International Journal of Academic Multidisciplinary Research (IJAMR)
ISSN: 2643-9670
Vol. 5 Issue 11, November - 2021, Pages: 1-6

A review of Internet of Things for Smart Homes Environment: Applications and Challenges

John W. Kasubi [1] and Manjaiah D. Huchaiah[2]

[1]Department of Computer Science, Mangalore University, INDIA, Local Government Training Institute, Dodoma, TANZANIA
johnkasubi7@gmail.com
[2]Department of Computer Science, Mangalore University, INDIA
drmdhmu@gmail.com

Abstract: The rapid growth of the Internet of Things (IoT) has led to the development of many smart devices that have empowered homes to become Smart Homes (SH). Smart Homes play an essential role in their applications in various fields such as security, healthcare, water, and energy usage, etc. This rapid growth of IoT has led to many positive impacts in society and challenges to its applicability. This paper first presents the concept of IoT and Smart Home, Architecture of IoT and Smart Home, applications of IoT and Smart Home, challenges of IoT and Smart Home. Different related previous works were discussed and identified most challenges that face both IoT and Smart Home that need to be addressed; finally, potential solutions are suggested for future IoT and Smart Home directions.

Keywords: Internet of Things (IoT), Smart Homes, Applications, Challenges

1. INTRODUCTION

The Internet of Things (IoT) provides a connection to millions of physical devices worldwide. It allows them to communicate automatically over a single network without human involvement. The concept behind the IoT is that everything speaks to everything; you remain updated and your machines. The aim is to provide self-reporting devices in real-time that increase the reliability, efficiency, and consistency of surface information distribution more rapidly than a system based on human involvement [1].

The IoT plays a significant role in Smart Homes' existence. It helps collect information from sensors, computers, networks, and applications to access important, operative information. The IoT gathers, handles, analyses, and visualizes data to predict human activities performed at smart homes. The IoT has facilitated different applications at homes such as security, healthcare, control, water and electricity usage, hence quality life at home.

2. INTERNET OF THINGS (IOT)

2.1 The Concept of Internet of Things (IoT)

The term Internet of Things (IoT) became famous in 1999 when Kevin Ashton first coined it. The Internet of Things (IoT) can be defined as the interconnection of physical objects or things globally through sensors and actuators. This includes any items such as rehabilitation equipment, house equipment, production machinery, devices, etc. The physical objects are connected to the Internet through standard protocols such as Wi-Fi, Zigbee, RFID, Bluetooth, and so on [2]. RFID use radio wave to recognize objects gathers and enters data about them automatically into computer systems with little to no human involvement. At the same time, Zigbee is an alternative to Wi-Fi and Bluetooth; it is used to transfer or share the collected data from connected devices over the network without human involvement. These protocols furnish the whole communication processes within the network, in the case, that information can be shared and controlled without visiting each thing independently. This is possible because the power belongs to these protocols. Things can identify with each other, share and communicate over the connected network, due to the common language, known as protocols [3].

Things:

These are objects equipped with sensors and actuators that allow data to be collected, transmitted and acted upon through the Internet over a local network or wireless. Things include; lights, fridges, coffee machines, heaters, doors-locks, buildings, etc. [4].

2.2 Architecture of IoT

The architecture of IoT comprises three significant layers; physical layer, Network layer and Application layer. The Physical layer consists of wireless sensors and actuators, Sensors gather data from the surrounding environment and convert it into useful information, different devices are employed to carter for this task, includes; surveillance systems, temperature sensors, light sensors, smoke sensors, humidity sensors, home voice controls, etc. The devices collect a large amount of data and send it to the Network layer. The network layer combines all data collected at the physical layer and converts raw sensor data into digital streams through a data acquisition system (DAS), aggregated and digitized data are routed over the network to the Application layer for further processing. The last layer under IoT architecture is an Application layer, the aggregated and digitized information are fed into the server for analysis and applied as a new product and services to the end-users [5].

