations for the protection, welfare, and privacy concerns due to the Internet of Things. Some critical sensor networks, which represent the most used sensor networks in many domains, such as Smart Applications, are included in this introduction section. A literature study on Internet-of-Things has been conducted for different aspects, such as infrastructure, implementation problems, *etc*. The authors offer several other applications that are significant. Future research directions for Internet-of-Things have been outlined in the study to equip novel researchers with the assessment of current status and to build upon them with creative ideas.

Keywords: Actuators, Internet-of-Things, Innovative homes, Sensors, Smart city, WSNs.

1. INTRODUCTION

The Internet of Things (IoT) is a network of physical devices and products used daily and connected to the Internet. It is interlinked with a multitude of devices

[*] **Corresponding author Pawan Singh Mehra:** Delhi Technological University, New Delhi, India; E-mail: pawansinghmehra@gmail.com

Samayveer Singh , Manju, Aruna Malik, and Pradeep Kumar Singh (Eds.)
All rights reserved-© 2024 Bentham Science Publishers

that communicate with one another through the use of sensors, actuators, and processors, among other means. The Internet of Things aims to reach high levels of intelligence with the least amount of human contact possible [1, 2]. Many elements of life are made more pleasant by the Internet of Things (IoT), which adds automation and intelligence to many parts of existence. In this context, things are made self-aware and capable of making intelligent decisions on their own, making them more pleasant. There are a large number of heterogeneous devices in the Internet of Things that are all linked over a network. The Internet of Things (IoT) now covers a wide variety of applications, with services accessible in various industries, including manufacturing, healthcare, transport, farming, and smart home. A smart city encompasses all societal areas that rely on information and communication technology (ICTs) [3]. It also encompasses many applications, making city services and surveillance more aware, interactive, and effective. The backbone of Internet-of-Things [3] is the wireless sensor network (WSN), without which the notion of a smart city cannot be achieved. The devices interacting with the physical environment and imposing changes are known as sensors and actuators. Many devices are networked together *via* sensors in a heterogeneous environment, generating a vast and enormous volume. This data is saved and evaluated to extract knowledge and help decision-making [4]. A smart city comprises a diverse range of gadgets, including a mart and basic essentials. Due to the enormous number of sensors linked to the items, a great sign of data is collected. In the case of an intelligent city, the Internet-of-Things network must be scalable since it may be necessary to add new devices and delete old ones at any time and from any location. Incorporating WSNs is difficult due to the wide range of applications and technological differences across devices [5]. The fundamental a basic problem with the Internet: We must develop cities that are private and secure; which are adaptive, independent, reliable; and which are responsive and dependable. The complex is growing in developing cities due to intelligence in smart infrastructure, and these include issues like a lack of interoperability, context sensitivity, scalability, and managing enormous amounts of informatics pics as well as issues such as security, privacy, and integrity, as well as dynamic adaptation, dependability, and latency. To do this, the city takes care of every facet of society, using a diverse array of applications. As shown smart city's main components are comprised, the city is made up of different sectors of society. A smart city is a city that has several essential and interdependent healthcare, industry, transportation, agriculture, and home automation. The intelligent smart uses many factors like intelligent TechnoMarine governance. It also includes a range of facilities and technologies to make people easier in several applications. Internet-of-Things is transforming the education industry as smart city security requirements [6]. The Internet of Things (IoT) will transform the Internet in such a way that machine-to-machine (M2M) learning will become a reality [7]. As a solid backbone, the Internet infrastructure will exist. The reconfiguration will occur by making physical equipment 'smart,' allowing them to accomplish things on their own, giving rise to the 'Internet of Things.' The Internet of Items (Internet-of-Things) promises to make smart technologies more accessible by linking things at any time and in any location. The Internet of Things (IoT) idea was created in 1998, and Kevin Ashton coined the phrase in 1999 [8, 9]. Internet-of-Things essentially enables the interaction of real-world objects to be autonomous but secure [10]. The Internet of Things (IoT) decreases physical labor by automating routine tasks [11]. The number of items linked to the Internet is continuously increasing. Smartphones have a variety of sensors and actuators that collect data, execute computations on it, and then send the important data acquired through the Internet [11]. The authors will be able to construct many fresh applications that will lead to persuasive benefits by employing such a network with various devices containing the sensors [12]. Internet-of-Things smart things may be uniquely recognized. Radio-Frequency Identification (RFID) tags or barcodes are used on these devices, which are detected by sensor devices [13, 14]. The sensors send the collected data to the processing unit through the Internet for processing. The results of the processing are conveyed to the decision-making and action-invoking system, which then takes the required action.

1.1. Major Issues Resolved by Internet of Things

One of the main ideas behind the Internet of Things is to bring information from different devices together. However, this can only be done perfectly if the right information is given at the right time. This can be done with the help of Augmented Reality, which lets you use a headset or mobile device to see relevant and actionable data over your environment whenever you need to. Microsoft, NASA, Volvo, Autodesk, and Caterpillar are just a few of the big companies that have put a lot of money into AR. Autodesk and NASA have tried out different ways to use Microsoft's Hololens.

To explain this further, the following are the real world problems that IoT could help solve.

- IoT and AI can be used to find out what went wrong with a machine and how to fix it. This can be shown with the help of a centrifugal pump as an example. Real-time sensors will keep an eye on how the machine is working and pick up on any problems. When they do, real-time CFD analysis will be used to find out what went wrong. With AR, a real-time image or CAD diagram can be shown on top of the pump to show exactly what needs to be done to fix it.

CHAPTER 2

A Perspective View of Bio-Inspire Approaches Employing in Wireless Sensor Networks

Ved Prakash[1,*], **Suman Pandey**[1] and **Deepti Singh**[2]

[1] *Department of Computer Science and Engineering, Kamla Nehru Institute of Technology (KNIT), Sultanpur, India*

[2] *Department of Computer Science and Engineering, Netaji Subhas Institute of Technology (NSIT), Delhi, India*

Abstract: In this chapter, we discuss a bio-inspired computational model that utilizes heuristic techniques. This model is robust and possesses optimization capabilities to address obscure and substantiated problems. Swarm intelligence is an integral part of this bio-inspired model, functioning within groups. The nature of these algorithms is non-centralized, drawing inspiration from self-management to solve real-life complex computational problems. Examples include the traveling salesman problem, the shortest path problem, optimal fitness functions, security systems, and the use of optimal computational resources in various areas. The deployment of a Wireless Sensor Network involves a group of sensor nodes, typically implemented at remote locations to observe environmental behaviors. However, these sensor nodes operate on batteries, making replacement or recharge nearly impossible once deployed. Energy is a crucial resource for wireless sensor networks to extend their lifetime. While numerous concepts have been proposed to improve the lifespan of wireless sensor networks, many issues in Wireless Sensor Networks (WSN) are designed as multi-dimensional optimization problems. The bio-inspired model offers a solution to overcome these challenges. Swarm Intelligence proves to be a simple, efficient, and effective computational methodology for addressing various issues in wireless sensor networks, including node localization, clustering, data aggregation, and deployment. The Swarm Intelligence methodology encompasses several algorithms such as Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO), Reactive Search Optimization (RSO), Fish Swarm Algorithm (FSA), Genetic Algorithm (GA), Bacterial Foraging Algorithm (BFA), and Differential Evolution (DE). This chapter introduces Swarm Intelligence-based optimization algorithms and explores the impact of PSO in wireless sensor networks.

