ISSN 2347 - 3983
Volume 9. No. 5, May 2021
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter10952021.pdf
https://doi.org/10.30534/ijeter/2021/10952021

Proposing a Novel IoT Framework by Identifying Security and Privacy Issues in Fog Cloud Services Network

Fida Hussain Khoso[1], Aijaz Ahmed Arain[2], Abdullah Lakhan[3], Asadullah Kehar[4], Shah Zaman Nizamani[5]

[1]Dept. of Basic Science, Dawood University of Engineering & Technology Karachi, Sindh, Pakistan, fidahussain.khoso@duet.edu.pk.

[2]Department of Computer Science, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Pakistan aijaz@quest.edu.pk

[3]Benazir Bhutto Shaheed University Lyari, Karachi, Pakistan abdullahrazalakhan@gmail.com

[4]Department of Computer Science Shah Abdul Latif University Khairpur asad.kehar@salu.edu.pk

[5]Department of Information Technology Quaid-e-Awam University of Engineering, Science and Technology Nawabshah, Pakistan shahzaman@quest.edu.pk

ABSTRACT

These days, the Internet of Things applications are growing progressively. However, the existing frameworks for IoT applications are not satisfied the security, allocation, and provisioning requirements. We propose a novel secure IoT application framework. Fog cloud execution model is serverless computing which is run by the server in cloud provider and the allocation of machine resources is dynamically managed. The application which consumes the actual amount of resources, the pricing is based upon that rather on pre-purchase units of capacity. The proposed framework consists of different methods, such as secure mobility, resource allocation, provisioning, and prediction under blockchain technologies.

Key words: Internet of Things (IoT); Security Issues; Privacy Issues, Fog Cloud Services

1. INTRODUCTION

The use of the Internet of Things (IoT) applications in Malaysia is growing increasingly recently [1]. The features are E-Healthcare, E-Business, E-Transport, E-Home, etc. as depicted in Figure 1. These application widely used in different regions such as china, Malaysia, Indian [2]. The faster than expected development of 5G provides the best way for IoT (Internet of Things) that run on potentially device on electronic system with conceivable form.

We have come to know that the Malaysian information and communication technology has commented that 5G advancement has remarkable boosted (IoT) applications and

reality for the internet gives the edge in IoT technology which runs on conceivable based on devices which technology oriented smart devices. Malaysian Communications & Information Technology, a government institute of research, said that 5G's progression has significantly boosted Internet of Things applications and made the "Internet of All" a reality. According to the Malaysian Economic Information Service, a combination of fastest technology that it depends on focused the countries for IoT industries for value of 1.2 trillion $168 billion, service for industry revenue rose 72.8% from 2020. IoT is driven mainly by favorable administration strategies & intense market race within

Fig. 1. IoT Applications in Malaysia

Forrester, world most significantly manufacturing technical leader, economic consultancy & business approaches. From 2022, IoT is estimated cost to expend $300 billion for annually on IoT pass United States [3]. We can see from Figure 2, the ratio of IoT applications growing and replacing all non-IoT applications year by year.

Speaking of authenticity in the terms of the non-professional, you do not want your smart door to be open to everyone; you just want your door to know you are. On the other hand, it must be ensured that the data is consistent and always accurate. When it comes to industrial appliances, there is

every reason to worry about data security. Hackers and competitors can intercept and manipulate the data for their interests to any length. As a result, the data must be transmitted and stored in such a way as to remain the way it is.The lack of framework with in some of companies is presented by the internet of things and that is one of the big issues.

Although traditionally frameworks are not secure that offers services to the IoT applications. The value of big data is acknowledged rapidly as another problem and IoT provides many new users data which cannot be got by the traditional devices.

Two problems discover:

1. IoT is insecure and provides many new ways of manipulating home networks.

2. IoT is used to send vast amounts of data to their suppliers, which consumers should not share.

The proposed study aims to evaluate these devices' communication and figure out how to create an appliance that limits contact to only what the consumer finds reasonable. This appliance would be a proof of concept for the final product.

