Community Services using Internet of Things

Sangeetha Komandur
Lecturer,
Department of Computer Science,
Jazan University

Sameena Shaik
Lecturer,
Department of Computer Science,
Jazan University

Sayyada Sara Banu
Lecturer,
Department of Computer Science,
Jazan University

Shazia Ali
Lecturer,
Department of Computer Science,
Jazan University

Samar Mansour Hassen
Lecturer,
Department of Computer Science,
Jazan University

Fazeelatunnisa
Lecturer,
Department of Computer Science,
Jazan University

ABSTRACT
This paper will go over community services, which are an Internet of Things application that relates to a prototypical category of cyber-physical platforms with cooperating components. Following that, basic smart community architecture is developed, and we explain how to ensure safe & strong communication throughout specific residences. It introduce two improved knowledge applications, Community Watch and Health, as well as enabling methodologies & challenges, that we anticipate some few valuation smart services to the community.

Keywords
community services, IoT, SN, Healthcare, Neighborhood Watch

1. INTRODUCTION
The Internet of Things is a new phrase for networked everyday objects that connect with one another via wireless sensors. Smart homes are a prominent Internet of Things application. It develops a prospective environment at home in which integrated sensors and devices (for example, home appliance devices) are auto and can be remotely controlled through Internet, enabling for variety of measurement and management applications. Such devices monitor and archive user behavior, anticipate subsequent behaviour, and plan everything advance depending on the user's preferences or requests, providing the user with maximum convenience, comfort, efficiency, and security [1]. IoT is a key impact area within these cyber-technologies, and "Smart Cities" initiatives reflect the aggregation of such cyber-technologies to aid in solving cities' difficulties [2].

The IoT is based upon that Computer Internet Network (CIN) and employs innovations including such Radio Frequency Equipment, Data Transmission Communication, Computer Vision and Identification, Spatial Analysis, and others to form a network that takes up an entire planet [3].

Social Internet of Devices (SIoT) is a new revolution for Internet of Things networks based on social relationships between things. Smart objects are linked together through social relationships such as parental (devices of the same model and queue), cross (devices in almost the same location), founder (gadgets that collaborate), equity (equipment controlled by another customer), but also community object (equipment with scattered correlations based on user relation) [4].

A Social Network (SN) for smart objects may be used to provide networks routing performance, network management, & compatibility in a safe environment. Ericsson researchers have suggested using SN for IoT [5].

2. RELATED WORK
In a trusted environment, using a Social Network (SN) for smart objects, one may accomplish network navigability, service discovery, and interoperability. Ericsson researchers suggested adopting SN for IoT as well [6]. One of the most important components of installing and maintaining future connected smart communities is building a safe access control system to protect user data security and privacy. Smart Communities (SCs) are emerging today as a result of the confluence of Internet, Cyber-Physical Systems, clouds and computing capabilities, especially intelligent approach based upon AI and Machine Learning technology. SCs are made up of physical equipment, items, and users, all of which are constantly linked and interacting with one another [7]. In the research community, smart communities have received a lot of interest. highlightedblockchain uses difficulties, and prospects for smart communities[8]. Wireless transmission techniques, as well as other native applications, problems, and future trends using IoT in intelligent logistical, really aren't taken into account, other essential uses, problems, and future directions of IoT in intelligent logistical are overlooked [9]. IoT is discussed exclusively from efficient logistics processing information (e.g., operational processes) with communication devices.

Monitoring systems, RFID, M2M, internet Technology, statistical data aggregation, information retrieval, IPv6, or other Iot supporting techniques are discussed in [11] and categorised: I technologies that enable "objects" to obtain context data, (ii) technology that enable "objects" to processing context data, & (iii) technology that enhance privacy and security [12]. Monitoring systems are thought of as morning systems comprised of autonomous navigation sensing devices (mobile robots) that collaborate and use distributed coordination to execute complex real-time tasks in the face of uncertainty. The fundamental challenge in building these networks is their dynamic topology and architecture, which is caused by either the mobility of sensing devices or the limited energy budget, which involves turning off individual sensors to preserve energy. This condition has the potential to have a significant impact on sensor network performance in terms of sensing coverage and network connectivity [13]. It is well accepted that the valuation received by devices reduces dramatically) with time - distance, and also that inertial sensors compilation must account for this [14].

3. THE INTERNET OF THINGS

IoT is a phrase which has been defined in such a number of different ways. At its most basic, the IoT is a connection of intelligent devices, sometimes known as things. Sensor nodes, actuators, everyday goods with computer and communication capabilities, and network nodes including such RFID tags, cellphones, smartwatch, ipads, smart thermostats, as well as other similar technologies are examples of things in the IoT. The majority of IoT devices communicate via wireless connectivity. More complex equipment, such as various types of production controls, could be part of an industrialized IoT system and, as a result, have a wired Internet connection. IoT devices are capable of detecting, gathering, and aggregating data from the real world. At the very same time, IoTs can "complete the loop." More advanced equipment, such as various types of process controllers, may be part of an industrial IoT system and have a wired Internet connection as a result. IoT devices are capable of sensing, collecting, and aggregating data from the real world. At the same time, the IoTs can "complete the loop" by acting on the environment in response to aggregated data via actuators and controllers. IoT may be thought of as Cyber-Physical Systems in this respect (CPS).