Keywords: Ant colony optimization (ACO), Clustering, Fish swarm algorithm (FSA), Particle swarm optimization (PSO), Reactive search optimization (RSO), Swarm intelligence, WSNs.

[*] **Corresponding author Ved Prakash:** Department of Computer Science and Engineering, Kamla Nehru Institute of Technology (KNIT), Sultanpur, India; E-mail: vedprakashknit@gmail.com

Samayveer Singh , Manju, Aruna Malik, and Pradeep Kumar Singh (Eds.)
All rights reserved-© 2024 Bentham Science Publishers

1. INTRODUCTION

A swarm is a huge group of homogeneous birds, ants, and simple electronic devices (agents) that communicate with each other in their locality and environment without central control to enable an interesting global behavior to emerge. The algorithms depend on a family of population-based and nature-inspired algorithms that have the capability of generating low-cost, high-performance, and stable solutions to multiple difficult issues [1]. Therefore, Swarm Intelligence is an era of artificial intelligence. It identifies activities of social groups in nature as to consider ant colonies, bird flocks, and fish swarms. These agents (insects or swarm folks) are relatively gossamer and have limited capacity on their own [2]. To work together to accomplish the tasks necessary for their survival, they communicate with certain behavioral patterns. Social interactions between individuals can be either direct or indirect. Examples of direct interaction are *via* visual or audio touch, such as honey bees' air dance. Indirect communication occurs when one person changes the situation and the other individuals act in response to the new-fangled (new path) situation, such as ants' pheromone trails that they put down on their way to finding food sources [3]. Fig. (**1**) is the flow chart of process of Swarm Intelligence. In the first step, initialize the positions and velocities of each particle using the random positioning method. In the second step, evaluate the fitness of each particle using objective function. In the third step, check the maximum iteration or optimal position. In the fourth step, if the condition is not satisfied, then update the positions and velocities of particles in the swarm as fitness value and reach the second step, else stop the process. After completion of the process, the final output gives the optimal result. Classical techniques of optimization need a gigantic computational attempt, as problem size incremented complexity of the system increases exponentially. In solving these problems, an optimization technique plays a very important role in moderate space and computational resources and yet producing desirable results, particularly for a single node implementation. The bio-inspired optimization method is alternative to computationally proficient systematic methods. This method of indirect contact is called the technique of stigmergy, meaning communication through the environment. Swarm Intelligence is the subject of the research area discussed in this in-depth article. This paper explores swarm intelligence's most popular model inspired by the pheromone actions of ants to solve the problem of the traveling salesman [4].

Wireless Sensor network is one of the most promising technologies in the field of electro-computer [5] with important various applications for monitoring climate and habitat, structural, health-care, and disaster management [6]. By sensing the physical properties of the environment, a wireless sensor network (WSN) can track the targeted area. WSN is a network of lightweight, cheap self-driving nodes capable of capturing, processing, and transmitting sensory data *via* wireless networks. The final target of the data is one or more base stations (no energy constraints). WSN's technical challenge properties include dense non-infrastructure nodes deployment, dynamic topology, bandwidth, spatial distribution, memory, computing and power resource constraints. There are many factors that also affect WSN, such as deployment, location, EAC (energy-awar--clustering), and data aggregation nodes as problems of optimization. Clustering is one of the most important techniques to improve the lifespan of a Wireless Sensor Network. In this technique, cluster head selection is the most important objective. As per researchers, cluster head selection problem falls in the NP-hard problem for the algorithm. Swarm Intelligence models have the capability to solve NP-hard problems [7]. PSO is a popular technique of multi-dimensional optimization [8]. PSO's strengths are effortless implementation, high-class solutions, software performance, and convergence speed. Literature in WSNs is full of PSO requests. The main target of this is to provide an idea of PSO in WSNs.

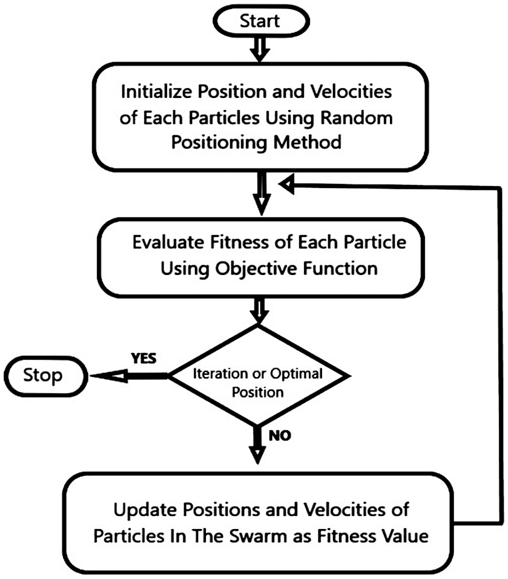

Start
Initialize Position and Velocities of Each Particles Using Random Positioning Method
Evaluate Fitness of Each Particle Using Objective Function
Iteration or Optimal Position
YES
Stop
NO
Update Positions and Velocities of Particles In The Swarm as Fitness Value

Fig. (1). Process flow diagram of swarm intelligence.

The paper is organized as follows: section 2 discusses the literature review of the related papers. Section 3 discusses the taxonomy of swarm intelligence and the paper is concluded in section 4.

CHAPTER 3

Automatic Accident Detection and Alerting System using IoT

Aman Jatain[1,*], **Sarika Chaudhary**[2] and **Manju**[3]

[1] *Department of Computer Science and Engineering, Amity University, Haryana, India*

[2] *Manav Rachna International Institute of Research and Studies (MRIIRS), Faridabad, Mohali, India*

[3] *Department of Computer Science and Information Technology, Jaypee Institute of Information Technology, Noida, Uttar Pradesh, India*

Abstract: This chapter proposes the implementation of an automatic accident detection and alerting system utilizing the Internet of Things (IoT). This system aims to swiftly and efficiently locate accident sites and notify emergency services, there by expediting the transfer of victims to medical centers. Road accidents are one of the leading causes of death annually, primarily due to delays in reporting the incidents. The proposed system operates in two main parts. First, when a vehicle is impacted, sensors installed in the vehicle activate and capture the location *via* the Global System for Mobile Communication (GSM) module. Subsequently, information about the accident site and the victim's condition is sent to a registered phone number through the GSM module. Essentially, when an accident occurs, the installed piezoelectric sensor immediately detects the impact, relaying this information to the microcontroller. The microcontroller then sends an alert message, including location and other pertinent details, to the registered unit to ensure timely medical assistance. This system aims to enhance the efficiency of medical services in reaching accident victims promptly, potentially saving lives that might otherwise be lost due to delayed accident reporting.

Keywords: Automatic accident detection, Alerting system, GSM, General packet radio service (GPRS), Internet of things vehicle, LTE.

1. INTRODUCTION

Road accidents are a leading cause of mortality worldwide, posing a significant global health challenge. The annual death toll from road traffic incidents is alarmingly high, underscoring a crisis in road safety [1]. Each year, road accidents claim the lives of 1.3 million people and injure approximately 50 million more worldwide. On average, this translates to 3,287 lives lost daily.

[*] **Corresponding author Aman Jatain:** Department of Computer Science and Engineering, Amity University, Haryana, India; E-mail: amanjatainsingh@gmail.com

Samayveer Singh , Manju, Aruna Malik, and Pradeep Kumar Singh (Eds.)

