International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 05 | May – 2025 DOI: 10.55041/ISJEM03889
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Real-Time Home Threat Detection Using IoT and ML Techniques

Dr. Mohan Babu C[1], Ravindra Kumar M[2], Suchithra N S[3], Nandini M[4], Shravani N S[5], Nayana M N[6]

[1] *Associate Professor, Department of ECE, SJC Institute of Technology, Chickaballapur, Karnataka, India*
[2]*Assistant Professor, Department of ECE, SJC Institute of Technology, Chickaballapur, Karnataka, India*
[3,4,5,6] *Student, Department of ECE, SJC Institute of Technology, Chickaballapur, Karnataka, India*
[1]mohanbabu015@gmail.com, [2]ravindra.kumar579@gmail.com, [3]suchi13ns@gmail.com,
[4]nandininandu0083@gmail.com , [5]suchi13ns@gmail.com, [6]nayanajanu546@gmail.com

----------***----------

Abstract - The IoT that's decreasingly furnishing people with objects to connected to the physical world which plays most important part in the people's diurnal life. Although it had brought us great convenience, there are also people who had suffered from security vulnerabilities and implicit pitfalls. Presently, the lack of the protection mechanisms for IoT bias with limited coffers makes it easy to be attacked. Then we design an intrusion discovery system in order to cover the IoT security. The system uses supervised literacy to achieve two main functions classifies the generated vicious business and identify the types of attacks.

We propose a light weight point selection system that uses a small number of features to estimate the functions. As a result, in the given bracket of trials, the given system automatically excerpts 88 features, and also the designed system will get a high delicacy rate of 98.7 and 98.99 which means that system has great delicacy by taking a many number of features.

***Key Words*:** Inetrnet of Things (IoT)Intrusion Discovery System (IDS), Industrial IoT, Unified Modeling Language (UML), Convolutional Neural Network (CNN), Support Vector Machines (SVM),

1. INTRODUCTION

IoT has an expanding array of the operations, ranging from the smart home appliances to critical bias, including IOTIPS and the Industrial IoT. The number of IoT bias is projected to grow from 8 million in 2017 to 2 billion in 2020 [1], which clearly brings about a number of security pitfalls. Because of limited computing coffers, sensitive and unencrypted data, open insecure anchorages, and un streamlined vulnerabilities with the firmware for a veritably long time, IoT bias come fluently targets or interceders for attack [1].

An Intrusion Discovery System (IDS) is a great element for network security [1], indeed wireless networks. Nonetheless, classical IT defense styles (e.g., firewalls) prove to be hard to apply in IoT systems. The reason for this is incompletely because the IoT terrain is dynamic and incompletely because there's limited computing. The elaboration of machine literacy technology has introduced new results, because it can constantly learn from variations in the terrain. Nonetheless, there are issues with the prevailing operation [1] of machine literacy technology to IoT intrusion discovery. For one, the intrusion attack types delved are fairly single, and more advanced attack types didn't take into the account. Secondly, in data processing, it's relatively clumsy to determine good features for training the machine literacy model manually because excerpt numerous features will bring a lot of coffers. So, there should be a light system to automatically prize a small number of features for machine literacy to identify multiple IoT attacks.

To break above problems, in this work, we're constructed the IoT platform and initiated six colorful types of network attacks are including the DoS and MITM spoofing, scanning, and Evil Twin AP. also, a statistical analysis- grounded point selection technology is proposed, which significantly saves resource consumption and the calculation. Eventually, by giving the training two- sub caste machine literacy model, the recognition delicacy of the first sub caste machine literacy for vicious business is over to 98.7, and the recognition delicacy of the alternate sub caste machine literacy is over to 98.99 from 6 attack kinds. In summary, the benefactions of this paper as follows.

- We enforced a two- layered IoT intrusion discovery System that can effectively descry vicious business and orders of colorful attacks.
- We put forward a light point selection schemes are grounded on statistical analysis that can effectively optimizes a use of computational coffers and offers effective protection.