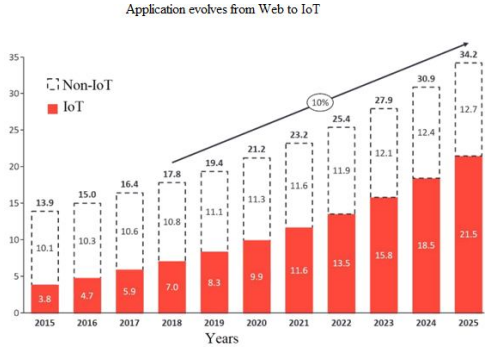

Fig. 2. IoT Growing in Malaysia

2. Related Work

Existing frameworks, for instance Ifogsim [1], edge clouds [2] and edge foundry [3] targets to carry each object (Smart Cameras, Sensors for Environmental, wearable, home appliances & vehicles) online, hereafter producing enormous capacity of data that can overcome storage systems and applications for data analytics. However, these frameworks only support no-secure and static environments. Whereas, secure dynamic and adaptive environment for IoT applications remain a challenge.

These frameworks [4-6] develop a protection scheme that authenticate IoT devices without their identity being exposed. The research emphases on safety and preventing the entry of malicious IoT devices into the network. The relevance is due to fact that a process is presented by which IoT devices can validate themselves with a certificate while preserving anonymity, which thus presents a possible way of ensuring that only valid IoT devices owned by a user can connect to the network.

These works [7-9] categorizes the dissimilar kinds of connectivity for IoT & list the present challenges concerning those types of connectivity. The IoT connectivity includes the definition of different types so that their challenges make this paper important which tries to identify and categorize the different IoT devices and it is the first step in our work.

The research works [10-13] discuss various aspects of security in context of sensor data, features, and security architecture. To categorize and identify problems make this paper useful and definitions are given. The conceivable problems might have an influence on the product or presented solutions and should, therefore, be taken into account.

These studies [14-16] provide an outlook for possible future implementation of IoT devices and their features. The paper is important because the authors mention issues that may occur or have not yet been addressed which can be evaluated together with the future outlook.

The studies [17-19] is emphasis on present and long-term problems concerning confidentiality. Research explores, ever-deepening diffusion of technology into social life anywhere it seeks to identify promising new privacy issues and security laps. The effectiveness and usage is to determine what effect our findings could have, primarily in the ethical aspect.

The works [18-21] provide a list of IoT product categories and relates privacy & security issues to those classes. Value is an advance thorough investigation into various security concerns for IoT devices. The safety concerns have to be addressed in the findings regarding our research proposal.

3. Research Gap

IoT devices are vulnerable to security attacks because of their increase in number and the way the devices are having network communication with each other. Current conventional IoT devices connected over traditional networks are viably insure to security threats that demands a massive need to propose a new secure IoT device that could glimpse a secure query control mechanism.

1. This study proposes a novel secure IoT framework in the Fog Cloud network. The framework consists of different layers. For instance, Business, Application, Service, and Resource Layers. How can a secure framework be designed to leverage the real-life use at home environment of IoT devices in daily use.

2. How can a new framework be designed to tackle the privacy concern of IoT devices in a home environment?

3. How can a secure framework be designed to leverage the real-world use of IoT devices in a home environment

4. How can a new framework be designed to tackle the privacy concern of IoT devices in a home environment?

The conventional IoT frameworks providing communication support to IoT devices over traditional networks are viably insure to security threats while a new secure IoT framework can provide a more secure query control mechanism.

4. RESEARCH OBJECTIVES

First of all, to investigate the security and privacy issues in current IoT devices in home environment. Then a new framework will be designed and developed catering the security and privacy challenges of Fog and Cloud network. In the last, the performance of new proposed framework will be evaluated.

5. RESEARCH METHODOLOGY

For the IoT applications, secure services in the network are the fundamental requirements these days. Blockchain technology is one of the possible ways. The list of records with blocks that are linked using cryptography originally called blockchain. Individually block comprises a cryptographic hash of the former block, a time stamp, and transaction data. By design, a blockchain is resistant to amendment of the data. However, existing blockchain technologies did not consider scheduling and resource allocation under security constraints. We propose a novel security-aware framework with blockchain technology determining distribution, provisioning, and security mechanism to run the IoT applications.