All rights reserved-© 2024 Bentham Science Publishers

Notably, road traffic deaths disproportionately affect young adults, accounting for more than 50% of fatalities. In particular, around 40,000 individuals aged 25 and below lose their lives in road accidents annually [2]. This dire situation is not confined to specific countries; even nations with robust road safety measures experience a significant number of fatalities each year due to road traffic incidents. In India, the statistics are particularly alarming. In year 2013 there were 1.3 lakh casualties from road accidents, a figure surpassing the total number of casualties from all wars combined [3]. Furthermore, in 2017, road accidents resulted in 1.46 lakh fatalities, a number equivalent to the entire population of Shillong, the capital of Meghalaya. Annually, road accidents claim over a lakh lives in India, and the ratio of injuries to fatalities is approximately three to four times higher [4].

There could be many possible reasons for deaths in road accidents, but these should be examined because the world we live in is based on technology, and we cannot ever deny the fact that everyone in this era is a slave to technology. Technology has made our lives easier in many ways. However, with the advancement in technology, everyone is looking for an easy life, and this desire for technology affects every individual. For example, the excessive use of automobiles has increased the occurrence of traffic hazards and road accidents. The very reason for a person’s demise in a road accident is often the delay in the process of conveying this information to medical centers [3]. Something extremely essential for the victims of vehicle accidents is emergency response time; when it comes to life, every minute counts. This applies to both the present and the future. Despite so much advancement in technology, there is still a lack of providing emergency services on time. From an analytical viewpoint, a just one-minute reduction in response time can increase a person's odds of survival by 6%. If an accident occurs, someone will have to inform the police or hospital personnel about the accident; then help will arrive, and it is also unknown how much time this process will take. Due to poor traffic management and delays in the transfer of accident information, it is impossible to be on time. However, with so much advancement in technology, a system can be designed to help manage traffic and accidents occurring on roads.

Vehicles equipped with advanced safety measures for accident avoidance represent an emerging concept that can be realized through technologies such as IoT, machine learning, and several others. These technologies can be utilized to construct a system that significantly contributes to mitigating road hazards. It is crucial to implement such advanced technologies in traffic and vehicles to reduce response times. In literature, extensive research has been conducted on accident rescue, predominantly focusing on the use of Information and Communication Technology (ICT) for efficient and rapid rescue operations. However, the majority of these works propose sophisticated solutions aimed at decreasing response times. While these solutions are comprehensive, they tend to be expensive and are not universally accessible to all vehicle types. Bearing this in mind, this research aims to introduce the design and implementation of an automatic accident detection system capable of autonomously capturing accident information and location, subsequently transmitting it to a corresponding unit. This functionality is instrumental in reducing the time required to communicate the occurrence of an accident, ultimately expediting the arrival of medical assistance to the accident site [5]. The system proposed herein autonomously detects accidents and proficiently locates the geographical position of the accident site. An Arduino microcontroller, selected for its cost-effectiveness and efficiency, powers the system. Programming is conducted using the Arduino IDE, and various modules are employed for tracking and detection purposes. The system is designed to rapidly detect accidents and promptly convey essential information to the relevant unit, including the accident site's latitude and longitude. Messages are transmitted swiftly, aiding in the preservation of precious lives. A button is incorporated to cease message transmission in rare instances where there are no casualties, ensuring the rescue team’s time is not wasted. Upon the occurrence of an accident, the system automatically activates and dispatches an alert message. This message is transmitted *via* GSM/LTE, a mobile communication technology that facilitates the exchange of mobile voice and data services. For communication between the mobile station and the Base Transceiver Station, the system operates within the 890MHz to 915MHz range for one direction, and 935MHz to 960MHz for the other [6]. The GPS module ascertains the accident location’s coordinates, while various other sensors are integrated into the proposed system.

As this system is automatic, capable of detecting accidents, and even able to ascertain the critical state of a patient, consider the potential impact if it were installed in every vehicle. This capability would streamline the process of understanding the actual critical state of a victim involved in an accident, enabling medical centers to dispatch help that is appropriately tailored to the situation. This feature enhances the value and utility of the design considerably. To further support rescue teams and minimize their efforts in cases of minor accidents, several additional features have been integrated. An emergency button is included, allowing individuals involved in an accident to communicate that the situation is not dire, obviating the need for extensive rescue efforts. Additionally, a heat sensor is incorporated to detect the onset of a fire, providing an early warning and potentially averting a more serious disaster. Overall, this system offers a comprehensive solution to the inadequate emergency facilities often available for road accidents, addressing the issue in the most effective manner possible.

CHAPTER 4

Optimal Election Unequal Clustering Routing Protocol with Improved Tradeoff Function for Wireless Sensor Networks

Ankur[1,*] and **Ajay K. Sharma**[1]

[1] *Department of Computer Science and Engineering, National Institute of Technology Jalandhar, Jalandhar, Punjab, India*

Abstract: In today's technological landscape, IoT-enabled Wireless Sensor Networks (WSNs) offer significant advantages over traditional networks, particularly when it is used under critical applications. However, network devices are typically limited in terms of their energy source; energy optimization has become a major concern in recent years. As a result, energy-efficient protocols are increasingly being prioritized to extend the network's functionality for a long period. In this chapter, we introduce a clustering routing protocol that operates on an unequal clustering basis. The protocol selects the best route for transmitting data to the sink based on various factors, such as the average residual energy of path sensor nodes, the average distance between nodes, the maximal distance nodes in the current path, and the number of hops. Our simulation results show that the proposed Optimal Energy Unequal Clustering Routing (OEUCR) protocol provides a significant improvement over the existing Energy Efficient Routing Protocol (EERP). Furthermore, we propose an optimal election clustering protocol that provides a new trade-off function based on near density factor and elect metric. Our simulation outcomes demonstrate that this protocol increases the network's functional duration by 6 rounds, reduces energy consumption by 0.727 J per round, and allows the base station to receive 975 more messages. Specifically, the packets received by the base station (BS) increased by 23%, while energy consumption decreased by 21% when using OEUCR instead of EERP.

Keywords: Base station, Cluster, Elect metric, LEACH, Near density factor, TEEN, Wireless sensor networks.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are used in many applications that require continuous monitoring of a specific region for as long as possible. Since deployed networks have sensors with limited and non-rechargeable energy resources, effec-

[*] **Corresponding author Ankur:** Department of Computer Science and Engineering, National Institute of Technology Jalandhar, Jalandhar, Punjab, India; E-mail: ankurbohora@gmail.com

Samayveer Singh , Manju, Aruna Malik, and Pradeep Kumar Singh (Eds.)

All rights reserved-© 2024 Bentham Science Publishers

tive and optimized usage of allotted energy is critical. In IoT-enabled WSNs, multiple types of devices receive information and send it to the respective head of the cluster, which sends the data further to the sink with the help of cluster nodes.

To prolong the network's functional duration, clustering is an effective approach that addresses the scalability and lifetime of WSNs. Sensors are divided into various types of clusters based on certain parameters, and only a single node is elected as the cluster head (CH) of the cluster, while the rest of the nodes in the proximity of the cluster heads are called cluster members (CMs). The CM node gathers data from its proximity and directs it to the CH, which aggregates the collected data and forwards it to the base station or sink node [1].

The main aspect of clustering is to extend the total functional duration of the deployed network. Most clustering protocols consider the remaining battery during the process of CHs' selection. However, the authors propose a novel and optimally distributed clustering scheme called the Optimal Election Clustering Protocol (OECP), which introduces a new elect metric during the CH selection phase.