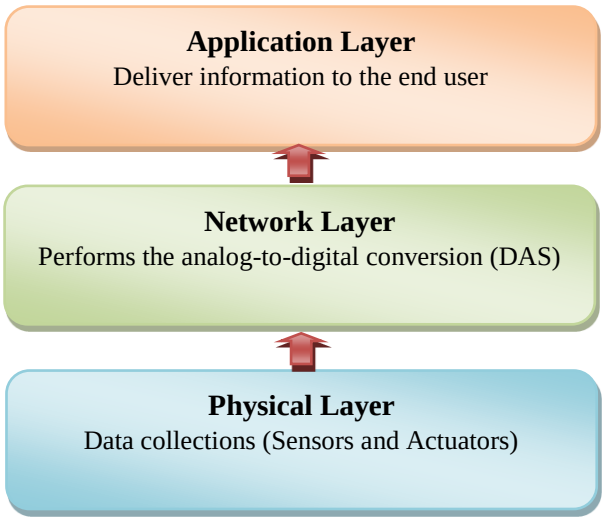

Fig.1 IoT Architecture

2.3 The applications of IoT

The IoT has made remarkable progress in different fields such as [6] [7]:

- *Healthcare* – IoT has helped diagnose the disease early, help healthcare professionals track patients inside and outside a hospital environment, and computers analyse data to help physicians change treatments and enhance patient results. During the covid-19 pandemic, IoT has helped track, diagnose, and predict the infection's spread, search for treatments and a vaccine, and social distance control.
- *Agriculture* – IoT is used in agriculture for precision farming, smart irrigation and smart greenhouse.
- *Industrial Automation* – IoT is used to produce quality products, time-saving, quality control, cost-effectiveness and security.
- *Disaster Management* – IoT is used to predict what is likely to happen in the near future. It helps for preparedness, response and resilience of what was predicted.
- *Smart City* – IoT has been used to Improves the efficiency, effectiveness, transparency, and accountability of quality delivering government services to the public at any time anywhere and at an affordable cost; such services include Healthcare, Education, Energy, Water Supply Management, Transportation Systems, Waste Management, Law Enforcement, Information Systems, and other community services.
- *Smart Homes* – IoT facilitates connections of all household appliances such as refrigerators, AC, lights, door-locks, cookers, heaters, TV, dryers, washing machines, etc.
- *Security* – IoT improves security by avoiding crimes and dangerous activities in public places such as banks, airports, and government offices and is used to control and monitor your data at smart home from your server machines using Web of Things (WoT).

2.4 Challenges of IoT

Though there are several advantages of IoT, there are certain disadvantages too, and this includes [9] [10] [11]:

- *Security* – IoT technology connects devices over a network; therefore, the system should offer authentication control on security threats and be able to reconfigure by itself after threats.
- *IoT Standards* – IoT is growing at a rapid speed. International standards have become inevitable, so far, there is no international compatibility standard for Internet of Things appliances. Each manufacturer has his/her standards, so now become a challenge which measures should be used.
- *Electricity* – IoT devices need a continuous power supply, challenging to maintain due to electricity problems, especially in developing countries.
- *Complexity* – The IoT system's architecture is also very challenging; its design, implementation and maintenance are not very simple; it needs the expertise to deal with it.
- *The complexity of software* – Software plays a significant role in IoT to facilitate organizations of the whole IoT activities; they can become exceedingly complicated, leading to a malfunction.
- *Privacy* – IoT reveals user's x confidential information without their knowledge, hence, causes many problems with their privacy.
- *Storage* – IoT generates a massive amount of data, integration with a big data frame like Hadoop. Spark becomes very necessary and helpful in analysing and extracting potential information using machine learning algorithms.

3. SMART HOMES

Smart Homes play a significant role in recognising the ADL of humans, which leads to a discovery of health issues, security issues, electricity and water usage, etc., hence, quality life.

3.1 The concept of Smart Home

In general, a smart home refers to a set of devices, equipment, middleware system and other technologies that connect to a shared network and can be controlled remotely. For example, the smart homes can connect all home appliances such as lights, security cameras, door-locks, heaters, TVs, kitchen appliances such as refrigerators, coffee machines, cookers, and more are all connected into one network ad of which can be controlled even remotely by using laptops, Smartphones through different Smart Home - IoT apps [12].

