Notification No. 554/2024

Date of Award: 14/02/2024

Name of Scholar: Krishan Kant Singh Gautam

Name of Supervisor: Professor (Dr.) Rajendra Kumar

Name of Department/Centre: Computer Science

Topic of Research: Security Issues and preventive measures in the applications of Internet of Things

Findings

The Culmination of my Ph.D. research, spanning seven chapters, the research summary of this thesis is as follow: The Chapter 1, present the state-of-the-art techniques in the area of Internet of Things. The Internet of Things (IoT) is a network of physical objects or people called “things” that are embedded with software, electronics, network, and sensors which allows these objects to collect and exchange data. The actual idea of connected devices was proposed in 1970 Four Key components of IoT framework are 1) Sensors/Devices, 2) Connectivity, 3) Data Processing, 4) User Interface Various applications of IoT are Smart Thermostats, Connected Cars, Activity Trackers, Smart Outlets, Connect Health, etc. Technical Optimization, Improve Data Collection, Reduced Waste, Improved Customer Engagement are key benefits of IoT Security, Privacy, Complexity, Compliance, are key challenges of IoT

. In Chapter 2, we have analysed two techniques which are Cryptography and Steganography and they are used for data security. Basically, cryptography deals with information encryption and security while steganography is basically used for communication security. It could be done to come up with some solutions to limited battery of IoT devices. Similarly, lightweight algorithms could be designed to save computing power. Data management is also a promising field of research. Currently data scientists are in demand everywhere.

. Chapter 3, The findings of this research highlight the urgent need to address these threats and improve the privacy and security of IoT infrastructure. The ramifications of this study's findings on the state of IoT security are substantial. They have the potential to bring about real changes in the sector, such as encouraging producers to priorities safety features or leading to the creation of, or improvement to, standards and regulations. To further enable people to adopt secure practices and safeguard themselves in the IoT ecosystem, it is also possible to enhance user awareness and education.

In Chapter4, we designed one of optimal module which is providing highly home security in very less cost because of developing the system using IoT and object identification. Through this system we can identified unknown person or objects and give the warning and forward the details to homeowner via SMS, Emails and IoT Mobile Application. These techniques are representing more growing nature for smart home security it is combined with IoT and Object identification algorithm. In Chapter 5, IOT are excellent platforms for implementing AI. Digital services may become fully automated as IOT service networks get bigger and more people use them. Withthe aid of AI techniques, the main privacy issues and their solutions could be highlighted. Due to its ability to learn and develop, artificial intelligence (AI) techniques for IOT security are currently receiving the most attention.

The intensity of DDoS and the ensuing damage have increased with the advent of several diversified attack sources, creating an environment that is favorable to harming the security and functionality of IoT technology.

In Chapter 6, we used K-Nearest Neighbour (KNN) and Naïve Bayes (NB) classifier to classify our data and we found better results from KNN instead of NB. In future many researchers can implement different Machine Learning based algorithm on data to classify with more accuracy. They can also work on security of data received from IoT devices and can used confusion matrix data to do so. Data analyst can also work on dark data that is available in huge amount and still not in use, this data can also provide lots of information about the users that can be beneficial for him or any organization but security issues are also present there. So, security will be the main focus of all IoT developers.

Finally, Chapter 7 suggests future research directions in this exciting and developing area of study while outlining the constraints and limitations of the current study.

Overall, research contributions have Developed Security System for IoT Applications Security Awareness Model for IoT Applications. It has laid the groundwork for future research into IoT security and privacy problems to handle the changing obstacles and propel progress.