Additionally, the authors introduce the Optimal Election Unequal Clustering Routing Protocol (OEUCRP), which is designed for serial data aggregation applications. It arranges the sensor network by multi-hop routing and unequal clustering.

The manuscript is structured as follows: Section 2 discusses existing research works, while section 3 describes the applied system model. Section 4 provides a detailed description of the proposed clustering protocol, OECP. Section 5 presents the experimental outcomes for OECP when compared with other existing works. Finally, section 6 concludes the manuscript and provides future directions.

2. RELATED WORKS

The authors [2] introduced the LEACH protocol, the first cluster-based routing protocol that allows a fraction p of sensor nodes to serve as CHs, with this role changing over rounds based on the pre-defined area covered by the network. The work discussed an energy efficient hierarchical clustering algorithm for wireless sensor networks that extends the network lifetime [3]. Work [4] proposed the HEED protocol, which identifies CHs with higher remaining energy and lower intra-cluster communication cost. The work discussed an adaptive llc-based and hierarchical power-aware routing algorithm that improves the network lifetime [5]. Authors [6] presented a cluster election and routing protocol based on voting that considers prime factors.

The manuscript [7] proposed EECS, a novel protocol for cluster-based routing that selects CHs based on residual energy and other parameters. Authors [8] introduced the EAP protocol, which selects CHs based on the ratio of residual energy to the average residual energy of all neighbors. In thses studies [9, 10], cost metrics, as well as energy efficiency, are considered. The research work [11, 12] presented a protocol for heterogeneous networks based on a weighted probability approach and a threshold function. The method [13] uses a genetic algorithm-based clustering approach for CH election, mainly designed for movable sinks, and a study [14] proposes a protocol for disaster management systems that use adjustable sensing range and deployment strategies for placing higher energy nodes near the sink to address hotspot problems.

The approach [15] uses a metaheuristic for finding cluster heads efficiently with the help of multiple mobile sinks. Singh *et al*. [16] proposed a nature-inspired clustering algorithm that uses a data aggregation method to reduce energy consumption. The OSEP protocol [17] is an extended version of SEP that incorporates 3-level heterogeneity and modifies energy and threshold formulas. DACHE [18] is an optimized cluster head election routing protocol that extends DEEC by incorporating 3-level heterogeneity and modifying the energy and threshold formula. The sustainable methodology for clustering [19] is an extension of the SEP protocol with a new threshold formula with multiple parameters. The approach [20] maintains sustainability while clustering for data aggregation. Finally, Singh *et al*. discussed hetDEEC, a heterogeneous DEEC protocol that prolongs lifetime in wireless sensor networks by incorporating 3-level heterogeneity and modifying energy and threshold formulas [21, 22]. However, this method also does not provide the lifetime latest defined level.

3. SYSTEM MODEL

A. Network Model:

In this chapter, we consider a sensor network deployed in a square field denoted as A, which possesses the following characteristics:

- The network is assumed to be static and densely deployed, with nodes randomly scattered throughout the field.
- A single sink node, referred to as the base station, is present, and it is located outside of field A.
- Each node is capable of sending data to the base station.
- Nodes are able to compute distances using the received signal strength.
- All nodes are homogeneous and have a fixed communication radius, rc, of 25 meters, similar to Berkeley Motes [12].

CHAPTER 5

Analysis and Performance Evaluation of Routing Protocols using Sink Mobility in IoT-enabled Wireless Sensor Networks

Samayveer Singh[1,*] and **Aruna Malik**[1]

[1] *Department of Computer Science and Engineering, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India*

Abstract: The effect of sink mobility on the improved dual-hop routing protocol (IDHR) and multiple data sink-based energy-efficient cluster-based routing protocol (MEEC) is taken into consideration. Sink mobility can be introduced into the network to prevent the creation of hotspots. The data sinks receive data from cluster heads which further collect data from the member nodes of the respective clusters. The cluster head (CH) performs data aggregation and sends the orchestrated data to the sink. The CH selection in IDHR and MEEC is done by taking into account the node density parameter along with other parameters, such as energy and distance between the node and the sink. In MEEC, multiple data sinks are used to resolve the burden on the relaying nodes involved in data transmission as well as to curb the hotspot problem. The movement of sinks is controlled and managed through the proposed approach, *i.e.*, Sink Mobility based on CH Energy (SMCHE). The node density factor proves to be good for the energy preservation of nodes as it takes into account the average communication distance between the nodes and respective CH. The simulation results show that the network lifetime of the proposed approach is increased by 268%, 191%, 27%, and 17% when compared to MEEC, IDHR, DRESEP and TSEP, respectively.

Keywords: Routing protocols, Cluster heads, Energy efficiency, Network lifetime, Mobile sinks.

1. INTRODUCTION

The wireless sensor nodes are tiny, battery-operated devices since it is not feasible to maintain the main power supply to their deployment site. So, power to these wireless sensor nodes is generally provided through primary batteries.

[*] **Corresponding author Samayveer Singh:** Department of Computer Science and Engineering, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India; E-mail: samayveersingh@gmail.com

Samayveer Singh , Manju, Aruna Malik, and Pradeep Kumar Singh (Eds.)

All rights reserved-© 2024 Bentham Science Publishers

These sensor nodes have processing and communicating functionalities that enhance their network-creating function in any attended or unattended (hostile/ remote) areas. A sensor node consists of three main components:

- The sensing section comprises the sensor itself, which is based on a particular technology. The variety of technologies means you can select a sensor technology that is most suited to the application required.
- The processing circuitry converts the physical variable into an electrical variable to process.
- The signal output contains the electronics connected to a control system.

The sensor nodes have only a limited energy resource (batteries), therefore, this energy should be dissipated only precisely to acquire a higher network lifetime. The battery consumption of a sensor node is directly dependent on how the nodes communicate with each other or with the sink and is utilized accordingly. The sensor nodes form a wireless network to collect data from their surroundings and then coordinate themselves according to the type of application that is needed to be performed. Later, these nodes send the aggregated data to the data sink or the base station, which helps in achieving the respective task [1]. The network formed as a result of the above is termed a wireless sensor network (WSN).

It is impossible to change or recharge the sensor nodes' batteries when they are used in unsupervised or remote locations. Therefore, it is assumed that when the battery of a node is exhausted, it is assumed to be dead, and if it happens to all other nodes, then the whole network becomes inactive and is considered to be dead. Therefore, the main concern is to enhance the network lifetime and the stability period (number of rounds covered until the first node is dead) of the network. The applications where wireless sensor network has an important role to play are only limited in the human imagination. It helps in monitoring the surroundings and therefore finds applications in remote healthcare, disaster management, environment, and industrial monitoring, reconnaissance and targeting system, battlefield surveillance, air pollution, and agricultural monitoring [2].

Problems in WSNs: The topology of the network decides the placement of the sink inside/outside the network. In some remote applications, where the area under consideration is quite large, the sink is needed to be placed outside that area and eventually, communication takes place through multi-hoping. A moment comes during transmission when the relaying nodes are completely exhausted and out of energy. As a result, the data transmission to the sink breaks, and a hot spot is created. This condition is termed as a hot-spot problem [3, 4]. This is due to the excessive relaying load on the nodes closer to the sink. When the single sink is operating, the nodes perform multi-hop communication and face the following problems:

- Procrastination in data delivery is the result of the congestion formed around the single sink.
- Scalability gets affected due to the large size of the network, which physically ends up increasing the communicating distance between nodes and the sink.
- The single sink of the network is prone to the ‘No Communication’ condition whenever sink failure occurs due to any particular reason, which makes the network dependent on a single sink.
- Frequent selection or frequent rotation of relay nodes gives rise to the number of overheads leading to network degradation.