3.2 Applications of Smart Homes

Smart Home has several applications of which includes; Healthcare, Security, Energy and Water usage, and so on [13] [14] [15].

- *Health Application* – Smart Home with the help of smart IoT devices such as sensors can help to collect information from residents related to their health status, which can be used to predict diseases at early stages, diseases such as Parkinson's disease (PD) can be detected through body movements; Heart attack, blood pressure, which can be identified through disorder sleeping of the residents at smart homes.
- *Security Application* – Through smart IoT devices such as security cameras, data collected can be used to

identify, avoid crime and dangerous activity from occurring at home.

- *Energy Saving Application* – Smart Home helps to control and monitor power consumptions that are taking place at home. Identify and forecast the energy flexibility of the houses in real-time. Energy flexibility is about modifying a household's electricity consumption while minimising the impact on occupants and operations. Smart thermostats may control, report energy usage and alert users, among other items, to adjust filters.
- *Water Management Application* – The smart home control and monitors water usage at home to ensure that water is used more efficiently.
- *Automation* – with the help of Smart Home, we can automate everything we need to automate in the household appliances and make home a better place to live, the restriction is where our thoughts end; whatever we want to automate to make life better and more meaningful.

3.3 The Architecture of Smart Home

Smart Home is built under IoT as a building block technology consisting of three layers; physical, network, and application layers [16].

- *Physical layer* – This consists of Sensors and actuators, and it is responsible for data collection from all home appliances. The physical layer collects data using sensors, and all collected data are sent to the network layer for the other process using Zigbee and Z-Wave protocols.
- *Network layer* – This layer is responsible for combining and converting the collected data from analogue to digital using a data acquisition system (DAS) and then sends to the upper layer – the application layer.
- *The application* layer is responsible for delivering information to the end-user through different applications for different purposes.

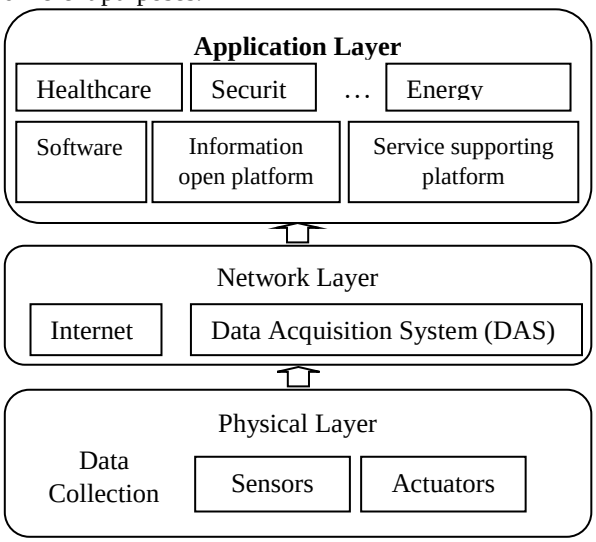

Fig.2 Smart Home Architecture

3.4 Challenges of Smart Homes

Even though Smart Home is beneficial in many fields such as health, security, energy and water control at home, there are specific challenges the Smart Home encounter [17] [18] [19].

- *Security Cameras* – In Smart Home, residents may track their homes when they are away and can be able to notify between visitors who were trying to disturb their home.
- *Privacy* – Smart devices around the home know every about the householder, such as security cameras, smart light bulbs, and so on, about homeowners' behaviours. In case if this information ends up to hackers, it may cause many problems to the householders. Privacy becomes at risk; hence the need for protection remains necessary.
- *Compatibility* – There are too many home automation control apps, householders get difficulty controlling their home technologies due to the number of different apps installed without a central control point.
- *High Cost* – Smart home devices and technologies are still expensive for the majority to afford; the rest of the industry is searching for more cost-effective products.
- *Device Control* - It is hard to control due to many connections of devices and technologies. It requires many apps to maintain them; hence, knowledge is needed to prevent different apps installed at home to control the connected devices.

