mHealth Communication Framework Using Blockchain And IoT Technologies

Tanweer Alam

Abstract— The mHealth is a term that is used for mobile health supported by smart devices such as mobile phones, tablets, and wearable smart devices, etc. The smart devices strengthen the efficiency and effectiveness of interaction with patients, physicians, and specialists. Patients nowadays would like to be intimately involved in their diagnosis as well as to make more informed decisions concerning their care. It has begun to measure the success of the quality of treatment. This was a reason that patients trust mHealth to provide them with consistency in their communications with the physicians. Most wireless strategies do not measure up to this standard so that patient engagement ultimately ended up decreasing. The blockchain can boost mHealth through storing and sharing electronic data securely and transparently. It can enhance the accessibility of patient information in real-time. The Internet of Things (IoT) provides a unique identification number to every connected device such as mobile devices, medical devices, and wearable devices. This framework uses the blockchain and IoT technologies together to provide quick help to the patients, monitor remotely, reduce the cost and unnecessarily hospitalization physically and find the real diagnosis. In order to increase patient involvement, mHealth framework with blockchain and IoT technologies has built with the key objective of providing patients with full information on their treatment and diagnosis.

Index Terms— mHealth, Blockchain, Internet of Things, Smart devices, Communication, Smart Devices, Emerging Technologies.

1 INTRODUCTION

The term mHealth is used to describe the use of mobile devices and several other wireless devices in healthcare [1]. The major advantage of mHealth is its convenience. More specific use of mHealth is the use of smartphones to notify users regarding the services of behavioral healthcare. It also enables patients and physicians to communicate with each other in real-time without having a physical meeting. The blockchain provides secure data communication between the patients and physicians [2]. IoT is known as transformative digital technology that played an important role in the development of next-generation IT initiatives such as smart cities, smart homes, and the smart healthcare system [3]. Just like an essential element of smart health, an interconnected healthcare system consists of such a variety of miniature biosensors that are transported or embedded to the patient. This is used to gather information about the health of a patient as well as provide this information to medical applications using wireless networking. However, due to the widespread evolution of mobile communications, the interconnected healthcare system presents tremendous security challenges. The shared Ledger, of which blockchains are nowadays the best-known instance, can solve one of the key problems concerning the industrial sector: the sharing of patient information while violating its confidentiality. The blockchain could have a significant optimistic effect on healthcare services [4]. The blockchain-based approach was developed in the article [5] to optimize physiological information security and enhance transmitting data performance by using the distributed ledger to secure data records from malicious node tampering attacks[13], [14], [15]. In addition, smart contracts are implemented to allow real-time data analysis to secure private data information[16]. The smart contracts will serve as trusted third parties to help two parties safely exchange ideas. Some findings of this study are as follows:

1. A distributed framework is introduced for interconnected healthcare, including some layers like a physical layer, a shared ledger, a connection, and an application [6]. Figure 1 represents the layered architecture of the proposed framework.
2. Possible privacy and security problems in this new framework are discussed in terms of verification, signing, and identification.
3. Depending on the above study, a blockchain approach is intended to address the issue of physiological information privacy and security.
4. Security efficiency analyses are carried out to verify the efficiency of the desired outcome, accompanied by simulation experiments.

The mHealth system is becoming incredibly popular throughout the world today. Compared to paper works, mHealth have many unavoidable benefits. Throughout the entire healthcare process, several health services can be used. The mHealth has become one of the directions that provide urgent medical help as well as healthcare services could be enhanced. mHealth allows early diagnosis of diseases as well as immediate medical care in emergency situations leading to reduced suffering or medical expenses. Using sensors to monitor and transmit vital signs of the patient is useful to identify patients at risk conditions [6].

Blockchains are one of the newest innovations that may have chosen the world by storm in recent years[17], [18]. The blockchains are nothing but a shared database that keeps records of operations and events moving on across the system [7]. Its most important aspect in a blockchain is that once a bit of information is applied to the shared database, nobody can change [19], [20], [21]. Any data stored on the ledger is fully secure in its essence. Throughout exchange for someone to make the change to a block, it is compulsory to make any changes for all subsequent blocks after that one[22], [23], [24].