It is worth noting that when only single-hop communication from CH to sink is implemented, there is no hot-spot problem. To implement single-hop communication in large area networks, the only possible and appropriate solution that also considers balancing energy is employing multiple data sinks. It is concluded from the above study of the heterogeneous protocols that they have employed a single sink in their approach toward acquiring network longevity. In some applications, where the network area is hostile and placement of sinks is supposed to be done outside the network, the scenario of multiple data sinks becomes significant. Some of the terminologies are given as follows:

- **Sink:** The data sink is a term used to describe a computer or any other medium capable of receiving data.
- **Cluster head:** A node in a cluster that is responsible for collecting data from sensors in its cluster and relaying these data to the sink.
- **Node density:** Node density describes the portion of the potential connections in a certain proximity.
- **Heterogeneous wireless sensor network:** A network of the wireless sensor having nodes of different energy capacity
- **Multi-hop routing:** Multi-hop routing is a type of communication in radio networks in which the network coverage area is larger than the radio range of single nodes. Therefore, to reach some destination, a node can use other nodes as relays.

The rest of the chapter is organized as follows: Section 2 discusses the related work similar to the routing protocols in IoT enabled wireless sensor networks. The system model is discussed in Section 3 and the proposed work is discussed in Section 4. The performance analysis is given in Section 5 and the paper is concluded in Section 6.

CHAPTER 6

IoT Based Home Security System

Manju[1,*] and **Priyanshi Pandey**[1]

[1] *Department of Computer Science and Information Technology, Jaypee Institute of Information Technology, Noida, Uttar Pradesh, India*

Abstract: Internet of Things (IoT)-enabled intelligent systems are proliferating rapidly, providing the capability to connect virtually any device to the Internet. Consequently, this concept can be effectively utilized in home security applications. In this paper, we have introduced an IoT-enabled system designed to send security alerts to users *via* email upon detecting human intrusion. The system comprises a PIR sensor, Pi camera, Raspberry Pi-3, and an Internet connection. There are two operational modes in the proposed security system. In the first mode, movement by an intruder is detected, and simultaneously, every time someone rings the doorbell, the Pi camera captures an image. The system then accesses a stored database to ascertain whether the individual is recognized. If the person is unfamiliar, the user receives an email notification, including the captured image of the individual. On the other hand, if the person is recognized, the system stores the captured image. In the second mode, when someone exhibits suspicious behaviour in front of the door, the system sends an alert email to the user, prompting them to activate the security alert system installed at the entrance. For face detection, we employ the Haar cascade technique. Face recognition involves two steps: feature extraction and classification. In the feature extraction phase, we compare various algorithms, and a comparative study of these provides a methodology that achieves 99.56% accuracy, outperforming other existing models. The developed system leverages the IoT platform to fortify security against intruders, thereby fostering a safe and secure environment.

Keywords: Face recognition, Home security system, Internet of things.

1. INTRODUCTION

In today's rapidly progressing world, automatic devices are increasingly replacing their manual counterparts, paving the way towards optimal and more convenient solutions. The Internet, serving as the foundation for communication, is being integrated into various devices to establish enhanced communication channels. Over the last few decades, internet usage has soared, and the field of the Internet

[*] **Corresponding author Manju:** Department of Computer Science and Information Technology, Jaypee Institute of Information Technology, Noida, Uttar Pradesh, India; E-mail: manju.nunia@gmail.com

Samayveer Singh , Manju, Aruna Malik, and Pradeep Kumar Singh (Eds.)

All rights reserved-© 2024 Bentham Science Publishers

of Things (IoT) has emerged, allowing for the sharing of various kinds of information whenever needed [1, 2].

From small gadgets to entire industries, information is now at our fingertips. Every device in your home can be controlled remotely from anywhere in the world using an automated home system, providing security against theft or hazards, and creating a sense of safety and peace of mind. In this 21st-century landscape, automating home devices is becoming a norm, simplifying daily tasks and transforming living spaces. However, for home automation to reach its full potential, technological advancements are necessary, allowing for seamless communication between devices, whether wired or wireless. IoT stands out as a transformative tool in this domain, providing a pathway to a more convenient and efficient life. This paper focuses on implementing a cost-effective and easily installable IoT-based home security system, featuring a range of controls and energy-saving capabilities. Users can access and control their homes from any part of the world, enhancing their sense of security. The system allows users to log into their accounts from anywhere, monitoring entries into their homes through an application connected to the internet. The user-friendly interface of the proposed system ensures accessibility for anyone with an internet connection. Additionally, the system's affordability sets it apart from similar products in the market. Our system ensures rapid response to any kind of intrusion, allowing users to access and monitor their desired location using just an internet connection and a device. It employs two main approaches: face detection and face recognition [3, 4]. These tasks, however, are challenging due to the variety of factors that must be considered. To address this, we explore various algorithms, identifying the three most promising approaches: pre-trained convolutional neural networks (ResNet-50 and VGG-16), and the Local Binary Pattern Histogram (LBPH) algorithm. Haar cascade is used for its efficiency in face detection, and the Support Vector Machine (SVM) algorithm for classification. Despite its advantages, the system is not without limitations. Giving access to unauthorized individuals through the system is akin to handing over your house keys, a risk present in traditional systems as well. Nevertheless, when compared to other security systems, such as fingerprint or house ID-based systems, our solution offers a more optimal approach. Various algorithms were compared based on speed, accuracy, and space requirements to identify the best possible solution. The proposed system includes a webcam for facial image recognition, and cross-referencing with stored images in a database. If face recognition is successful, the door unlocks, the user receives an email with an image of the visitor, and the information is saved in the database. In the case of an intruder, the door remains locked, and the homeowner is immediately notified *via* email. The Raspberry Pi 4 serves as the main controller of the system, with the Face Recognition (FR) system validating identities against a database and employing the OpenCV library for image processing. The system's camera module, together with the haar cascade classifier for face detection and SVM algorithm for face recognition, ensures accurate and reliable security measures [5].

2. RELATED WORK

Face detection and face recognition are crucial parameters for home security systems, requiring 24-hour surveillance, cost-effectiveness, and the highest possible accuracy. In this section, we have discussed various models based on these parameters and conducted a comparative study to analyze their challenges, with the aim of developing a model that maximizes accuracy while maintaining cost-effectiveness and low time and space complexity.

One of the studies [6] presents a comparative study of two different face recognition models, utilized to build a home security system capable of detecting the presence of an intruder and alerting the user. The Viola-Jones method has been employed for face detection, while Independent Component Analysis (ICA) and Principal Component Analysis (PCA) have been considered for face recognition. Photos of intruders are taken as soon as they enter, and these are subsequently sent to the system for comparison with a database of authorized individuals. The two models, ICA and PCA, yield accuracy rates of 86.7% and 76.7%, respectively, leading to the conclusion that the ICA algorithm surpasses the PCA algorithm in terms of accuracy.

The CNN [7] method, known for its high accuracy in face recognition, has been implemented in a home security system. A database consisting of a number of 1048 images of user faces has been used to train the model, employing the AlexNet convolutional neural network, which comprises eight layers. The results indicate an accuracy rate of 97.5%.