2. LITERATURE SURVEY

Y. D. S. V. D, A. Rakhmansyah, et al. he paper titled "Implementasi Sistem Kunci Pintu Otomatis Untuk Smart Home Menggunakan SMS Gateway" by Yan Detha Shandy V.D., Andrian Rakhmansyah, and Novian Anggis Suwastika, published in 2015, discusses the development of an automatic door locking system for smart homes utilizing SMS gateways [1].

A. Siswanto, A. Efendi, et al. The paper titled "Door Access Control Device with Fingerprint Technology in Smart Home Environment with Encrypted Data" by A. Siswanto, A. Efendi, and A. Yulianti, published in 2019, discusses the development of a door access control system for smart homes that utilizes fingerprint technology and data encryption to enhance security [2].

A. Yudhana, et al. The paper titled "Design of a Fingerprint-Based Home Door Security System Using UML Method" by A. Yudhana, published in 2018, discusses the development of a home door security system that utilizes fingerprint recognition technology, designed using the Unified Modeling Language (UML) methodology [3].

B. Septian, et al. This study focuses on designing a fingerprint-based home door security system using UML (Unified Modeling Language). Traditional door locks can be lost or forgotten, but fingerprints provide a natural, unique key that cannot be misplaced. The system utilizes a C3 fingerprint sensor as input, processed by an Arduino Uno ATMega 328

ISSN: 2583-6129
DOI: 10.55041/ISJEM03889

microcontroller. Upon successful fingerprint recognition, a solenoid lock is activated, allowing the door to open [4].

M. Yan, et al. The paper proposes a variable group convolution mechanism to balance computational efficiency and feature extraction. This method replaces depthwise convolutions with a more efficient variable group convolution approach, improving performance in constrained environments [5].

A. Krizhevsky, et al. The paper "ImageNet Classification with Deep Convolutional Neural Networks" by Alex Krizhevsky, Ilya Sutskever, and Geoffrey Hinton (2012) introduced the deep learning model known as AlexNet, which significantly advanced image recognition tasks. This model was the first to successfully apply deep convolutional neural networks (CNNs) to large-scale image classification, achieving breakthrough performance in the ImageNet Large Scale Visual Recognition Challenge (ILSVRC) [6].

A. Najmurrokhman, et al. The paper "Development of a Secured Room Access System Based on Face Recognition Using Raspberry Pi and Android Based Smartphone" by A. Najmurrokhman et al. discusses a security system that uses facial recognition to control access to a room. The system is built using a Raspberry Pi, a webcam, a solenoid door lock, and an Android-based smartphone running Telegram for remote access control [7].

R. A. Isaac, et al. The paper "Face Recognition Security Module using Deep Learning" discusses a face recognition system for smart home and office security applications. The system utilizes OpenCV and dlib to generate face encodings, ensuring efficient recognition with only one image per person. It includes a database verification step to prevent incompatible images and uses a tolerance threshold of 6% for recognition accuracy. The implementation features a web- based interface for image uploads and real-time face authentication [8].

J. Nasir et al. The paper "Development of a Secured Room Access System Based on Face Recognition Using Raspberry Pi and Android Based Smartphone" by A. Najmurrokhman et al. discusses a security system that uses facial recognition to control access to a room. The system is built using a Raspberry Pi, a webcam, a solenoid door lock, and an Android-based smartphone running Telegram for remote access control [9].

Susanto et al. proposed a door security system using the Fisherface method for facial recognition. The system demonstrated reasonable accuracy in identifying individuals and granting access, making it suitable for small-scale security applications. This study emphasized the practicality of integrating facial recognition with physical security hardware [10].

Faisal and Hossain implemented a smart security system using Raspberry Pi and face recognition. Their work showed the feasibility of building low-cost, portable security systems using embedded systems. It highlighted the affordability and accessibility of facial recognition solutions for home security [11].