6. PROPOSED FRAMEWORK

To deal with the security issue problem for the IoT applications, we propose a novel framework, as shown in Figure 3. The proposed framework consists of four layers.

Business layer offers interface level services to run the IoT applications. For instance, runtime, communication protocols, and interpretability. The application Layer provides solutions to different enterprises based on their requirements. Service Layer is significant, which offers various libraries, runtime environment, and platform to run any application with different binaries and protocols. Resource Layer is a heterogeneous resource provisioning and resource offering phase, where users can buy or rent various services with different pricing models. Business layer supports any workload of IoT applications. For instance, real-time, discrete, and continuous. However, the existing frameworks only supported on type at a time. Moreover, the data-intensive and compute-intensive workload of applications simultaneously handles in the system. Many organizations exploit different services to run their operations. Therefore, they require a decentralized security system instead of single entity management.

We provide different decentralized choices to the firms either they want to use private services or public services via the Application layer. Our proposed system will offer an open-source service development platform to write independent services with different languages. The proposed method provides trusted cheap services based on the serverless standard as compared to the existing monolithic platform.

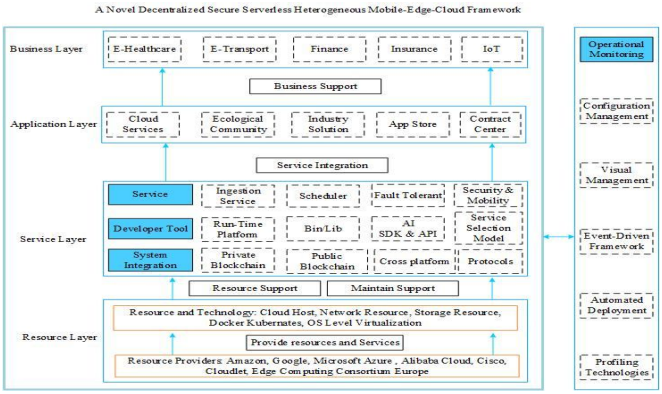

Fig. 3 A novel Secure Aware IoT Fog Cloud Framework.

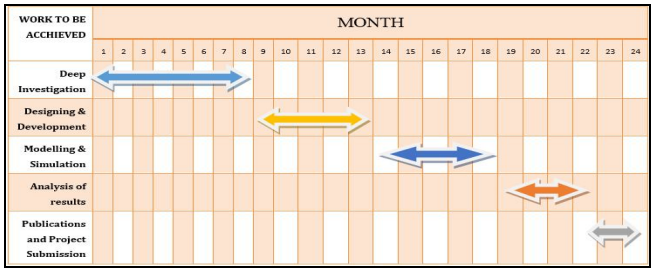

Fig. 4 Flowchart of Activities

7. RESEARCH ACTIVITIES AND MILESTONES WITH DATES

This research will try to answer the research questions related to the security and privacy issues of current conventional IoT devices and propose a new secure device that could cater the privacy concerns of users.

In this phase, we will perform deep investigation of problem by investigating IoT devices integrated with servers (e.g., fog, and edge). Since the servers are connected via a software defined network (SDN) so they are communicating with different switches and control by the SDN controller. The Applications E-Transport, E-Healthcare, E-Commerce are integrated with IoT devices and connected to the SDN controller. Whereas, IoT servers offer different cloud services to the run applications as mentioned earlier. However, sensitive data of apps to run on the untrusted IoT servers is a challenging question. We will try to investigate aspects of devices, servers and their services in context of security and privacy.

After having an exhaustive review of related devices, we will design the new framework investigating the following techniques,

1. **Machine Learning:** It is the best technique that makes sense of any organization's security threats and lets the workers concentrate on more important, strategic tasks. Machine learning is known at its simplest level "ability (for computers) to study without the explicit programming. "Using mathematical techniques through large datasets,

algorithms of machine learning construct behavioral models and use these models as a basis for making future predictions based on new input data. Machine learning will, in theory, help-companies identify threats better and react to attacks and security incidents. It could also allow more menial tasks traditionally performed by exhausted and sometimes under-skilled security teams to be automated. Machine learning is subsequently a fast-growing trend in security.