Home security is a paramount concern, and the system proposed in [8] addresses this issue through the use of IoT, training a model to perform face detection and recognition. The system compares images from an existing database with captured images to determine whether an individual is authorized to enter. This automated system is cost-effective, consumes low power, and its efficiency is enhanced by IoT, making it suitable for real-time applications. It achieves an approximate accuracy of 95% and enables remote monitoring of the house over a Wide Area Network (WAN).

The trend of smart homes is escalating daily, with increasing numbers of people opting for automated security systems for convenience and safety. According to a 2022 survey report [9], over 500 smart devices are in use by families, offering convenience and ease of use. Smart devices, supported by continuous

CHAPTER 7

Cyber Security from a Business Perspective

Vikas Verma[1], **Amit Garg**[2] and **Saurabh Singhal**[3,*]

[1] *iNurture, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India*

[2] *Department of Computer Science, Manipal University, Jaipur, India*

[3] *Department of Computer Science and Engineering, Apex Institute of Technology, Chandigarh University, Chandigarh, India*

Abstract: In today's era of Information Technology, we have encountered drastic changes in computing methodologies due to a tremendous increase in ONLINE communication traffic both in terms of the number of users and data communication. The COVID–19 pandemic has brought the entire world online. Cyber Security plays an important role in the field of information technology. In order to secure information, one can face many challenges. Nowadays, governments and other organisations are following various measures to prevent vivid cybercrimes. In this chapter, we have raised concern over the drastic increment in an ONLINE communication system, which urges the need for the development and deployment of Cyber Security in a business environment.

Keywords: Business resilience, Cloud computing, Data breach, Internet of things.

1. INTRODUCTION

The transition of the entire education system to an online format has rendered the situation increasingly catastrophic. Taking into account the current trends in online communication, we have been analyzing and progressing at a defined pace. However, the current situation presents a significant challenge that we are struggling to cope with. This sudden shift in the behavior of data transmission has catapulted us approximately 10 years forward, forcing us to adapt to a communication system that is not deemed suitable for meeting these abrupt demands [1]. The one-minute intervals over the last three years on the Internet illustrate the surge in online communication.

The graph depicted in Fig. (**1**) highlights the growth in the number of Google users accessing the Internet per minute. In 2017, the count stood at 3.5 million users; it increased to 3.7 million in 2018, 3.8 million in 2019, and reached 4.7 mil-

[*] **Corresponding author Saurabh Singhal:** Department of Computer Science and Engineering, Apex Institute of Technology, Chandigarh University, Chandigarh, India; E-mail: saurabh.singhal09@gmail.com

Samayveer Singh , Manju, Aruna Malik, and Pradeep Kumar Singh (Eds.)
All rights reserved-© 2024 Bentham Science Publishers

lion by 2020. Examining the rate of increase showcased in Fig. (**2**), the year 2019-2020 witnessed an almost fivefold surge compared to earlier periods. Observing these trends, our IT sector has progressively shifted towards embracing the latest in computing innovations, undergoing significant transformations from Cloud Computing to IoT, then to Cloud IoT, and eventually to Fog Computing.

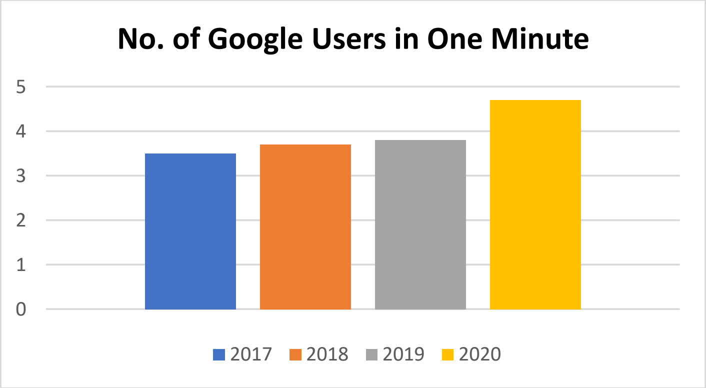


Fig. (1). Number of Google users in one minute over the years.

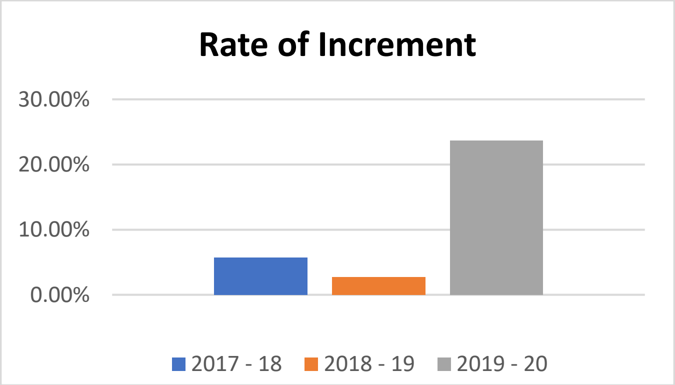


Fig. (2). Rate of increase in the number of Google users.

Before moving further, let us discuss these terms:

- **Cloud Computing** – Cloud computing is defined as the online delivery of various software and hardware services *via* the Internet. These resources encompass high-computing servers, data storage, networking, databases, and software [2]. Rather than storing data on a personal hard drive or local storage device, cloud-based storage enables saving it to a remote database. As a result, data can be accessed from anywhere, provided there is an electronic device with

Internet connectivity. Nowadays, users manage vast amounts of data due to the proliferation of numerous IoT devices. Consequently, cloud computing has become a preferred option for individuals and businesses alike, offering benefits such as cost savings, increased productivity, speed, efficiency, performance, and security [3].

- **IoT** – The Internet of Things (IoT) refers to a network of interconnected computing devices, mechanical and digital machines, objects, animals, or people, each provided with unique identifiers (UIDs). These entities have the capability to transfer data over a network without the necessity for human-t--human or human-to-computer interaction [4]. In the realm of IoT, a "thing" could be a person with a heart monitor implant, a farm animal equipped with a biochip transponder, an automobile outfitted with sensors to alert the driver of low tire pressure or any other natural or man-made object that can be assigned an Internet Protocol (IP) address and capable of transmitting data over a network [9, 10].
- **CloudIoT** – An IoT cloud constitutes an extensive network that supports IoT devices and applications, incorporating the requisite infrastructure, servers, and storage necessary for real-time operations and processing. Examples include Amazon Web Services IoT, IBM Watson IoT Platform, and Microsoft Azure IoT Hub.

These transitions have led us to encounter unexpected and challenging situations regarding implementation, due to the unique characteristics and behaviors specific to each methodology. Nevertheless, we have managed to cope with these circumstantial challenges using our knowledge and intelligence, striving to implement advancements in computing methodologies to prevent such issues from arising in the future. According to INFOGIX trends around 2017, there has been an amalgamation of Big Data, IoT, and Cloud Computing. Implementing any one of these technologies is not possible without interacting with the domains of the others. They are closely and strongly interconnected, along with their sub-dimensions. However, when implementing any computing methodology, another major concern and aspect that we must consider is the Security Aspect.