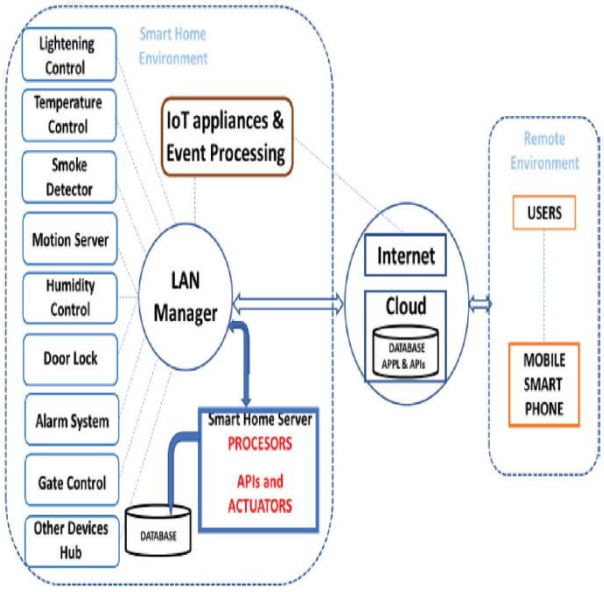

Fig.3 Integrating Smart Home, IoT and Cloud computing [20].

4. RELATED WORKS

Park et al.[21] described the security threats to IoT that could cause information leakage in smart homes. Furthermore, given their close relation with human life, these smart home-based IoT devices are a problem because of social damage. The researcher suggested quantifying the danger that IoT devices will present in smart homes based on security scenarios to resolve this.

Dragos et al. [22] offered a review of various IoT based smart home technologies, the author highlighted several challenges that IoT based Smart Homes face this includes the big amount of data generated which requires a process, analysis and storage. Security and privacy are also crucial considerations for the effective deployment of smart homes technologies as well as the computer developers for the implementation of intelligent IoT devices, management and analysis of the data.
Moniruzzaman et al. [23] discussed about the challenges of security, transparency, and privacy for users of data in smart homes. Smart homes are vulnerable to attacks from hackers who want to steal data for their own gain. Hence, the results show that, security and privacy are becoming increasingly vital in smart homes.
Zaidan et al. [24] recommended most challenges related to the use of Internet devices in smart homes are linked to security, energy usage, safety, and control. In order to have emerged smart home these challenges should be addressed.
Tao et al. [25] report that smart home technologies are improving people's lives; however, several challenges hinder this enjoyment; such challenges include scalability, security, lack of global standards, and privacy. Due to the intricacy of these issues, collaboration among various stakeholders is required to address them.
Augusto-Gonzalez et al. [26] demonstrated how to address the security issues in the smart home. The author suggested integrating multiple layers in the smart home architecture to be applied to deal with threats posed by various types of attacks.
Hall et al. [27] Hall examined the challenges that smart homes face and recommended best practices for minimizing those problems. The author(s) reported that the major challenges in smart homes are cyber-security and privacy, data are collected and controlled by the third parties without user knowledge, and hence, user does not have control to his/her data which is very risk. Therefore it was suggested by the author(s) that these challenges must be addressed in order to provide optimal security and privacy.
Ammar et al. [28] surveyed different IoT security frameworks, observed that they are different methodologies applied to these frameworks. It was discovered that the major concern in the frameworks despite of their different methodologies in setting their security framework ware privacy and security.
Yao et al. [29] investigated smart house privacy attitudes and design concepts, discovering that smart home design help inhabitants maintain their privacy. As a result, involving stakeholders and balancing future smart house design will aid in privacy control in smart homes.
Gebremichael et al. [30] discussed the privacy and security in IIOT how still difficult to manage as a result the end user's information are at risk, this enforcement more security measure to be take to make sure integrity and confidentiality of the end user's information are safe.
Wan, et al. [31] introduced IoTArgos system that captures, examines, and classifies the data communications through routers in order to monitor security at home. The system deploys both supervised and unsupervised techniques to detect abnormal behavior at smart home with a precision of 98.76% and recall of 97.63%.