- *Tanweer Alam is currently with Department of Computer Science, Faculty of Computer and Information Systems, Islamic University of Madinah, Saudi Arabia. E-mail: tanweer03@iu.edu.sa*

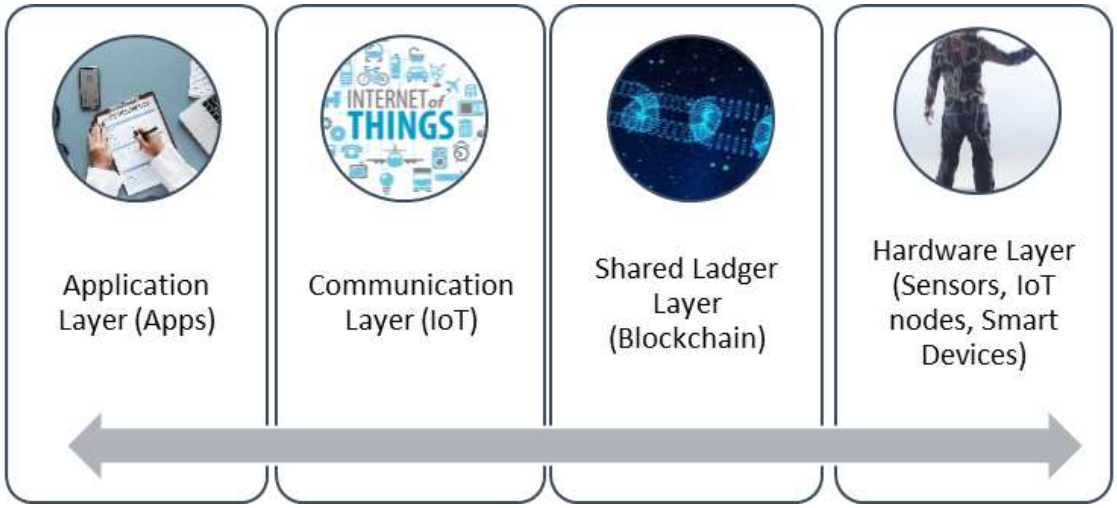

Figure 1: Layered architecture of proposed mHealth System

Internet of Things (IoT) has become a modern as well as an emerging concept [25], [26], [27] that offers internet communication using sensors for smart proof of identity as well as management in such a diverse communication situation. With an independent living viewpoint, this emerging aspect would allow new interaction routes among disabled patients as well as care facilities via revolutionary network security interfaces. mHealth has described as "wireless technology, health instruments and telecommunications innovations towards healthcare". Such a developmental idea offers mobility and always connected usability for public healthcare apps [28], [29].

The information has become a fundamental building block for health care. Computerization of health data has produced great opportunities in terms of data transmission, patient management, and analysis. the health information has been expanding exponentially, with ever more platforms producing information, including within health organizations. Information security is a growing challenge.

Our solution utilizes blockchain technology at the system architectural layer, being distributed by default, acting as a peer-to-peer platform designed to connect the various entities, corresponding to the multiple services or institutions that can store, generate and/or modify mHealth information. Endpoints in the system synchronize with each other by following a set of guidelines:

1. Whenever a device generates a new block, such a block would be transmitted to the network.
2. If a node joins in the network to a new peer, then the current block will be queried.
3. When a device discovers a block with a high indexed than the last identified block, then it either adds the block to its current blockchains or asks another device to get the complete blockchains.

Blockchains could be used to construct a new framework to improve mHealth services security. Blockchains must be used, among several other situations, if there are several participants, further trust is needed, there's a need for consistent monitoring operation, and information needs to have been consistent throughout time duration. The mHealth is undergoing an explosion in information due in part t o the ubiquitous wearables (e.g. exercise trackers), fitness trac king apps (e.g. weight loss monitoring) or environmental supp orted living platforms.

The rest of this article is organized as below. Over the next section, I introduce a distributed data privacy and security framework focused on blockchain. It is accompanied by a description of research issues related to security as well as privacy in interconnected healthcare. Throughout fact, I discuss possible solutions to these problems of privacy and security. Finally, in the last concluded.