2. Deep Reinforcement Learning: The number of networks is connected with internet has enlarged significantly & systems are more than ever vulnerable to cyber-attacks. Cyber-attack difficulty and dynamics need devices to be adaptive, responsive, & broad-scale to protect. Machine learning, or more specifically deep reinforcement learning (DRL), approaches to address these issues have been widely proposed. DRL is very skilful of solving complex, dynamic, and especially high-dimensional cyber-defense problems by integrating deep learning into conventional RL. We address various dynamic features, containing DRL based cyber-physical system methods for security purpose, autonomous detection for intrusion techniques, & multi agent DRL based on simulations game theory for cyber-attack defense approaches. There is also widespread communication, discussion, and recommendations for forthcoming study on DRL-based cybersecurity. We suppose about the comprehensive appraisal delivers the foundations for facilitates future educations on exploring the potential of developing DRL to cope with increasingly complex cybersecurity problems.

3. **Serverless computing:** Architecture is an execution model for mobile cloud computing in which the server is run by the cloud provider and handles the allocation of computer resources dynamically. Serverless offers isolated security i.e., function as a service (FaaS) with different micro services to the fine grained applications. Moreover, due to open-source runtime, serverless can adopt any security protocol during runtime of the system. The serverless architecture for different IoT applications placement with security QoS will be effective and efficient.

4. **Fully Homomorphic Encryption:** It is a cryptosystem enabling arbitrary cipher text computation is known as Fully Homomorphic Encryption (FHE). Such a scheme allows creating programs for any desired features, which can be performed on encrypted inputs to generate result encryption. FHE is an open protocol for security, it will be very effective in a secure distributed system for IoT applications.

5. **The blockchain technology:** It supports many aspects of the IoT applications, such as mobility, interactivity, vehicular type services and so on. Blockchain technology is the state of art new technology for organize the data with various blocks.

8. EXPERIMENTAL RESULTS

This study tested the proposed schemes on different applications in order minimize end to end delay of applications. Figure 5 shows that the proposed hybrid blockchain outperform all existing security mechanism in both global and local industrialization.

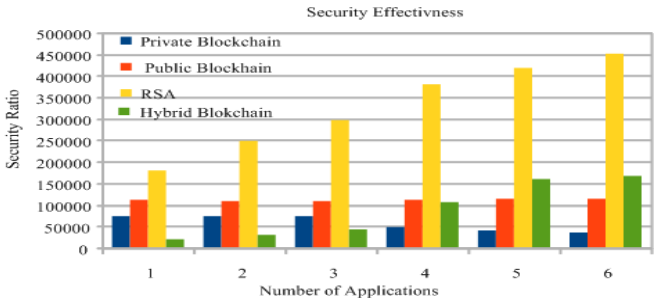

Fig. 5 Proposed Hybrid Blockchain

9. CONCLUSION

These days, the Internet of Things applications are growing progressively. However, the existing frameworks for IoT applications are not satisfied the security, allocation, and provisioning requirements. We propose a novel secure IoT application framework Fog cloud execution model is serverless computing which is run by the server in cloud provider and the allocation of machine resources is dynamically managed. The rates for cloud computing are based on the real amount of resources spent by an application, rather than on pre-purchased units of capacity. The proposed framework consists of different methods, such as secure mobility, resource allocation, provisioning, and prediction under blockchain technologies.

REFERENCES

[1] Gupta, Harshit, Amir Vahid Dastjerdi, Soumya K. Ghosh, and Rajkumar Buyya. "iFogSim: **A toolkit for modeling and simulation of resource management techniques in the Internet of Things,** Edge and Fog computingenvironments." Software: Practice and Experience 47, no. 9 (2017): 1275-1296.

[2] Sonmez, C., Ozgovde, A. and Ersoy, C., 2018. Edgecloudsim: **An environment for performance evaluation of edge computing systems. Transactions on Emerging Telecommunications Technologies**, 29(11), p.e3493.