The Security Aspect encompasses mechanisms related to all dimensions of the IT sector, including physical, hardware, software, firmware, network, application, and any other dimensions that one might consider. Expert professionals have consolidated these dimensions under the term "CYBER SECURITY". The term "CYBER" covers all aspects related to computing, computing devices, and Internet communication. In brief, we can assert that cyber security can be implemented in any scenario if we successfully apply the principles of the CIA Triad – Confidentiality, Integrity, and Availability. We must also be mindful of implementing the Principles of Information Assurance, which provide assurance

CHAPTER 8

Security and Privacy of Application of Smart Cities

Amit Garg[1,*], **Ashish Kumar**[2] and **Ankur Rastogi**[3]

[1] *IIMT Engineering College, Meerut, Uttar Pradesh, India*

[2] *ITS Engineering College, Greater Noida, Uttar Pradesh, India*

[3] *Jain University, Bengaluru, Karnataka, India*

Abstract: In this chapter, we have discussed smart cities, their applications, and the associated security and privacy issues. We will begin with a brief introduction to smart cities, followed by a focus on the major and essential applications required to transform a city into a smart city. We will cover topics such as smart education, healthcare, governance, transportation, and services. Each of these applications plays a crucial and efficient role in realizing the objectives of a smart city. Furthermore, it is imperative to address the security and privacy concerns related to these applications, particularly concerning data access and protection, and to identify the necessary security requirements for these applications.

Keywords: Smart city, Security, Smart city applications.

1. INTRODUCTION

The size and population of urban areas are steadily increasing, as indicated by global estimate reports. Consequently, the day-to-day challenges in metropolitan areas are intensifying due to limited resources and services such as healthcare, education, environment, and transportation. To maintain the sustainability of these services in urban areas, innovative strategies for effective data management must be prioritized. The term 'smart city' derives from the integration of mobile computing systems through practical data management networks across all components and layers of the city itself. Cities are increasingly focusing their efforts on becoming smarter through the use of data management networks, such as the Internet of Things (IoT), big data, and cloud computing technologies [1]. These comprehensive systems enhance various aspects of operations and services, including traffic management, sustainable resource management, quality of life, and infrastructure in the smart city.

[*] **Corresponding author Amit Garg:** IIMT Engineering College, Meerut, Uttar Pradesh, India; E-mail: foramitgarg@gmail.com

Samayveer Singh , Manju, Aruna Malik, and Pradeep Kumar Singh (Eds.)
All rights reserved-© 2024 Bentham Science Publishers

The rapid advancement of IoT technologies motivates researchers and scientists to create new application areas and services, and these novel smart services must adequately address the needs of citizens worldwide. Furthermore, to promote awareness of smart city concepts globally, human needs must be considered through the exchange and collection of data within IoT services. Therefore, the network should be embedded with sensing, computing, networking, and actuation capabilities. Another major goal is to monitor, collect, archive, and share public sensor data from IoT devices to facilitate the development and analysis of smart cities.

In the current literature, a vast array of studies addresses various key topics related to smart cities. Examples include environmental monitoring for smart urban areas, quality of life for residents in a smart city (with a specific focus on four city-scale phenomena: weather, public transportation, and people flows), as well as data aggregation and quality analysis in a semantic web environment within smart cities. Various applications of smart cities are illustrated in Fig. (**1**). The existing literature contributes to research on different components such as smart people, smart economy, smart governance, smart mobility, smart environment, and smart living. However, the definitions of these terms vary across numerous articles, and these components change according to preferences. For instance, one smart city might focus on a disaster management system, falling under the category of the smart community theme, while another city might prioritize integrating the waste management system into the urban infrastructure [2].

These days, more than 54 percent of the world's population resides in urban areas, and by 2050, this percentage is expected to reach 66 percent. The rapid population growth, coupled with increased urbanization, has given rise to a variety of technical, social, economic, and administrative challenges that tend to threaten the efficient and environmental sustainability of cities. As a result, many governments have been showing interest in adopting “smart” concepts to enhance the utilization and management of both tangible and intangible assets. The 'smart city' concept refers to the application of all available technology and resources in an intelligent and coordinated manner, aiming to develop urban centers that are at once integrated, livable, and sustainable [3]. The smart city boasts a range of remarkable applications in contemporary societies. Examples include smart energy, which enhances the generation, monitoring, and consumption of various types of energy and resources using digital technologies; smart buildings, which autonomously control and manage lighting and temperature systems, security, and energy consumption throughout large constructions; smart mobility, which enables intelligent transportation through innovative and integrated technologies and solutions; smart technology, which facilitates intelligent network connectivity and edge processing solutions in cities worldwide; smart healthcare, which enables intelligent systems and connected medical devices to promote health, provide health monitoring, and diagnostics; and smart governance and education, which offer digital services and policies from the government and foster the educational system through cutting-edge technologies. Additionally, there is smart security, aimed at reducing security risks and providing managed security services to protect people, properties, and information.

2. SMART CITIES APPLICATIONS

Building a smart city aims to benefit inhabitants in various aspects closely related to the standard of living of residents, such as energy, environment, industry, living, and governance, as illustrated in Fig (**1**).

2.1. Smart Government

The smart government plays a pivotal role in a smart city. Its purpose is to better serve citizens and communities by interconnecting data, networks, processes, and physical infrastructures based on information technology. Additionally, smart governance enables citizens to participate in public decisions and city planning, enhancing efficiency while increasing information transparency. For example, e-government allows individuals to access governmental services online, such as scheduling appointments, paying bills, and reporting issues [4].

2.2. Smart Transportation

Smart transportation aims to provide a 'smarter' use of transport systems. Specifically, smart transportation networks can better serve the public by enhancing safety, speed, and reliability. Using transport-oriented mobile applications, consumers can easily organize their schedules and find the most economical and fastest routes. Other common applications in smart transportation include driver’s licenses, license recognition systems, and vehicle parking, among others.

2.3. Smart Environment

A smart environment can contribute significantly to building a sustainable society. Specifically, by adopting technical management tools, a smart city can monitor energy consumption, air quality, structural stability of buildings, and traffic congestion, efficiently addressing pollution or waste. Ideally, novel environmental sensor networks might even be capable of predicting and identifying natural disasters in the future.

CHAPTER 9

Security Metric for Information Network

Saurabh Singhal[1,*] and **Manju**[2]

[1] *Department of Computer Science and Engineering, Apex Institute of Technology, Chandigarh University, Chandigarh, India*

[2] *Department of Computer Science and Information Technology, Jaypee Institute of Information Technology, Noida, Uttar Pradesh, India*

Abstract: Given that dislodged working conditions are in play, system administrators are tasked with handling security solutions that, in turn, impact most of the working layers of the OSI model. This comprehensive approach depicts a situation in which the originator perceives that their data is traversing through a specified encryption process at every stage/layer, starting from the top layer (*i.e.*, Application Layer) and gradually proceeding down to the last one (*i.e.*, Physical Layer). Similarly, the decryption process takes place at every stage/layer at the destination end.

Keywords: Network security, OSI model, Security metrics.

1. INTRODUCTION

In the Internet of Things (IoT) era, the widespread propagation of networks has made network access easier, subsequently allowing a more comprehensive range of unauthorised users to exploit vulnerabilities. Powerful encryption algorithms like the Advanced Encryption Standard (AES) and the Protection in Depth approach are employed to address emerging threats [1]. This work aims to highlight several shortcomings embedded in various layers of the Open Systems Interconnection particularly focusing on issues related to the 8th layer. Growing lapses in cybersecurity within the military sector have led to an increased risk of embedded malware and cyber-attacks from harmful entities and nations, highlighting the growing importance of the new domain of cryptography. At the same time, the accessibility of IoT device networks by a more extensive base has increased the chances of unauthorised access by hackers aiming to exploit these systems. This risk can be mitigated by deploying more complex security algorithms [2].