2 Related Works

There are presently numerous beginning-ups as well as development projects targeted at introducing Blockchain in healthcare services. Patients are indeed extremely engaged throughout the caring process nowadays. Because everyone now is using a smart device so that the mHealth has bright futures for user growth. At the same moment, however, it is essential to consider that user acceptance can, therefore, increase if the implementations are simple to choose. Persons are likely to give up on an evaluation unless they discover convenience in their use. It makes the situation much more complicated if every patient has specific health needs. mHealth has the potential to transform the health care paradigm for the better. Moreover, it is also important to realize the issues associated with its execution as well as to overcome it. Even though these issues are a big challenge, but these are not impossible.

1) mHealth System in the context of IoT

This paper describes the mHealth system in the scope of the Internet of Things. They described the basic properties of mHealth systems like simplicity, IP interconnection, low power consumption, and securities. The authors address the development of mHealth data through health devices or wearable devices and the implementation of such data to the tracking of various medical issues such as Electrocardiogram, blood pressure, asthma, blood sugar and so on. They address problems connected to confidences, security, and privacy in the context of a secure m-health system. They also provided a list of measures that protect patient information and mHealth data [8].

2) Internet of Medical Things

The Internet of Medical Things refers to the connectivity of connectivity-enabled medical equipment as well as their integration into higher scale health platforms in order to enhance the health of patients. Moreover, due to the general nature of healthcare systems, the Internet of Medical Things even now faces a set of challenges, especially in terms of reliability, security, and privacy. The authors represent an extensive research study of the latest contributions intended to improve the Internet of Medical Things by the use of the latest techniques [9].

3) Blockchain in healthcare and health sciences

The goal of this research would be to critically extract, analyze and evaluate the blockchain to enhance processes and services in healthcare, health sciences, and health research. The results show that digital health records and personal medical records are the most supported areas using blockchain. Permissions, integration, provenance and information integrity are the challenges that are intended to improve through blockchain technology in this field. The research shows that efforts are being made to use blockchain technology in healthcare [10].

4) Examining the Potential of Blockchain Technology to Meet the Needs of 21st-Century Japanese Health Care

The healthcare system of Japan would face increased demand for healthcare services, the acute need for older and deep-term care, shortages of healthcare professionals, and inequalities between access to healthcare in rural and urban regions. Blockchains has the ability to address some of these challenges, but only when a health blockchain is intended, designed, localized and deployed in a fashion that is consistent with Japan's centrally controlled public healthcare. Blockchains must also adapt to challenges and limitations relevant to Japan's healthcare and innovations strategy, along with its regulatory frontier structure [11].

3 mHealth Communication Framework using blockchain and IoT Technologies

Blocks in Blockchain represent securely registered data containing information on user transactions. Each transaction in the blockchain is identified as a string in hexadecimal form (unprocessed transaction form) that is hashed to acquire transaction signatures. The blockchain hash function is created, that is taken into consideration by the successive block, guaranteeing the immutability and accuracy of the database. A node hashing value is collected using Merkle Tree, a paradigm that was invented by Ralph Charles Merkle in 1979 [12].

The hashing in Blockchains has enabled verification of transactions, the verification of the credibility of Blockchains submission is performed by verifying the hash blocks. The users are willing to confirm the credibility of the information that do not need to recalculate all the hashes to authenticate the transaction details and can enquire for Merkle's evidentiary, it consists of the integration of the left and the right hash of the branches and the verification of the outcome towards the family member [12].

Each move is replicated until the source of the Merkle is identified. Through appending the necessary hashes and making comparisons to the root, the patient ensures that the transaction is in location [12].