5. RESULTS AND DISCUSSION

Through various technologies and other embedded software, IoT has enabled homes to become smart homes, which has improved residents' healthcare, security, automation, energy, and water usage. Smart homes generate massive vital data that comes in different formats and types. Machine learning and other technologies are applied to make predictions to examine human activities performed at homes; as a result, the findings are used to develop different apps for managing homes, like security apps, healthcare apps, etc, hence quality life. Regardless of the various applications available in the smart home environment via smart IoT devices, both IoT and Smart Homes have substantial difficulties that must be addressed to make a better place to live. This study has discovered that the majority of reviewed papers from the previous studies still confesses that security and privacy are still major challenges face both IoT and smart homes. The user's information is at risk; the third parties can breach and have access to the user's information without their knowledge. There is no one standard for the manufacturers of different smart IoT devices and the stakeholders are not involved in the process. Handling massive data generated in the smart homes is a challenge and still there are few technical knowhow to cater for these data. High cost of the devices as well as to run the system, complexity of software some software are not user friendly, compatibility and device control-knowledge of how to control these devices at home is required. Table 1 below shows the various previous studies' the alarming challenges and applications in both IoT and smart homes.

Table 1: Challenges and Applications for both IoT and Smart Homes

No:	Challenges (IoT and SH)	Applications (IoT and SH)
1	Security and privacy	Healthcare
2	Standards	Security
3	Complexity of software	Energy Usage
4	Storage	Water Management
5	Compatibility	Automation
6	High Cost	Agriculture
7	Device Control	Disaster Management

6. Conclusion and Future Direction

IoT is essential as the building block technology used for developing Smart Homes. This paper focused on the concepts of IoT and Smart Homes, the architecture of loT and architecture of Smart Homes, IoT, and Smart Home applications, and the challenges found for both IoT and Smart Homes. There is excellent work done in the discovery of new technologies for IoT and Smart Homes. The IoT and Smart Homes discoveries have led to remarkable progress in various

fields such as security, health, agriculture, energy, water management, etc. Despite the remarkable progress, both IoT and Smart Homes encounter security and privacy challenges that need to be addressed. These challenges impact human life and the sustainability of development; as for now, we almost depend on IoT and Smart Homes technology for each and everything we do. There is a great need for different manufacturers and alliances to harmonize intelligent IoT devices to solve the existing problems in a future direction. Hence, this will increase customers' confidence in the security and privacy of their Smart Home data.

REFERENCES

[1] Babar, M., Arif, F., & Irfan, M. (2019). Internet of things–based smart city environments using big data analytics: A survey. In Recent Trends and Advances in Wireless and IoT-enabled Networks (pp. 129-138). Springer, Cham.

[2] Subbarao, V., Srinivas, K., & Pavithr, R. S. (2019, April). A survey on internet of things based smart, digital green and intelligent campus. In 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU) (pp. 1-6). IEEE.

[3] Gomez, C., Chessa, S., Fleury, A., Roussos, G., & Preuveneers, D. (2019). Internet of Things for enabling smart environments: A technology-centric perspective. Journal of Ambient Intelligence and Smart Environments, 11(1), 23-43.

[4] Madakam, S., Lake, V., Lake, V., & Lake, V. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(05), 164.

[5] Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. Information Systems Frontiers, 17(2), 243-259.

[6] Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). Deep learning for IoT big data and streaming analytics: A survey. IEEE Communications Surveys & Tutorials, 20(4), 2923-2960.

[7] Siow, E., Tiropanis, T., & Hall, W. (2018). Analytics for the internet of things: A survey. ACM computing surveys (CSUR), 51(4), 1-36.

[8] M. P. Kumar, S. P. Santhoshkumar, T. Gowdhaman, & S. S. Shajahaan. A survey on IoT performances in big data. *International Journal of Computer Science and Mobile Computing (IJCSMC)*, *6*(10), 26-34, 2017.

[9] Kumar, J. S., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. International Journal of Computer Applications, 90(11).

[10] Baños-Gonzalez, V., Afaqui, M. S., Lopez-Aguilera, E., & Garcia-Villegas, E. (2016). IEEE 802.11 ah: A technology to face the IoT challenge. Sensors, 16(11), IEEE, 2016.