[3] Kwon, Do-Hyung, Hyun-Kyo Lim, Youn-Hee Han, Min-suk Kim, and Yong-Geun Hong. "**Implementation of IoT control system based on EdgeX Foundry**." In Proceedings of the Korea Information Processing Society Conference, pp. 995-997. Korea Information Processing Society, 2018.

[4] KuoChun Chen, Sheng-Tung Hsu, Jia-Sian Jhang, and Chun-Shuo Lin. **Internet of things security appliance**, 2019.

[5] Vasaki Ponnusamy, Yen Pei Tay, Lam Hong Lee, Tang Jung Low, and Cheah Wai Zhao. **The usage of internet of things: Survey.** In Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications, pages 956{976. IGI Global Kuala Lumpur, Malaysia, 2020.

[6] Ibrar Yaqoob, Ibrahim Abaker Targio Hashem, Arif Ahmed, SM Ahsan Kazmi, and Choong Seon Hong. **Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. Future Generation Computer Systems,** 92:265{275, 2019.

[7] Paul C Van Oorschot and Sean W Smith. **The internet of things: Security challenges. IEEE Security & Privacy,** 17(5):7{9, 2019.

[8] Mehiar Dabbagh and Ammar Rayes. **Internet of things security and privacy. In Internet of Things From Hype to Reality**, pages 211{238. Springer, 2019.

[9] Antonio Celesti, Oliver Amft, and Massimo Villari. Guest editorial special section on cloud computing, edge computing, internet of things, and big data analytics applications for healthcare industry 4.0. IEEE Transactions on Industrial Informatics, 15(1):454{456, 2019.

[10] Akashdeep Bhardwaj and Sam Goundar. **A framework to define the relationship between cybersecurity and cloud performance.** Computer Fraud & Security, 2019(2):12{19, 2019.

[11] Xiaofeng Wang. **Application of cloud computing in power security monitoring. Journal of Computational Methods in Sciences and Engineering,** (Preprint):1{7, 2019.

[12] Jixian Lv, Yi Wang, and Jinze Liu. **A security problem in cloud auditing protocols.** In 2019 International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI), pages 43{46. IEEE, 2019.

[13] Rupam Banerjee, Arup Kumar Chattopadhyay, Amitava Nag, and Kaushik Bose. **A nobel cryptosystem for group data sharing in cloud storage.** In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pages 0728{0731. IEEE, 2019.

[14] Esther Daniel, S Durga, and S Seetha. **Panoramic view of cloud storage security attacks: an insight and security approaches**. In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), pages 1029{1034. IEEE, 2019.

[15] Ning Zhang, Dajiang Chen, Feng Ye, Tong-Xing Zheng, and Zhiqing Wei. **Phys-ical layer security for internet of things. Wireless Communications and Mobile Computing,** 2019, 2019.

[16] Subramani Jegadeesan, Maria Azees, Priyan Malarvizhi Kumar, Gunasekaran Manogaran, Naveen Chilamkurti, R Varatharajan, and Ching-Hsien Hsu. **An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications.** Sustainable Cities and Society, 49:101522, 2019.

[17] Rojalina Priyadarshini, Mohit Ranjan Panda, and Brojo Kishore Mishra. **Security in healthcare applications based on fog and cloud computing. Cyber Security in Parallel and Distributed Computing:** Concepts, Techniques, Applications and Case Studies, pages 231{243, 2019.

[18] Kuan-Ching Li, Beniamino Di Martino, Laurence T Yang, and Qingchen Zhang. Smart Data: **State-of-the-art Perspectives in Computing and Applications.** CRC Press, 2019.

[19] Joel Philip and Dhvani Shah. **Implementing the signature recognition system as saas on Microsoft Azure cloud**. In Data Management, Analytics and Innovation, pages 479{488. Springer, 2019.

[20] Hua Huang, Yi-lai Zhang, and Min Zhang. **Research on cloud work of engine supporting three-level isolation and privacy protection.** In 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), pages 160{165. IEEE, 2019

[21] Mamata Rath and Sushruta Mishra. **Advanced-level security in-network and real-time applications using machine learning approaches.** In Machine Learning and Cognitive Science Applications in Cyber Security, pages 84{104. IGI Global, 2019.