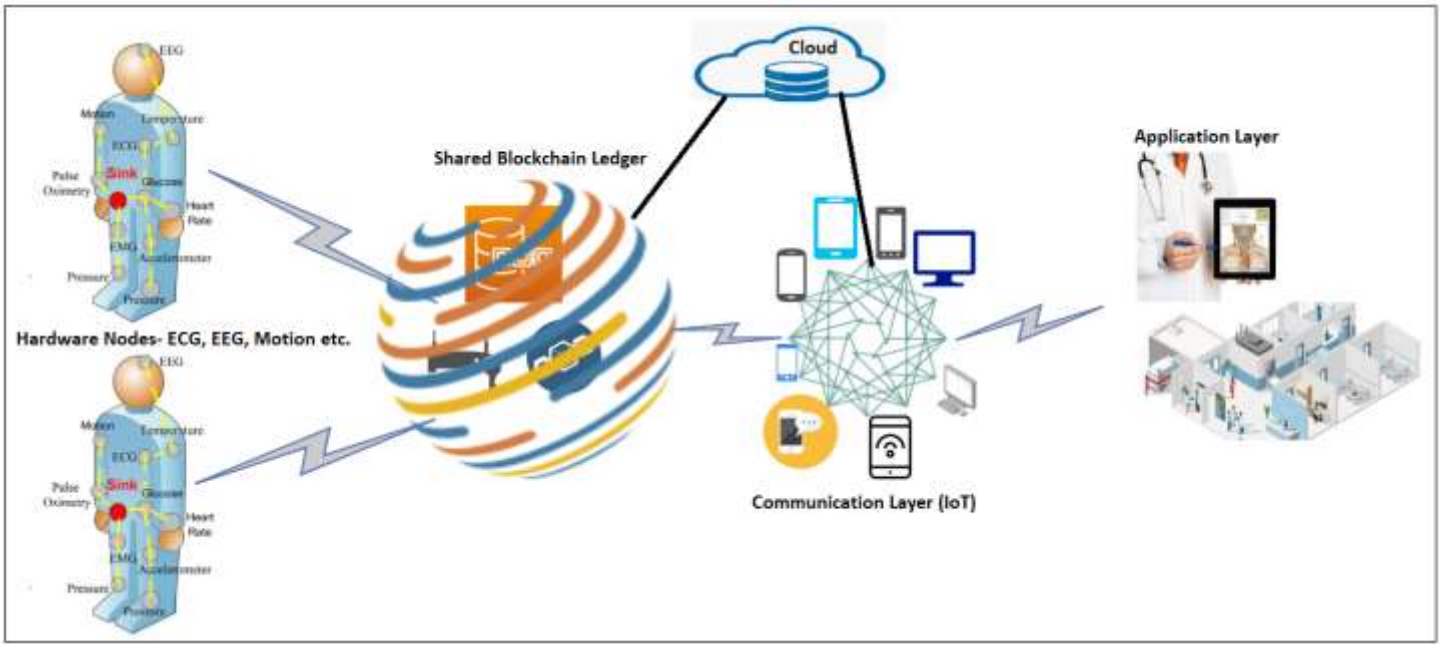

Figure 2: Distributed privacy protection architecture for connected health

Throughout this section, the author is introducing a distributed security infrastructure for interconnected health services. Blockchains play an important role in achieving privacy, transparency, and validity in the proposed system. A conceptual structure is proposed that can be classified into four parts: The Hardware, the shared ledger, the connectivity, and the application. Figure 2 shows the distributed privacy protection architecture for connected health. The hardware consists of sensors and/or mobile devices that gather and transmit information to the top layers. Because sensors gather diagnostic information from patients, the sensor node must have been authenticated before it enters

the model. The endpoint could only be considered relevant whether it has been satisfactorily verified. Sensors and smart devices are gathering information and stored in the shared ledger. Particularly in comparison to centralized approaches that would cause congestion problems at the central point, the shared repository provides better usability and efficiency. The protection of information integrity requires a signature that is built at each detector when the information is exchanged. Smart contracts are widely used to dynamically control and execute the shared signatures mechanism. Throughout the communication services, different communication techniques could be used to encourage the communication of information among devices connected. The information is stored through the transmission to smart devices operated by patients as well as practitioners of health services. Consensus should be established between patients and practitioners of medical services such that functional information could be exchanged with security. The network created with connected devices can, therefore, be designed as a peer-to-peer (P2P) platform [30]. The application layer requires multiple programs/utilities to interact with each other in order to produce collaborative actions. For instance, an application might be configured by a healthcare service professional who requests the sensory data gathered from the patient's devices. Patients should authorize the information when transmitting it to the system, which in practice authenticates the signing to make sure information security. Whether the verification is accurate, a valid diagnostic recommendation will be decided on the basis of the information supplied; that anyway, the data would be rejected. The healthcare system has become an information-intensive environment including massive amounts of data produced, processed and distributed on a regular base. However, patient information is usually segregated in organization-centric patient data, contributing to the inconsistency of effects varying from inefficient continuity of service to lack of critical records throughout emergency cases. The distributed database records every approved transaction and has been repeated between authorized parties. This is a public ledger mechanism–transparency is guaranteed by a distributed ledger containing approved, verified, confidential information exchanges. Exchanges have not been connected to the identification of the stakeholder. The consensus is reached by validating and attempting to enter into transaction processing. Known and trusted stakeholders lead to decrease cost–assistance of several configurable consensuses include proof of work, proof of interest, multi-signature and much more–user information security and privacy is controlled by allowing users power regarding information sharing to service providers and applying user privileges to system services for recognized participants. Blockchains validates the extreme redesign of security, transparency, authentication, and integrity of information. It is a distributed chain of transactions through a peer-to-peer system, the need for a central third-party entity verification authority has been effected. The need for verification and validation access to often sensitive information, medical services, and information exchange should be recognized in order to access the capacity for mHealth. Such a study discusses existing processes and aims to make the argument for Blockchains an enhanced security framework that could reduce the price of trust as well as an option for handling the level of proof. The physical health information gathered through smartphone and mobile innovations may provide vital information to healthcare professionals and medical practitioners, however, these data should be secured in order to make sure the privacy of patients. Its limitations of existing healthcare information systems have motivated experts to create a user-centric, blockchain-based health information exchange framework for mHealth apps to boost the convenience and security of sharing healthcare information. Throughout the proposed blockchain-based system, wearable devices gather health data from the patients, like physical activities, heartbeats, and breathing conditions, etc. Information can then be transferred to a cloud repository stored on a secured platform through a mobile app. The patients can handle all physical health information and are liable for identifying the amount of access to the cloud server for healthcare professionals as well as other intermediaries.