[*] **Corresponding author Saurabh Singhal:** Department of Computer Science and Engineering, Apex Institute of Technology, Chandigarh University, Chandigarh, India; E-mail: saurabh.singhal09@gmail.com

Samayveer Singh , Manju, Aruna Malik, and Pradeep Kumar Singh (Eds.)
All rights reserved-© 2024 Bentham Science Publishers

2. RELATED WORKS

Network security consists of the policies, procedures, programs, hardware, software, and people you use to protect your corporate IoT network. In general, network security aims to stop unauthorised access to sensitive information, which mainly includes protected health information (PHI) data, payment card industry (PCI) data, and sometimes corporate financials or intellectual properties [3].

The following are the fundamental terms related to network security [4, 5]:

- **Authentication** – This is related to multi-factor authentication, where a user's ID and password are needed to access any application or data stored by some organisation. Most critical industries do not use single-factor authentication (like passwords), as it is pretty easy to retrieve or crack passwords.
- **Firewalls** – It controls the incoming and outgoing overthe network. Nowadays, organizations need to configure firewalls according to their requirement, which is imposed by the application usage.
- **Antivirus, Intrusion Detection, and Intrusion Management Systems** – Firewalls may not be able to catch everything, especially viruses and worms, so antivirus, intrusion detection (IDS), and Security Information and Event Management (SIEM) systems can help detect and stop malware.
- **Encryption** – To enhance security at theorganizational level, they sometimes use various encryption techniques to communicate within the network. This way, they can further protect the data from outsiders.

Apart from these four areas, which are basically followed by small organizations, large corporate networks, and structures enforce a variety of ways to secure their critical data. Below are some more techniques followed by these large organizations to increase network security:

- **Penetration testing** (also known as "ethical hacking") – Penetration testing is a service that involves a professional penetration tester uncovering network security weaknesses.
- **Vulnerability scanning** identifies big risks such as misconfigured firewalls, malware hazards, and remote access vulnerabilities.
- **On-site audits** – Depending on whether you are working towards security mandate compliance (PCI, GDPR, HIPAA), you may need to schedule an onsite audit for your organization.
- **Remediation** –There are some IT teams that can open and close ports on your network and also check someone's activity and regularly install patches.

2.1. Gray Area Network

Due to large businesses and organizations operating with one central headquarters and numerous smaller remote or satellite locations—including telecommuting employees—security efforts, while often focused on the headquarters, must also consider these remote areas as critical to overall network security.

In some cases, organizations have seen their entire headquarters' operations held ransom by malware initially downloaded onto the network through a remote franchise location. Such situations arise due to a portion of the network known as the 'gray area,' which tends to surround remote locations, creating ambiguity around responsibility for security. Questions arise: Is it the headquarters that is responsible for data security and compliance, the franchise, or the telecommuting employees? How reliable is their home network's security [6, 7]. In these scenarios, the main question becomes: Who is responsible? The employee or the corporation? The company does not own the employee's network, yet that network presents a very real vulnerability. Risks increase significantly when there is little to no visibility into these gray area networks. This lack of visibility is also why remote network owners often hesitate to provide insight into their networks, typically citing privacy concerns. However, when remote connections are allowed into your network, you automatically assume some responsibility for any threats that the network may pose, whether you wish to or not.

Therefore, the major concern that arises is: what can be done to help mitigate the risks that gray area networks present to your network while ensuring privacy and control are maintained by the respective network owners [8, 9].

For a large organisation or franchise with numerous remote locations, it becomes crucial to find a network security company capable of providing a level of visibility into your gray area networks to monitor for threats.

To address these issues, the International Standard Organization (ISO) has introduced a layered approach to communication, aiming to overcome the challenges posed by unstructured communication, where the aforementioned threats are more inevitable. ISO's theoretical model provides characterization and standardization of a communication system, dividing it into layers. Created by the International Standard Organization (ISO), this model unifies similar communicating functions into a single layer. Each layer provides services to the one above it and receives services from the layer below [10, 11]. The application and implementation domains of the OSI model are so diverse that it defines how industries related to Information Technology should frame and postulate their networking protocols and rules. The development of each layer is done independently, making them flexible, and enhancements in one layer can be made

SUBJECT INDEX

Samayveer Singh , Manju, Aruna Malik, and Pradeep Kumar Singh (Eds.)
All rights reserved-© 2024 Bentham Science Publishers

Samayveer Singh

Dr. Samayveer Singh received his B.Tech. in Information Technology from Uttar Pradesh Technical University, Lucknow, India in 2007 and his M.Tech. in Computer Science & Engineering from the National Institute of Technology, Jalandhar, Punjab, India, in 2010 and PhD in the Department of Computer Engineering, from Netaji Subhas Institute of Technology, New Delhi, (University of Delhi) India, in 2016. Currently, he is working as an Assistant Professor in the Computer Science and Engineering Department, National Institute of Technology, Jalandhar, Punjab, India. He has published more than 100 research articles in various International Journals and Conferences of repute. He has been included in the list of Top 2% scientists in the world ranking of 2021, released by Stanford University and Elsevier. He is serving as reviewer/member of editorial board for many journals/conferences. His research interests include wireless sensor networks, the internet of things, data hiding, and information security.

Manju

Dr. Manju received a Ph.D. in computer science in 2018. She is currently working as an assistant professor in the Department of Computer Science and Engineering, Jaypee Institute of Information Technology (JIIT), Noida, India. Her research interest includes algorithm designing in wireless sensor networks for coverage, connectivity, routing, and optimized algorithms for Internet of Things (IoT).

Aruna Malik

Dr. Aruna Malik is currently working as an assistant professor in the Department of Computer Science & Engineering in Dr. B R Ambedkar National Institute of Technology Jalandhar, India. Prof. Aruna Malik received B. Tech. in computer science and engineering from Uttar Pradesh Technical University, Lucknow, India and M. Tech. in computer science and engineering from National Institute of Technology, Jalandhar, Punjab, India. She completed Ph.D. in computer science & engineering from National Institute of Technology Jalandhar, Punjab, India. She has a life membership of Computer Society of India (CSI), life membership of IEI, IEEE and ACM. She has published many research papers in various international journals and conferences of repute. Some of his SCI/ SCIE publications in journals of repute are, IEEE Sensor Journal, IEEE Internet of Things Journal, Multimedia Tools and Applications, and Computers and Electrical Engineering. Her research areas lie in the area of internet of things, wireless networks, data hiding and image processing.

Pradeep Kumar Singh

Dr. Pradeep Kumar Singh is currently working as an associate professor at the Department of Computer Science & Engineering in Central University of Jammu, J&K, India. He completed Ph.D. in computer science & engineering from Gautam Buddha University (State Government University), Greater Noida, UP, India. Dr. Singh has a life membership of computer society of India (CSI), life member of IEI etc. His research interests include; data science technologies, wireless sensor networks (WSNs), internet of things (IoT) and information security. He has published many research papers in various international journals and conferences. He has 203 articles in Scopus account. He has authored and co-authored nearly 50 research papers and a number of books. He has a total Google scholar citations of 3800, h-index of 34 and i-10 index of 75. He has received different sponsored research projects grants.