Hassan et al. introduced a Convolutional Neural Network (CNN) approach for recognizing human actions, particularly for fall detection. While not directly focused on facial recognition, this study contributes to the broader field of intelligent monitoring systems by leveraging deep learning for real-time event detection in smart environments [12].

Wilson et al. conducted a socio-technical analysis of smart home technologies, discussing both the benefits and risks associated with their deployment. The study explored issues such as user privacy, system reliability, and technology acceptance, emphasizing the importance of balancing innovation with ethical considerations [13].

Ahanger and Aljumah provided a comprehensive review of IoT security threats and defense mechanisms. They highlighted the vulnerabilities in interconnected smart devices and proposed frameworks for improving system resilience. Their work is crucial for understanding the risks associated with deploying facial recognition in IoT-based environments [14].

BITAG offered detailed recommendations for IoT security and privacy, stressing the need for standardized protocols, encryption, and user transparency. This report serves as a guideline for developers and policymakers aiming to safeguard personal data in smart security systems [15].

3. METHODOLOGY

- **Existing Methodology**

Existing methods of IoT and machine learning based home security and prevention include: anomaly detection using sensors like motion detectors, smart cameras, door/window sensors to identify unusual patterns, real-time threat analysis through data from multiple IoT devices, intelligent intrusion detection systems, facial recognition for access control, predictive maintenance based on device behavior, and learning-based intrusion detection algorithms to adapt to changing environments; all leveraging machine learning to analyze data streams from connected devices and proactively identify potential security threats in a home setting.

Key aspects of IoT and machine learning in home security:
SENSOR DATA ANALYSIS:

A. Motion Detection: Cameras and motion sensors can detect movement in restricted areas, triggering alerts if unusual patterns are identified using anomaly detection algorithms.
B. Environmental Sensors: Monitoring temperature, humidity, and noise levels can help detect anomalies that might indicate a potential intrusion.
C. Door/Window Sensors: Detecting unauthorized opening of doors and windows in real-time using machine learning to identify suspicious activity.

VIDEO ANALYTICS:

A. Facial Recognition: Identifying known individuals via facial recognition on smart cameras for access control and monitoring.
B. Object Tracking: Tracking movement of objects within a monitored area to detect suspicious behavior.
C. Network Behavior Analysis: Traffic Anomaly Detection: Monitoring network traffic for unusual patterns that might indicate a hacking attempt.
D. Device Authentication: Verifying the identity of connected IoT devices to prevent unauthorized access.

PREDICTIVE MAINTENANCE:
Device Health Monitoring: Analyzing sensor data from IoT devices to predict potential failures or malfunctions in security systems.

MACHINE LEARNING ALGORITHMS USED:
Supervised Learning:

A. Decision Trees: Classifying events as normal or suspicious based on features extracted from sensor data.

ISSN: 2583-6129
DOI: 10.55041/ISJEM03889

B. Random Forests: Combining multiple decision trees to improve accuracy.
C. Support Vector Machines (SVM): Identifying patterns in data for intrusion detection.

Unsupervised Learning:
A. Anomaly Detection: Identifying deviations from normal behavior in sensor data to detect potential threats.
B. Clustering: Grouping similar sensor readings to identify patterns and potential issues.

Benefits of IoT and Machine Learning in Home Security:
A. Proactive Threat Detection: Identifying potential security risks before they escalate.
B. Personalized Security: Adapting security protocols based on individual user behavior and routines.
C. Remote Monitoring: Accessing security status and managing devices from anywhere.
D. Automated Response: Triggering actions like alerts, locking doors, or activating security cameras based on detected threats.

Challenges:
A. Data Privacy Concerns: Protecting sensitive data collected by IoT devices.
B. Network Security: Securing communication channels between IoT devices and the cloud.
C. Device Compatibility: Integrating various IoT devices from different manufacturers.

