A REVIEW PAPER ON WOMEN SAFETY USING IOT BASED TECHNOLOGY

[1]Ravi Kiran Rajbhure

1Research Scholar, Department Of Computer Science and Engineering
Dr. A. P. J. Abdul Kalam University, Indore, M.P.

Abstract:The world of intelligence always deals with the updating concepts day-by-day. The intellectual ability of human beings is increasing in vigorous manner, whereas safety with respect to this ever increasing updating technology is a challenging task. Since, security credentials are much vulnerable but at the same time it is very open to the working environment. Also, the safety of that vulnerable data is very important to preserve so as to keep the data at high security new technologies were developing. The updating in technology with that regards goes to IoT based platform. The future of the Internet of Things (IoT) makes many everyday elements to be connected via network. Collection and sharing of information within themselves through monitoring, collecting through sensors are the basic idea behind the concept of IoT.

Keywords: IoT, Network, Mobile, Sensors, Actuators

I. INTRODUCTION

In past decades women hesitate to step out from their house for normal things, so it required more safety. But in the recent situation various mechanism viz. Network mechanism, Mobile mechanism, Helpline numbers and various systems were designed to overcome the women in critical situations but the accuracy with those mechanism is less which results in many crime situations. Every system has different techniques to measure the severity of the situations

More accuracy in this system comes with the use of updating technology which helps to reduce the risk factors among women and even though children. In this paper, we discuss about the scenario of how updating technology makes data more vulnerable and how it helps to make the safety of women & child through its application point of view. Some sensing parts mentioned in the system which helps to generate data at high and future risk of such situations got reduce using sensors and actuators used in the design. Many crimes against women has increased to a greater extent and due to which harassment takes place at working place, shopping, evening walk, eve teasing and many more.

II. WHAT IS IOT?

The internet of things, or IoT (we mentioned in next phases), is a system of interrelated computational devices, mechanical and digital machines, objects, animals or people with unique identification and the potential to communication in transmission as well as receiver point of view without intervention with human being. A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an IP address and is able to transfer data over a network. With increase in various technological updation and upgradation the use of IoT is icreasing day by day

- ***History of IoT***

Kevin Ashton, co-founder of the Auto-ID Center at MIT, first mentioned the internet of things in a presentation he made to Procter & Gamble (P&G) in 1999. Wanting to bring radio frequency ID (RFID) to the attention of P&G's senior management, Ashton called his presentation "Internet of Things" to incorporate the cool new trend of 1999: the internet. MIT professor Neil Gershenfeld's book, *When Things Start to Think*, also appearing in 1999, didn't use the exact term but provided a clear vision of where IoT was headed.

IoT has evolved from the convergence of wireless technologies, microelectromechanical systems (MEMS), microservices and the internet. The convergence has helped tear down the silos between operational technology (OT) and information technology (IT), enabling unstructured machine-generated data to be analyzed for insights to drive improvements. Although Ashton's was the first mention of the internet of things, the idea of connected devices has been around since the 1970s, under the monikers *embedded internet* and *pervasive computing*.

The first internet appliance, for example, was a Coke machine at Carnegie Mellon University in the early 1980s. Using the web, programmers could check the status of the machine and determine whether there would be a cold drink awaiting them, should they decide to make the trip to the machine. IoT evolved from machine-to-machine (M2M) communication, i.e., machines connecting to each other via a network without human interaction. M2M refers to connecting a device to the cloud, managing it and collecting data. [1]

III. IoT UNDER RESEARCH

The traditional fields of embedded system, wireless sensor networks, control system, automation systems are together interconnected to form the IoT. That means the internet of things builds over the revolutionary success of mobile and internet network [9, 10]. Even a few decades back, nobody could have imagined having a video chat with their families. Nowadays, it is merely a child's play. All of this is due to the wide availability of internet and creation of devices with Wi-Fi abilities. Technology costs are going down, and smart-phones are capable of doing almost anything with their inbuilt features and apps. What we have till now is "Internet of Computers (IoC)" and it is gradually growing in size. This so called IoT is sitting on a perfect storm. And the storm revolves around five basic areas Sensor technologies, Local processing, Networking models, Data Science and Predictive Technologies, Machine Learning and Security. The Secure Internet of Things Project is a cross-disciplinary research effort between computer science and electrical engineering faculty at Stanford University, University of California - Berkeley, and the University of Michigan. The research effort focuses on three key domains:

- ***Hardware and software systems***

  Construction of hardware and software systems that will make the IoT enabled systems intelligent and secure.