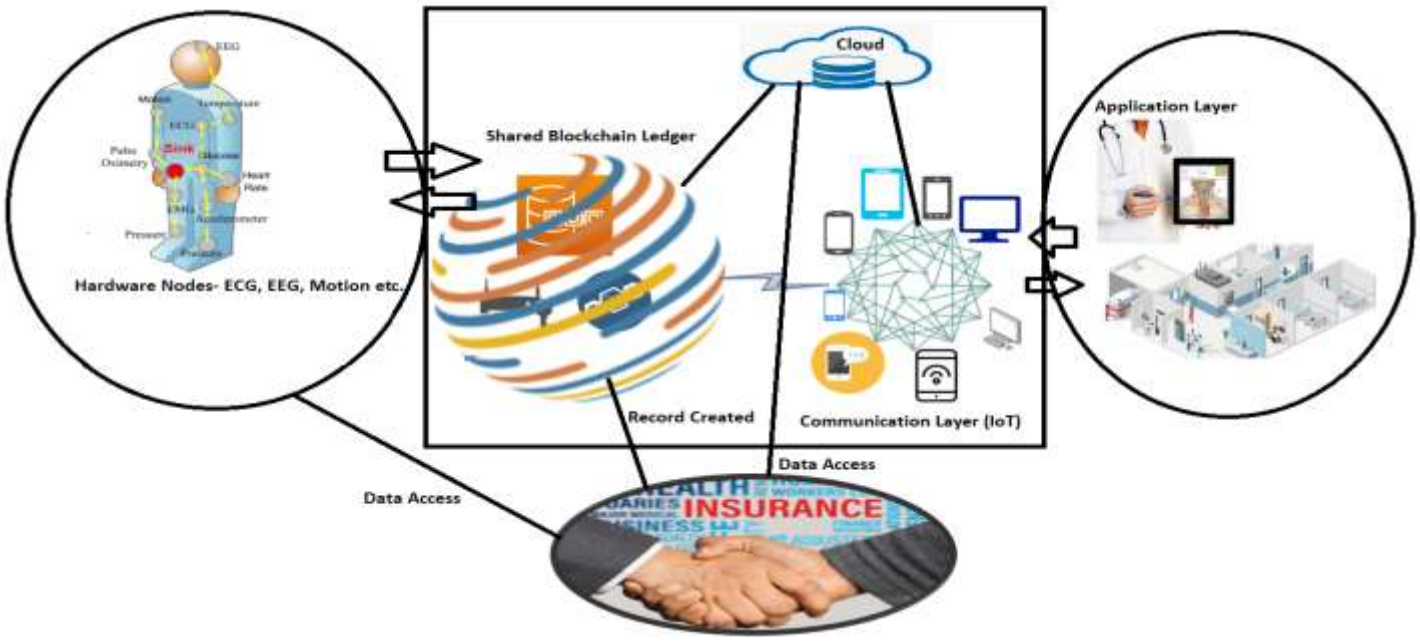

Figure 3: Transmission of health data

mHealth research is just an example of an increasing concentration on blockchains across the health sector. The blockchains can make improvements in the transmission of health data. Further than the collection of personal health information, blockchains will make health records transparent, allowing hospitals and insurance companies will use health records more easily for faster processing of patients and insurance claims. Figure 3 represents the transmission of health data.