ML algorithms can analyse network traffic, device logs, and other data related to known attacks or suspicious activity. Anomaly detection ML algorithms can learn IoT device behavior and network interactions through anomaly detection. ML models can detect unusual IoT activity using real-time data.

- **Proposed Methodology**

The proposed system is an embedded automation system. Here the microcontroller will perform the task of a central processing unit. There it will integrate into multiple inputs and output components in order to enable automation, control, and remote access functionalities. The key components are as follows:

SYSTEM OVERVIEW:

The design depicts an overall system armature and pipelining approach. Specifically, the first step of this approach is to gather the business of the network information of the device. The coming step is to apply a machine literacy approach to determine whether the packet is vicious. Incipiently, once the attack happed, determine the attack type. The system affair must include whether a packet entered is vicious and the type of the attack.

Our system armature is shown in Figure 2. To apply the intrusion discovery system to the factual Internet of Things (IoT) effects terrain, we use shell script to emplace Wi- Fi network with jeer Pi as wireless Access Point (AP). We connect the Smart Socket, Smart Light Bulb, Mobile Phone and small Genie to the jeer Pi. After that, the data collection and discovery process is performed on the jeer Pi. The attack machine is our laptop with Kali system. We employ the TCPDUMP [19] tool to capture data and store the captured network business with the PCAP format in the database. And also employ T- wolf tool to prize network features from PCAP train, which is stored as CSV format train. The uprooted data will be uploaded to our laptop for processing data and training model.

DATA COLLECTION:

According to the network structure outlined over, we've conducted a three- day data collection work and gathered around 70000 pieces of data. The contents are bluffing the normal smart home life, e.g., the process of entering and leaving the network of bias, controlling the color of Smart Light Bulb or the on- off of Smart Socket by Mobile Phone, waking up commerce of voice adjunct and controlling other bias, starting a series of network attacks similar as DoS, Scanner, MITM, Faker AP, Injection, ARP, Spoof, DNS caricature. We store every attack packet and normal packet independently to support the following data processing and meanwhile, logs of the launch time and end time of the attack.

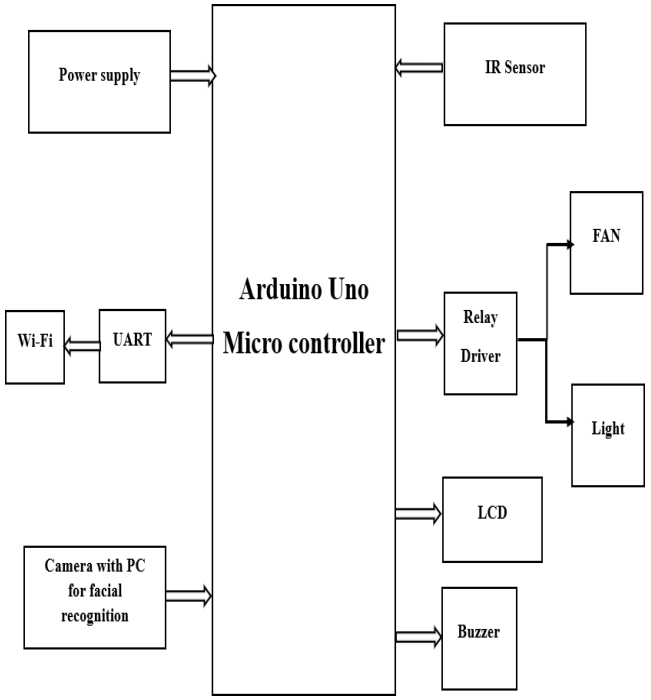

Fig 1: Proposed system Block Diagram

COMPONENTS AND FUNCTIONALITY

1. Microcontroller
   - Core of the system, responsible for processing inputs executing control logic, and managing outputs.
   - Interfaces with switches, relays, sirens, and Wi-Fi modules to enable automation.
2. Power Supply Microcontroller
   - Provides the necessary operating voltage and current for the microcontroller and peripheral devices.
3. Switch/Button Microcontroller
   - Acts as manual input devices to trigger specific operation such as turning ON/OFF appliances.
4. Siren for Alert Microcontroller
   - Used for security or emergency alerts, activated based on pre-programmed conditions.
5. Microcontroller Relay Bulb & Fan /AC