[11] Stojkoska, B. L. R., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. Journal of Cleaner Production, 140, 1454-1464.

[12] Gram-Hanssen, K., & Darby, S. J. (2018). "Home is where the smart is"? Evaluating smart home research and approaches against the concept of home. Energy Research & Social Science, 37, 94-101.

[13] Pujaria, U., Patil, P., Bahadure, P., & Asnodkar, M. (2020). Internet of Things based Integrated Smart Home Automation System. Available at SSRN 3645458.

[14] Daissaoui, A., Boulmakoul, A., Karim, L., & Lbath, A. (2020). IoT and big data analytics for smart buildings: a survey. Procedia Computer Science, 170, 161-168.

[15] Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. Journal of Network and Computer Applications, 97, 48-65.

[16] Gaikwad, P. P., Gabhane, J. P., & Golait, S. S. (2015, April). A survey based on Smart Homes system using Internet-of-Things. In 2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC) (pp. 0330-0335). IEEE.

[17] Mani, A. R, L. charan, Bhuvaneswaran and Hassain , S.E (2018). A survey on IoT based systems for smart home automation and theft control, IJMTER.

[18] Wilson, C., Hargreaves, T., & Hauxwell-Baldwin, R. (2015). Smart homes and their users: a systematic analysis and key challenges. Personal and Ubiquitous Computing, 19(2), 463-476.

[19] Ghayvat, H., Liu, J., Babu, A., Alahi, E. E., Gui, X., & Mukhopadhyay, S. C. (2015). Internet of Things for smart homes and buildings: Opportunities and Challenges. Journal of Telecommunications and the Digital Economy, 3(4), 33-47.

[20] Domb, M. (2019). Smart home systems based on internet of things. In Internet of Things (IoT) for Automated and Smart Applications. IntechOpen.

[21] Park, M., Oh, H., & Lee, K. (2019). Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective. Sensors, 19(9), 2148.

[22] Mocrii, D., Chen, Y., & Musilek, P. (2018). IoT-based smart homes: A review of system architecture, software, communications, privacy and security. Internet of Things, 1, 81-98.

[23] Moniruzzaman, M., Khezr, S., Yassine, A., & Benlamri, R. (2020). Blockchain for smart homes: Review of current trends and research challenges. Computers & Electrical Engineering, 83, 106585.

[24] Zaidan, A. A., Zaidan, B. B., Qahtan, M. Y., Albahri, O. S., Albahri, A. S., Alaa, M., ... & Lim, C. K. (2018). A survey on communication components for IoT-based technologies in smart homes. Telecommunication Systems, 69(1), 1-25. [25] Tao, M., Zuo, J., Liu, Z., Castiglione, A., & Palmieri, F. (2018). Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. Future Generation Computer Systems, 78, 1040-1051.

[26] Augusto-Gonzalez, J., Collen, A., Evangelatos, S., Anagnostopoulos, M., Spathoulas, G., Giannoutakis, K. M., ... & Nijdam, N. A. (2019, September). From internet of threats to internet of things: A cyber security architecture for smart homes. In 2019 IEEE 24th International Workshop on

Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) (pp. 1-6). IEEE.
[27] Hall, F., Maglaras, L., Aivaliotis, T., Xagoraris, L., & Kantzavelou, I. (2020). Smart Homes: Security Challenges and Privacy Concerns. arXiv preprint arXiv:2010.15394.
[28] Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8-27.
[29] Yao, Y., Basdeo, J. R., Mcdonough, O. R., & Wang, Y. (2019). Privacy perceptions and designs of bystanders in smart homes. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-24.
[30] Gebremichael, T., Ledwaba, L. P., Eldefrawy, M. H., Hancke, G. P., Pereira, N., Gidlund, M., & Akerberg, J. (2020). Security and privacy in the industrial internet of things: Current standards and future challenges. IEEE Access, 8, 152351-152366. [31] Wan, Y., Xu, K., Xue, G., & Wang, F. (2020, July). Iotargos: A multi-layer security monitoring system for internet-of-things in smart homes. In IEEE INFOCOM 2020-IEEE Conference on Computer Communications (pp. 874-883). IEEE.