4. SMART COMMUNITY APPLICATIONS

4.1 Healthcare

By making better use of community healthcare resources and recognising life-threatening problems early, healthcare apps built in a smart community reduce community residents' need on special caregivers and cut their healthcare expenses. The applications rely on constant monitoring of environmental factors and the physiological state of community inhabitants given by wireless body sensors spread throughout the human body to provide accurate and prompt emergency responses. As a result, the improved knowledge environment provides a smooth wifi connection to neighbouring healthcare experts and remote healthcare institutions from any position inside the neighbourhood.

Residents' personal health information (PHI) is shared over the collaboration via healthcare applications, exposing it to unlawful acquisition, exposure, or even other inappropriate purpose, providing a privacy risk to those residents. One privacy risk is the sensitive and hidden nature of PHI. Another concern is that if an observation understands that what a residence often submits her or his PHI to a specific medical professional, the observer can properly predict that resident's sickness based on the medical treatment domain of the healthcare worker. As previously indicated, cryptography, packet re-encryption, and mixed techniques can all assist to mitigate these issues?

4.2 Neighborhood Watch

There are typically implemented as a component of a neighbourhoodorganisation, which consists of a collection of people devoted to the prevention and detection of crime and destruction. Instead of interfering when questionable behaviour is seen, members notify authorities. Due to unavailability, exhaustion, attentiveness, and limited perception, sentient community watches are unpredictable and ineffectual. The smart community setup is excellent for adopting unattended and pervasive always-on neighbourhood watches, which saves time and money while increasing effectiveness and efficiency. Surveillance cameras are installed in each home. These cameras continually watch their associated residences' surrounds, encompassing not just the yards but also adjoining road/street parts.

5. COMMUNITY SERVICES NETWORKING

The smart community architecture's home domain is focused on intra-home networking, or how to connect smart objects, home automation, security systems, as well as other applications in a smart home environment. In the community sector, the smart community concept has resulted in a new inter-home (community) networking problem. To make the presentation simple, we should use terms nodes, access point, and home devices (or house) consistently.

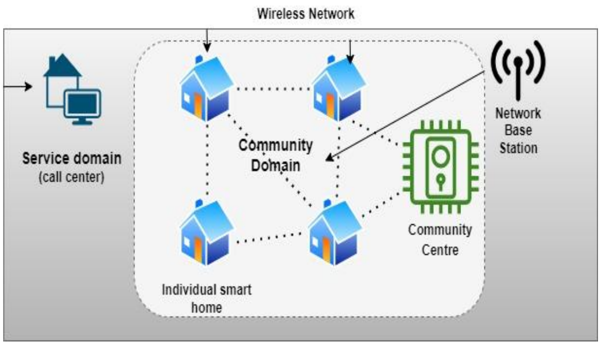

Fig. 1. Community service

The community network is a traditional wireless ad hoc network, as you can see. The five essential security requirements are data exclusivity, consistency, validity, quasi, and password protection. In order to meet the first four goals, traffic on the network in a smart grid system must be protected. The last requirement can be accomplished in a variety of ways depending on the type of traffic. A community network's traffic can be classified as either publicly or privately. Both types of communication have their information encrypted to prevent outsiders from reading private communication, including such personal health information collected for the benefit of specific homes.

These contents must not be shared with the other community members. The goal of public transportation, including safety warnings, is really to benefit a whole community. As a result, it is open to everyone in the community.

HEALTHCARE

Healthcare applications developed in a smart environment reduce the need for special caregivers and save healthcare expenditures by making better use of community healthcare resources and detecting existence events earlier. To provide an accurate and timely emergency response, the apps rely on continuous monitoring of ambient conditions and the physical status of community residents provided by wireless body sensors placed throughout the human body.Residents' personal health information (PHI) is shared over the community via healthcare applications, exposing it to unlawful acquisition, exposure, or even other inappropriate usage, providing a privacy threats to those citizens. One privacy risk is the delicate and hidden character of PHI. Another difficulty is that if an investigator learns that a residence often submits her or his PHI to a certain health professional, the observer can properly predict that resident's sickness based on the medical treatment domain of the healthcare worker. Cryptography, packet re-encryption, and hybrid approaches can all aid in the resolution of these issues.

5.1 Utility Management

Individual house utility consumption may be measured more easily in a smart community context. It sends the data to the contact center regularly, which subsequently provides it to the utility providers for automated billing. Because the utility management process does not require direct human participation, the utility company's operational costs are minimized.