International Scientific Journal of Engineering and Management (ISJEM)
Volume: 04 Issue: 05 | May – 2025
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
DOI: 10.55041/ISJEM03889

- The microcontroller sends control signals to the relay module, which switches high-power electrical appliances like bulbs and fans/AC units.
- The relay ensures electrical isolation between the low - power microcontroller and high-power loads.

6. Microntroller UART Wi-Fi Module

- A universal asynchronous receiver transmitter (UART) interface enables communication between the microcontroller and the Wi-Fi module.
- This allows remote control of appliances via a cloud-based or mobile application.

4. EXPERIMENTAL RESULTS

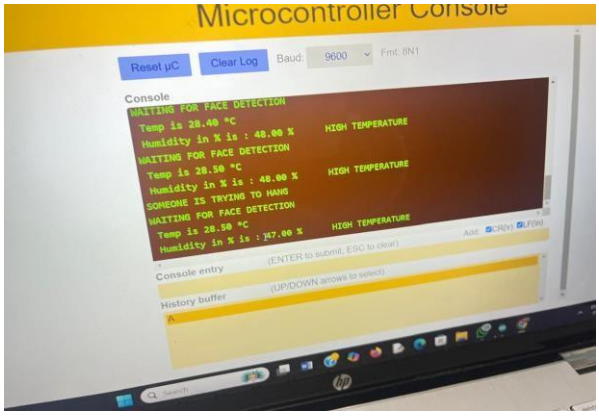

Fig 2: Microcontroller console output displaying temperature and humidity.

Microcontroller Console: This means that the system is interfacing with a microcontroller, a tiny computer on a single integrated circuit. Microcontrollers are commonly used in embedded systems and for device control.

Console Output: The primary part of the screen shows text output from the microcontroller or the software it's executing. This output gives information about the system's status and activities.

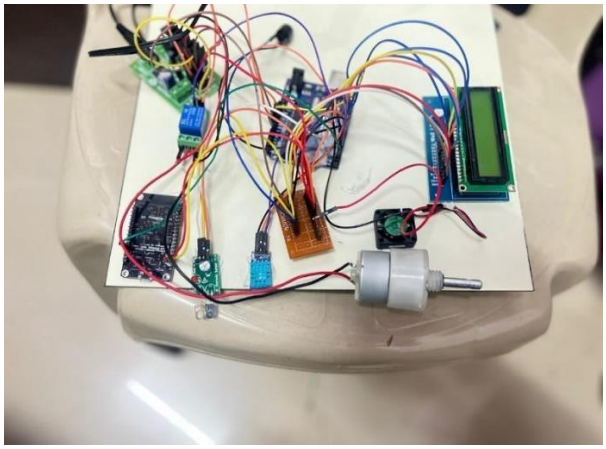

Fig 3: Hardware Circuit Connections

The circuit is connected as shown in the fig 3. This circuit gives the precision output of temperature & humidity displayed on the LCD screen. It displays count of the people present in the home. It detects the suicide the moment a person goes near the fan and gives alert message displaying “Someone is trying to hang” and the buzzer will give beep sound.