- ***Analytics***

  Integrating and analyzing enormous field of Hardware with all of existing data.

- ***Security***

  Developing pervasive sensing and analytic systems to preserve and protect user security.

- ***Technologies to support IoT***

Some of the technologies converging to support and enable IoT applications are architecture, Identification, Communications, Network Technology, Network Discovery, Software and algorithm, Hardware Technology, Data and signal processing, Discovery and Search Engine, Net-work Management, Power and Energy Storage, Cyber Security, Information security etc. Challenges and research areas of IoT [3]

- Robustness
- Privacy
- Cloud computing
- Cyber physical system
- Autonomic Computing
- Social Networks
- Security

IV. IoT IS THE BEST SOLUTION

While discussing with various fundamental solution finding solution with the basic need of physical factor is of utmost importance.And to follow to this IoT provides the best possible solutions and are discuss as follows:

4.1. Secure the IoT Network

Protect and secure the network connecting IoT devices to the back-end systems on the internet by implementing traditional endpoint

Security features such as antivirus, anti-malware, firewalls, and intrusion prevention and detection systems.

4.2. Authenticate the IoT Devices

Allow the users to authenticate the IoT devices by introducing multiple user management features for a single IoT device and implementing robust authentication mechanisms such as two-factor authentication, digital certificates, and biometrics.

4.3. Use IoT Data Encryption

To protect the privacy of users and prevent IoT data breaches, encrypt the data at rest and in-transit between IoT devices and back-end systems by using standard cryptographic algorithms and fully-encrypted key lifecycle management processes to boost the overall security of user data and privacy.

4.4. Use IoT PKI Security Methods

To ensure a secure connection between an IoT device & app, use IoT public key infrastructure security methods such as X.509 digital certificate, cryptographic key, and life-cycle capabilities including public/private key generation, distribution, management, and revocation.

4.5. Use IoT Security Analytics

Use IoT Security Analytics Solutions that are capable to detect IoT-specific attacks and intrusions, which can’t be identified by traditional network security solutions like firewalls.

4.6. Use IoT API Security Methods

Use IoT API Security methods not only to protect the integrity of the data movement between IoT devices, back-end systems, and applications using documented REST-based APIs, but also to ensure that only authorized devices, developers, and apps are communicating with APIs or detecting potential threats and attacks against specific APIs.

4.7. Test the IoT Hardware

Place a robust testing framework in place to ensure the security of IoT hardware. This includes stringent testing of the IoT device’s range, capacity, and latency. The chip manufacturers of the IoT devices also need to reinforce the processors for more security and less power consumption without making them too expensive for the buyers or too impractical to be used in the current IoT devices given the fact that a majority of the IoT devices available today are cheap and disposable with a very limited battery power.

Also, the IoT device manufacturers need to do a broad testing of all the third-party components and modules that they are using in their IoT devices to ensure their proper functioning with their IoT applications.

4.8. Develop Secured IoT Apps

Given the immaturity of the current IoT technology, the developers of the IoT applications must emphasize on the security aspect of their IoT applications by strictly implementing all the above-mentioned IoT security technologies. Before developing any IoT applications, the developers must also do a complete research on the security of their IoT applications and try their best to strike a perfect balance between the User Interface and Security of their IoT apps.

4.9. Avoid Launching IoT Devices in a Rush

To stay ahead in the competition, the manufacturers of the IoT devices are often in a rush to launch their products in the market at the lowest prices. And, while doing that, they don’t pay enough attention to provide security updates and patches. This poses a serious threat to the security of their IoT devices in the long run.

To overcome this challenge, the manufacturers of the IoT devices should avoid launching their products without proper planning for the long-term support for the security of their IoT devices and applications.

4.10. Beware of Latest IoT Security Threats & Breaches

To ensure the security of the IoT devices and applications, the device makers and app developers must beware of the latest IoT security threats and breaches. Since the IoT is still an emerging technology, its security breaches are bound to happen. Hence, both IoT device manufacturers and the IoT app developers must be ready for the security breaches with a proper exit plan to secure maximum data in case of a security attack or data breach.

