V.S.B.ENGINEERING COLLEGE, KARUR

Department of Computer Science and Engineering

IBM NALAIYA THIRAN

LITERATURE SURVEY

TITLE : Safety Gadget For Child Safety Monitoring and Notification

DOMAIN NAME : Internet Of Things.

LEADER NAME : Diwakar S

TEAM MEMBER NAME : Dinesh babu P, Dhasarath K P, Ashok Bharathi K

MENTOR NAME : Anandan D

ABSTRACT

Nowadays,the crime rate associated with children keeps increasing due to which draws peoples' attention regarding child safety. This research is conducted to propose a child security smart band utilizing IoT technology. Online questionnaires and semi-structured interviews are methodologies used to collect data. The online questionnaire gains feedback by sending questions electronically, where answers need to be submitted online. In the semi structured interview, researchers meet and ask respondents some predetermined questions while others being asked are not planned in advanced.Through information obtained, a smart band has been proposed to monitor the safety of children. By this, parents know what is happening remotely and can take actions if something goes wrong. The future improvements of this device will be adding functions and software to make it work like a phone such as messaging, gallery, Google, YouTube,meanwhile, adding more child security features so that child safety is guaranteed.

INTRODUCTION

Internet of Things (IoT) is a set of systems and devices interconnected with real-world sensors and actuators to the Internet. It is able to make decisions via detecting the surrounding environment without human interaction. In this research, IoT is applied to propose a wearable smart band which helps parents to monitor and get known of their child's condition anywhere and anytime even if they are not by their children's side. Via the IoT smart band, children's safety is guaranteed, and crime rate is reduced as immediate actions can be taken in case the child is in danger. Besides, unlike the existing smart band, which is less focused on the child security aspect, the proposed system emphasizes getting as much data as possible so that actual situations can be identified.

LITERATURE SURVEY

The Author describes [1] the present era with equal rights, where both men and women are taking equal responsibility in their respective works. Hence women are given equal competition next to men in all fields, they are assigned works in both the even and odd shifts. Every single day women and young girls from all walks of life are being assaulted, molested, and raped. The streets, public transport, public spaces in particular have become the territory of the hunters'. Because of these reasons women can't step out of their house. The only thought haunting in every woman's mind is when they will be able to move freely on the streets even in odd hours without worrying about their security. In critical situations the women will not feel insecure or helpless if they have some kind of safety device with them.

The Author describes[2] IoT devices serve as possible entry points for attackers to breach a company's network, which is why robust security measures are needed to protect them. Today, IoT's scope has expanded to include traditional industrial machines and has equipped them with the ability to connect and communicate with a network. You can find IoT technologies being used for various purposes like medical devices, education, business development, communications, and so on.Before we dive deeper into understandingIoT security, let's shine some light on IoT devices.

The Author describes[3] a recent GSMA intelligence survey that revealed that ninety-eight percent of enterprises want an end to-end security solution that protects data integrity and confidentiality from IoT devices where data is collected, to the cloud where it is stored and processed. Seventy-two percent of enterprises consider device-to-cloud security as a very important feature when selecting a solution. The most common method of protecting data from devices to the cloud is Transport Layer Security (TLS), or Datagram Transport Layer Security (DTLS2). This is especially true of IoT devices. Often the credentials needed to establish this TLS layer are stored in insecure locations in the IoT device. Credentials for access to mobile networks have, on the other hand, been securely stored in tamper-resistant hardware since the inception of GSM networks and SIM cards in the 1990s.

The Author describes[4]Human safety has become one of the most targeted fields for the researchers, owing to its grave importance and the increased competition in the market for human safety gadgets. Hundreds and thousands of human safety devices (HSD) are being developed because of the rapid advancement in the field of Internet of things (IoT) that involve sensing technologies, embedded systems, wireless communication technologies, a variety of sensors etc. An essential function of these devices is human activity recognition (HAR). Present human safety devices continuously track human activities with the help of sensors and track down any unusual activity by performing sensor data analysis (SDA)using machine learning (ML) algorithms. This paper aims at reviewing the latest reported systems for human safety and listing down the various sensors that can be used in human safety devices to detect unusual activities along with the machine learning algorithms that are used for the sensor data analysis.

REFERENCE:

1.Zikriya, M., Parmeshwar, M. G., Math, S. R., Tankasali, S., & Mallapur, J. D. (2018). Smart gadget for women safety using IOT. IJERT, 6(13).

2.Gandhi, Usha Devi, et al. "HIoTPOT: surveillance on IoT devices against recent threats." Wireless personal communications 103.2 (2018): 1179-1194.

3.Lombardi, Federico, et al. "A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids." (2018): 42-6.

4.Sharma, Kritika, and Deepali D. Londhe. "Human safety devices using IoT and machine learning: a review." 2018 3rd International Conference for Convergence in Technology (I2CT). IEEE, 2018.