Blockchains have a transformational ability for our health structures. However, it provides an opportunity for the development of new business strategies in the healthcare industry. Trustworthy exchanging of health information could contribute not just to activities becoming done differently, as well as to new techniques being performed. Effectively, some of the most significant impacts would be to give patients control over their own health information. Blockchains would potentially allow patients to handle consent and accessing the health information and they see appropriate.

4 Conclusion

The mHealth offers a variety of mobility services and products. Its involvement in remote diagnostics and tracking, patient management, medical informatics, strategic community health, public health data collection, healthcare providers and human resources. A variety of impacts of mHealth solutions vary greatly depends on the industry. The quality of mHealth solutions is depending on the degree of growth and the features of each sector.

REFERENCES

[1] Olla, Phillip, and Caley Shimskey. "mHealth taxonomy: a literature survey of mobile health applications." Health and Technology 4, no. 4 (2015): 299-308. DOI: https://doi.org/10.1007/s12553-014-0093-8

[2] Patel, Vishal. "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus." Health informatics journal (2018): 1460458218769699. DOI: https://doi.org/10.1177/1460458218769699

[3] Alam, Tanweer, Abdulrahman A. Salem, Ahmad O. Alsharif, and Abdulaziz M. Alhejaili. "Smart Home Automation Towards the Development of Smart Cities." APTIKOM Journal on Computer Science and Information Technologies 5, no. 1 (2020). DOI: https://doi.org/10.11591/APTIKOM.J.CSIT.153

[4] Tanweer Alam, "Blockchain and its Role in the Internet of Things (IoT)", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), Volume 5, Issue 1, pp.151-157, 2019. DOI: https://doi.org/10.32628/CSEIT195137

[5] Zhang, Rui, Rui Xue, and Ling Liu. "Security and Privacy on Blockchain." ACM Computing Surveys (CSUR), 2019 Article No.: 51, DOI: https://doi.org/10.1145/3316481

[6] Wang, Ruyan, Hanyong Liu, Honggang Wang, Qing Yang, and Dapeng Wu. "Distributed Security Architecture Based on Blockchain for Connected Health: Architecture, Challenges, and Approaches." IEEE Wireless Communications 26, no. 6 (2019): 30-36. DOI: https://doi.org/10.1109/MWC.001.1900108

[7] Alam, Tanweer. "IoT-Fog: A Communication Framework using Blockchain in the Internet of Things." International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-7, Issue-6, March 2019. Retrieval Number: F2453037619/19©BEIESP, URL: https://www.ijrte.org/wp-content/uploads/papers/v7i6/F2453037619.pdf

[8] Almotiri, Sultan H., Murtaza A. Khan, and Mohammed A. Alghamdi. "Mobile health (m-health) system in the context of IoT." In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp. 39-42. IEEE, 2016. DOI: https://doi.org/10.1109/W-FiCloud.2016.24

[9] Gatouillat, Arthur, Youakim Badr, Bertrand Massot, and Ervin Sejdić. "Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine." IEEE Internet of Things Journal 5, no. 5 (2018): 3810-3822. DOI: https://doi.org/10.1109/JIOT.2018.2849014

[10] Hasselgren, Anton, Katina Kralevska, Danilo Gligoroski, Sindre A. Pedersen, and Arild Faxvaag. "Blockchain in healthcare and health sciences–a scoping review." International Journal of Medical Informatics (2019): 104040. DOI: https://doi.org/10.1016/j.ijmedinf.2019.104040

[11] Mackey, Tim, Hirofumi Bekki, Tokio Matsuzaki, and Hiroshi Mizushima. "Examining the Potential of Blockchain Technology to Meet the Needs of 21st-Century Japanese Health Care: Viewpoint on Use Cases and Policy." Journal of Medical Internet Research 22, no. 1 (2020): e13649. DOI: DOI: https://doi.org/10.2196/13649

[12] Merkle, R. Secrecy, Authentication, and Public Key Systems. Ph.D. Thesis, Stanford University, Stanford, CA, USA, 1979. URL: https://www.merkle.com/papers/Thesis1979.pdf

[13] Alam, Tanweer, and Mohamed Benaida. "Blockchain, Fog and IoT Integrated Framework: Review, Architecture and Evaluation." Technology Reports of Kansai University 62, no. 02 (2020).