Last but not least, both IoT device makers and IoT app developers must also take an initiative to teach their employees and users about latest IoT threats, breaches, and security solutions.

V. Structure of its working

Basically, there are three IoT architecture layers:

1. The client side (IoT Device Layer)

2. Operators on the server side (IoT Getaway Layer)

3. A pathway for connecting clients and operators (IoT Platform Layer)

Therefore, all the above-mentioned requirements are addressed in 4 stages of IoT architecture described here—on each separate stage and after completing the overall building process. In simple terms, the 4 Stage IoT architecture consists of

1. Sensors and actuators

2. Internet getaways and Data Acquisition Systems

3. Edge IT

4. Data centre and cloud.

VI. Application in women safety

6.1. Involvement of Embedded System

It can be concluded that the system helps to supports the gender equality by providing safe environment to women in the society, and allows them to work till late nights. Anyone before doing any crime against the women will be deterred and it help reducing the crime rate against the women. [4]

The level of security can be increased more by electronics assistance device in the vehicle, which can track the journey or women passenger, and ensure she has completed journey without any problems, this will not only make them safe but their parents, kids or husbands will also feel stress free as they are virtually in touch during complete journey [5]

Ladies' security is a basic issue in this day and age and it's especially required for each person to be acting over such an issue. This paper depicts a "GPS, GSM and Zapper Circuit based ladies security framework" that gives the mix of GPS gadget particular to track the area and in addition give alarms and messages a crisis catch trigger. It additionally contains stun instrument to create non-deadly electric stun in crisis circumstance. Our try behind this paper is to outline and create a device which is so conservative in itself that give favourable position of disguise. The fundamental point of interest of this framework is that the client does not require a Smartphone dissimilar to different applications that have been created before. [6]

This system it detects the fall detection accelerometer, temperature, acid gas detection and heart beat in both normal and abnormal conditions of the patients. In mobile screen both normal and abnormal values are displayed. Adriano microcontroller compares the maximum and minimum values and if the patient is in abnormal condition then abnormal values are detected and the buzzer indicate a beep sound and the data are sent through the gsm/gps module always the mobile receives the data. The doctor / relatives receive the data and if the patient is in critical condition by their turn can send an ambulance to the patient location [7]

VII. Advantages

1. Save time: As it reduces the human effort then it definitely saves out time. Time is the primary factor which can save through IoT platform.
2. Enhance Data Collection
3. Improve security: Now, if we have a system that all these things are interconnected then we can make the system more secure and efficient.

VIII. Disadvantages

1. There are security measures that are taken to protect information, but there is always the possibility of hackers breaking into the system and stealing the data.
2. Also, companies could misuse the information that they are given access to. This is a common mishap that occurs within companies all the time. Just recently Google got caught using information that was supposed to be private. Information, such as the data collected and stored by IoT, can be immensely beneficial to companies.
3. The privacy issues also leads to the question of who will control the Internet of Things?
4. Another argument against IoT is the over-reliance on technology. [8]

IX. Conclusion

Hence more accuracy in this system was achieved with the use of updating technology which helps to reduce the risk factors among women and even though children. Discussion was made about the scenario of how updating technology makes data more vulnerable and how it helps to make the safety of women & child through its application point of view. Some sensing parts mentioned in the system which helps to generate data at high and future risk of such situations got reduce using various embedded devices. Many crimes against women has increased to a greater extent and due to which harassment takes place at working place, shopping, evening walk, eve teasing and many more. This technology helps to generate the simulation with resect to panic situation by considering various body measures and help in the case of emergency.

REFERENCES

[1] https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

[2] http://dst.gov.in/internet-things-iot-research-initiative

[3] https://www.rapyder.com/top-10-iot-security-solutions-common-iot-security-issues/

[4] https://pdfs.semanticscholar.org/10ba/edd4c57b43ba4dadac45852d17a322123659.pdf

[5] https://ijireeice.com/upload/2016/march-16/IJIREEICE%208.pdf

[6] http://data.conferenceworld.in/NEXGEN/78.pdf

[7] http://ijsrcseit.com/paper/CSEIT184506.pdf

[8] https://sites.google.com/a/cortland.edu/the-internet-of-things/disadvantages