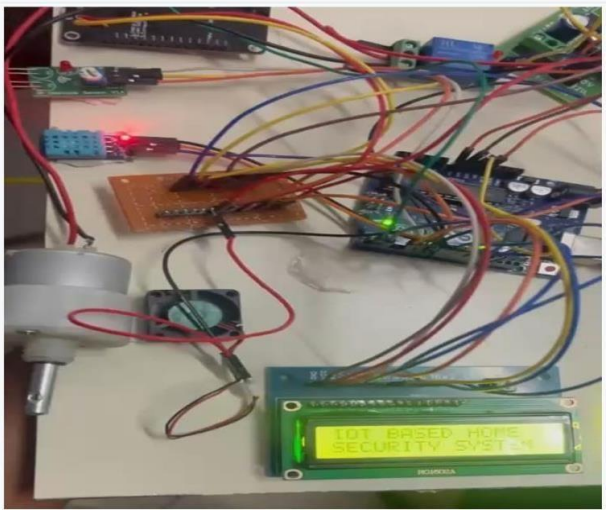

Fig 4: Working Model

5. CONCLUSION

The house security system designed with Arduino Uno, ESP32, and detectors effectively gives an overall safety result by incorporating intrusion discovery, fire peril monitoring, and unusual exertion discovery. The addition of a camera module for face discovery adds security through the forestallment of false admonitions and icing that uncelebrated people are the only bones driving admonitions.

The system effectively identifies and responds to security pitfalls through the display of real- time dispatches on the TV, the periodical examiner, and instant announcements to the stoner's mobile device. Upon an unauthorized entry, fire hazard, or suspicious exertion on the ceiling addict, the system automatically triggers admonitions and exigency responses to act snappily. With Wi- Fi grounded real- time monitoring, home possessors are suitable to admit security events from anywhere.

This design shows how IoT and bedded systems can be used to ameliorate home security, a cost-effective and reliable result. Unborn advancements, like integration with the pall for storing alert logs and images captured, can further ameliorate the system's functionality, making it a worthwhile addition to current smart homes.

ACKNOWLEDGEMENT

Remembering with reverence,We offer my pranamas at the lotus feet of Byravaikya Padmabhushana Pramapoojya Jagadguru Sri Sri Sri Dr. Balagangadharanatha Mahaswamiji.

Submitting devote pranamas and seeking the blessings of his holiness Sri Sri Sri Dr. Nirmalanandanatha Mahaswamiji and poojya Sri Sri Mangalanatha Swamiji .

We own sincere gratitude to Principal Dr. G T Raju, SJC Institute of Technology, Chickballapur for the continuous support, encouragement and insightful suggestions which helped me successfully to complete this Research Work.

We are thankful to Dr. Rangaswamy C, Prof and HOD, Department of Electronics and Communication Engineering, SJC Institute of Technology, Chikkaballapur for supporting me to carry out this Research Work.

ISSN: 2583-6129
DOI: 10.55041/ISJEM03889

Finally, we express our sincere thanks to our Parents, Teaching and Non-Teaching staff of the Department, well-wishers and friends for their constant moral support and encouragement that helped me immensely in the completion of the Research Work.