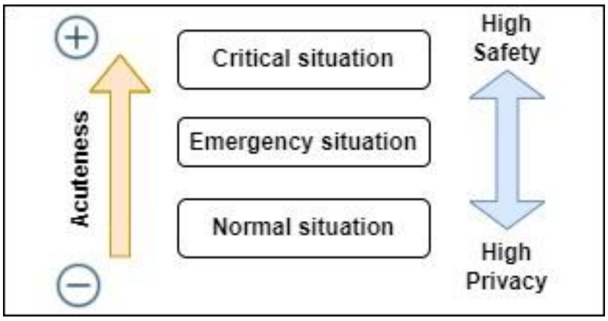

Fig. 2. Access control in healthcare

5.2 Social Networking

In the smart community context, there is also a social network platform. Residents can contact with people in the region in a simple and cost-free manner by using the community network. Because of the geographic proximity, this form of social network may be more helpful than Web networks in many situations. Playing online games is a popular activity that has increased in popularity significantly in recent years. The superior community technology of the smart community enables the development and implementation of low-cost online games.

6. CHALLENGES

Existing target tracking algorithms, such as those employed by Neighborhood Watch, are unsuitable for benefits scenarios in which a target's mobility is limited to community streets/roads. This constraint simplifies the problem's solution. Certain intrusion detection techniques may be borrowed to help with this problem. Finally, an intelligent context-aware matching algorithm is intended to avoid or reduce both false positives and false negatives [16]. Fine-grained access control is utilised in healthcare to address community members' contextually adjusted privacy concerns. The brute-force method is time and computation inefficient, and therefore is not a realistic alternative. Finding successful ABE schemes based on disguised access rules might be a future research priority for providing ubiquitous healthcare in smart community settings [17].

7. CONCLUSION

In this paper, we explored community services as just a different Internet of Things service. Based on wireless communications and networking technologies, a community service unites smart dwellings in a surrounding area, enabling a variety of useful and prospective services such as neighbourhood watch and healthcare. It opens the door to a new line of inquiry and a load of new difficulties to address.

8. REFERENCES

[1] Domb, M. (2019, February 28). Chapter: Smart Home Systems Based On Internet Of Things. Smart Home Systems Based on Internet of Things | IntechOpen. https://www.intechopen.com/chapters/65877.

[2] Zanella, A., Bui, N., Castellani, A., Vangelista, L., &Zorzi, M. (2014). Internet of things for smart cities. IEEE Internet of Things journal, 1(1), 22-32.

[3] Khanna, A., &Kaur, S. (2020). Internet of things (IoT), applications and challenges: a comprehensive review. Wireless Personal Communications, 114(2), 1687-1762.

[4] Atzori, L., Iera, A., Morabito, G., & Nitti, M. (2012). The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization. Computer networks, 56(16), 3594-3608.

[5] Fizza, K., Banerjee, A., Mitra, K., Jayaraman, P. P., Ranjan, R., Patel, P., &Georgakopoulos, D. (2021). QoE in IoT: a vision, survey and future directions. Discover Internet of Things, 1(1), 1-14.

[6] Kowshalya, A. M., &Valarmathi, M. L. (2015). Improved network navigability and service search in social internet of things (SIoT). International Journal of Research and Scientific Innovation, 2(9), 75-77.

[7] Rao, P. M., &Deebak, B. D. (2022). Security and privacy issues in smart cities/industries: technologies, applications, and challenges. Journal of Ambient Intelligence and Humanized Computing, 1-37.

[8] Aggarwal, S., Chaudhary, R., Aujla, G. S., Kumar, N., Choo, K. K. R., &Zomaya, A. Y. (2019). Blockchain for smart communities: Applications, challenges and opportunities. Journal of Network and Computer Applications, 144, 13-48.

[9] Song, Y., Yu, F. R., Zhou, L., Yang, X., & He, Z. (2020). Applications of the Internet of things (IoT) in smart logistics: a comprehensive survey. IEEE Internet of Things Journal, 8(6), 4250-4274.

[10] Noura, M., Atiquzzaman, M., &Gaedke, M. (2019). Interoperability in internet of things: Taxonomies and open challenges. Mobile networks and applications, 24(3), 796-809.

[11] Patel, K. K., & Patel, S. M. (2016). Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. International journal of engineering science and computing, 6(5).

[12] Capitan Fernandez, J., Martinez-de-Dios, J. R., Maza, I., Ramon, F. F., &Ollero, A. (2015). Ten years of cooperation between mobile robots and sensor networks. International Journal of Advanced Robotic Systems, 12(6), 70.

[13] Martínez-de Dios, J. R., de San Bernabé, A., Viguria, A., Torres-González, A., &Ollero, A. (2017). Combining unmanned aerial systems and sensor networks for earth observation. Remote Sensing, 9(4), 336.

[14] Patel, P. D., Lapsiwala, P. B., & Kshirsagar, R. V. (2012). Data aggregation in wireless sensor network. International Journal of Managment, IT and

Engineering, 2(7), 457-472.

[15] Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. Information systems frontiers, 17(2), 261-274.

[16] Carpenter, B. B. (2005). Science. gov: FirstGov for Science. Reference Reviews.

[17] Guo, C., Zhuang, R., Jie, Y., Ren, Y., Wu, T., &Choo, K. K. R. (2016). Fine-grained database field search using attribute-based encryption for e-healthcare clouds. Journal of medical systems, 40(11), 1-8.