[14] Tanweer Alam , Mohamed Benaida . "Blockchain and Internet of Things in Higher Education." Universal Journal of Educational Research 8.5 (2020) 2164 - 2174. doi: 10.13189/ujer.2020.080556.

[15] Tanweer Alam, “Internet of Things: A Secure Cloud-Based MANET Mobility Model”, International Journal of Network Security, Vol. 22(3), 2020.

[16] Tanweer Alam, “A Middleware Framework between Mobility and IoT Using IEEE 802.15.4e Sensor Networks”, Jurnal Online Informatika, Vol 4, No 2 (2019). DOI: https://doi.org/10.15575/join.v4i2.487

[17] Alam, T. Cloud Computing and Its Role in the Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI) 2020, 1, 108-115. DOI: https://doi.org/10.34306/itsdi.v1i2.103

[18] T. Alam "Design a blockchain-based middleware layer in

the Internet of Things Architecture," JOIV : International Journal on Informatics Visualization, vol. 4, no. 1, Feb. 2020. https://doi.org/10.30630/joiv.4.1.334

[19] Tanweer Alam, “Efficient and Secure Data Transmission Approach in Cloud-MANET-IoT integrated Framework”, Journal of Telecommunication, Electronic and Computer Engineering (JTEC), Vol. 12 No. 1, 2020.

[20] Tanweer Alam, Mohamed Benaida, The Role of Cloud-MANET Framework in the Internet of Things (IoT), International Journal of Online Engineering (iJOE), Vol. 14(12), pp. 97-111.

[21] Alam, Tanweer. "Middleware Implementation in Cloud-MANET Mobility Model for Internet of Smart Devices", International Journal of Computer Science and Network Security, 17(5), 2017. Pp. 86-94

[22] Tanweer Alam, Mohamed Benaida, CICS: Cloud–Internet Communication Security Framework for the Internet of Smart Devices, International Journal of Interactive Mobile Technologies (iJIM), 2018 Nov 1;12(6):74-84.

[23] Alam, T, Rababah, B. Convergence of MANET in Communication among Smart Devices in IoT. International Journal of Wireless and Microwave Technologies (IJWMT). Vol.9, No.2, pp. 1-10, 2019.

[24] Alam, Tanweer. (2018) "A reliable framework for communication in internet of smart devices using IEEE 802.15.4." ARPN Journal of Engineering and Applied Sciences 13(10), 3378-3387.

[25] Tanweer Alam, "A Reliable Communication Framework and Its Use in Internet of Things (IoT)", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), Volume 3, Issue 5, pp.450-456, May-June.2018 URL: http://ijsrcseit.com/CSEIT1835111.

[26] Alam, Tanweer, and Mohammed Aljohani. "Design and implementation of an Ad Hoc Network among Android smart devices." In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on, pp. 1322-1327. IEEE, 2015. DOI: https://doi.org/10.1109/ICGCIoT.2015.7380671

[27] Alam, Tanweer, and Mohammed Aljohani. An approach to secure communication in mobile ad-hoc networks of Android devices. International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), pp. 371-375. IEEE, 2015.

[28] Alam, Tanweer, and Mohammed Aljohani. Design a new middleware for communication in ad hoc network of android smart devices. Second International Conference on Information and Communication Technology for Competitive Strategies, p. 38. ACM, 2016.

[29] Alam, Tanweer. "Fuzzy control based mobility framework for evaluating mobility models in MANET of smart devices." ARPN Journal of Engineering and Applied Sciences 12, no. 15 (2017): 4526-4538.

[30] Tanweer Alam, “5G-Enabled Tactile Internet for smart cities: vision, recent developments, and challenges”, JURNAL INFORMATIKA, Vol. 13, No 2, July 2019, pp. 1-10.