REFERENCES

1. Han, G., Wu, B., Pu, Y., 2020. A triboelectric nanogenerator grounded on waste plastic bags for flexible perpendicular connection system. Microsyst. Technol. 26(12), 3893 – 3899. https//doi.org/10.1007/S00542-020-04879-6.
2. A. Siswanto, A. Efendi, and A. Yulianti, "Alat Kontrol Akses Pintu Rumah Dengan Teknologi Sidik Jari Di Lingkungan Rumah Pintar Dengan Data Yang Di Enkripsi" J. Penelit. Pos dan Inform. vol. 8, no. 2, p. 97, 2019.
3. A. Yudhana, "Perancangan pengaman pintu rumah berbasis sidik jari menggunakan metode uml" (Jurnal Teknol. Informasi) Sist. PENGGAJIAN KARYAWAN PADA LKP GRACE Educ. Cent., vol. Vol. 1, No., no. 2, p. 12, 2018
4. B. Septian, A. Wijayanto, F. Utaminingrum, and I. Arwani, "Face Recognition Untuk Sistem Pengaman Rumah Menggunakan Metode HOG dan KNN Berbasis Bedded" Pengemb. Teknol. Inf. dan Ilmu Komput, no. 3, pp. 2774 – 2781, 2019
5. M. Yan, M. Zhao, Z. Xu, Q. Zhang, G. Wang, and Z. Su, "VarGFaceNet An Effective Variable Group Convolutional Neural Network for Lightweight Face Recognition" Iccvw 2019, pp. 2647 – 2654, 2019.
6. A. Najmurrokhman, K. Kusnandar, A. B. Krama, E. C. Djamal, and R. Rahim, "Development of a secured room access system grounded on face recognition using jeer Pi and Android grounded smartphone" MATEC Web Conf., vol. 197, pp. 1 – 6, 2018.
7. A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet bracket with deep convolutional neural networks" Adv. Neural Inf. Process. Syst., vol. 2, pp. 1097 – 1105, 2012.
8. R. A. Isaac, A. Agarwal, and P. Singh, "Face Recognition Security Module using Deep literacy, " J. Netw. Commun. Emerg. Technol., vol. 8, no. 10, pp. 10 – 13, 2018.
9. J. Nasir and A. A. Ramli, " Design of Door Security System Grounded on Face Recognition with Arduino, " vol. 3, no. 1, pp. 127 – 131, 2019.
10. B. M. Susanto, F. E. Purnomo, and M. F. I. Fahmi, "Sistem Keamanan Pintu Berbasis Pengenalan Wajah Menggunakan Metode Fisherface Security System Based On Face Recognition Using Fisherface Method" J. Ilm. Inov., vol. 17, no. 1, p. 10, 2017.
11. F. Faisal and S. A. Hossain, "Smart security system using face recognition on jeer Pi" 13th Int. Conf. Software, Knowledge, Inf. Manag. Appl. Ski. 2019, no. August, 2019.
12. M. F. A. Hassan, A. Hussain, M. H. Muhamad, and Y. Yusof, "Convolution neural network- grounded action recognition for fall event discovery" Int. J. Adv. Trends Comput. Sci. Eng., vol. 8, no. 1.6 Special Issue, 2019.
13. C. Wilson, T. Hargreaves, and R. HauxwellBaldwin, "Benefits and pitfalls of smart home technologies" Energy Policy, vol. 103, pp. 72 – 83, Apr. 2017.
14. T. A. Ahanger and A. Aljumah, "Internet of effects A comprehensive study of security issues and defense mechanisms" IEEE Access, vol. 7, pp. 11020 – 11028, 2019.
15. Internet of effects (IoT) security and sequestration recommendations BITA G (Online). Available https//www.bitag.org/report-internet-of-thingssecurity-privacy-recommendations.php, 2016.

BIOGRAPHIES

Dr. Mohan Babu C is Associate Professor in the Department of Electronics and Communication Engineering at SJC Institute of Technology (SJCIT), Chickballapur. With over 17 years of teaching experience, he has made significant contributions to engineering education through his dedication to academic excellence and professional development.

Mr. RAVINDRA KUMAR M presently working as an Assistant Professor in the Department of Electronics and Communication Engineering, SJC Institute of Technology (Sri Jagadguru Chandrashekaranatha Swamiji Institute of Technology). With over 10 years of teaching experience and 2 years of Industrial experience, he has made significant contributions to engineering education through his dedication to academic excellence and professional development.

Ms. Suchithra N S is a Student in the Department of Electronics and Communication Engineering, SJC Institute of Technology (Sri Jagadguru Chandrashekaranatha Swamiji Institute of Technology).

Ms. Nandini M is a Student in the Department of Electronics and Communication Engineering, SJC Institute of Technology (Sri Jagadguru Chandrashekaranatha Swamiji Institute of Technology).

Ms. Shravani N S is a Student in the Department of Electronics and Communication Engineering, SJC Institute of Technology (Sri Jagadguru Chandrashekaranatha Swamiji Institute of Technology).

Ms. Nayana M N is a Student in the Department of Electronics and Communication Engineering, SJC Institute of Technology (Sri Jagadguru Chandrashekaranatha Swamiji Institute of Technology).