OPTIMAL USE OF BLOCKCHAIN IN SMART MEDICAL SERVICES.

Shahbaz Pervez
Computer Science and Engineering Department, Yanbu University College, Royal Commission Yanbu, Kingdom of Saudi Arabia
shahbazchattha@gmail.com
Afraa Sayah Alshammari
Computer Science and Engineering Department, University of Hail, Hail, Kingdom of Saudi Arabia
afra.alshammari@uoh.edu.sa
Sultanah Abdullah Albakri
Computer Science and Engineering Department University of Hail, Hail, Kingdom of Saudi Arabia
s.albakry@uoh.edu.sa
Sarah Alswedani
Computer Science and Engineering Department, University of Hail, Hail, Kingdom of Saudi Arabia
s.alswedani@uoh.edu.sa

ABSTRACT—*In the current era of digitization every commercial company is in the process to move their businesses on the internet thus just not relying on local customers. To support their online transactions with proper security and tracking all transactions. To address conventional security issues, use of blockchain is getting more popularity with every passing day, which is a decentralized transaction and data management technology. Since it provides security, secrecy and data integrity without the involvement of any third party organization to control smooth completion of transactions. With the introduction of smart city services for end-users and need to keep track of all the inventory tractions for every kind of businesses ranging from a retail shop till provision of smart medical services, every step needs to be tracked and documented to ensure its privacy and integrity. In this paper, our objective is to understand the current research topics, challenges and future directions regarding blockchain technology in the context of smart services (e.g. smart medical systems) from the technical perspective while keeping inline security and privacy of end-users. This research is focusing on enlightening and refining limitations of blockchain from privacy and security perspectives including scalability, throughput and latency. On the basis of this study, recommendations on future research directions are also provided for researchers.*

Keywords— IoT; M2M; PPSO; PSO; Security; anonymity; Smart city; Blockchain.

I. INTRODUCTION

Internet of things (IoT) is a unique paradigm that engaged in every smart system development. The main idea of IoT is to communication between sensors, actuators, agents, smartphones, etc. communication means to share information and its analysis. Nowadays, cloud storage is used to store the gathered information between the talking objects. To clarify this concept, let's consider a case study of a patient with wearable sensors that can record any change in the patient health – such as – high blood pressure, heart attack, faintness, blood sugar level, etc. and send the information to a cloud storage, where analytical procedures are built and other data related to the patient such as his record are already saved to conduct the classification and prediction of the patient case and then send the findings to a monitoring doctor that can get alert of the changes in condition of that particular patient. To achieve these IoT enabled services there is a need for new technologies that can define the term 'smart' and level of their 'smartness'. Over time, IoT is expected to have a significant role in every domain of human life, from domestic, industrial, medical, education and so on. IoT devices are in continuous demand. The overall IoT market is expected an annual worth that is over than one billion U.S. dollars since 2017 and onwards [2] and they continuously increasing with every passing day. To understand this you can see the gradual growth of IoT devices usage with a projecting increase from 17.6 billion in 2016 to 26.6 in 2019 and will be 75.44 billion by 2025 [2, 3]. Lately, many types of research and studies in IoT are towards information exchanging between different domains which need symbiotic cloud services [1]. From this point, the role of cloud computing is clear to play a critical role in the success of IoT environments. Many studies in IoT are aiming to solve cloud services problems such as storage and security in an IoT environment. In this paper, the scope is to focus on the security issues and the new approach of using blockchain as a prospered technique to grip these issues in different domains of this field. Blockchain is notorious as the technology behind the application Bitcoins cryptocurrency that was introduced by Satoshi Nakamoto who introduced it to the world in his paper " Bitcoin: A Peer-to-Peer Electronic Cash System" in 2008, as it provides a decentralized platform since it cancelled the need of a third party such as a bank will not be needed in this peer-to-peer system. Blockchain works as distributive ledger using blocks of data, each block contains multiple transactions and each transaction will have the network timestamps on it by hashing them. When a new block is created it will be added to the previously written blocks. Then all blocks and details of all previous transaction are stored in the user disc storage named node. The information held inside of nodes will be used to verify new transaction so new nods will be added to the user chain or will be aborted. This technique is named mining which ensures proof-of-work feature [4, 5, 6].

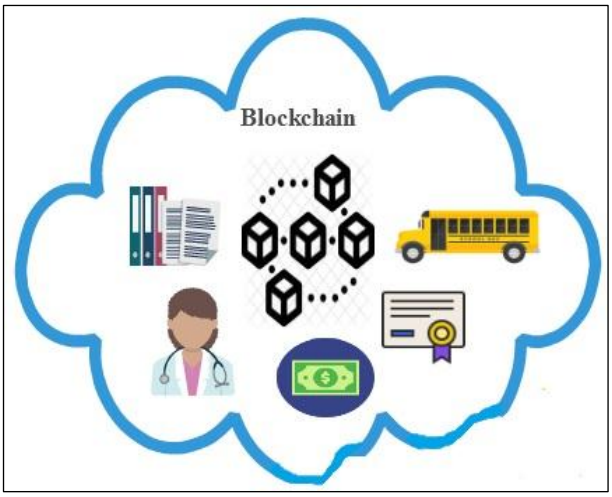

Figure 1: Applications based Blockchain Scenarios

In this paper, we have presented a unique idea to implement security by effectively applying blockchain. Section-1 tell about introduction and background of this technology, Section-2 provide information about current trends for technology, blockchain related work by prominent researchers has been discussed in section-3, and the problems and deficiencies are discussed in section-4. Section-5 presents a proposed approach after comparison with other traditional approaches, finally, the conclusion and future work have been discussed in section-6.

II. BLOCKCHAIN DOMAINS AND ARCHITECTURE

Blockchain consists of a sequence of blocks; each of them has a local copy of a ledger. The blocks belong to various organizations in many systems. The blocks communicate with each other with the aim of getting agreement on the contents of the ledger and a central authority is not required to coordinate and validate transactions. The process of reaching this agreement among nodes in a network is called consensus. Users request a transaction to the blockchain in order to perform the operation the chain is designed to provide. A block for this transaction is created then sent it to every node in the network.

Once a digital transaction is completed, a record of the transaction is added to the cryptographically protected block [30]. After adding a block to the blockchain system, it cannot be deleted or modified. Blockchain technology uses an asymmetric cryptography technique to validate the authentication of digital transactions so the transaction can be accessed and verified by any user in the network [31].

The blockchain networks can be classified into public blockchain and private blockchain. The main difference between public and private blockchain network is that the public blockchain network is fully open-ended and anyone is able to participate in the network without any permission. However, a private blockchain network is a restricted membership that requires an invitation for participation. [30].

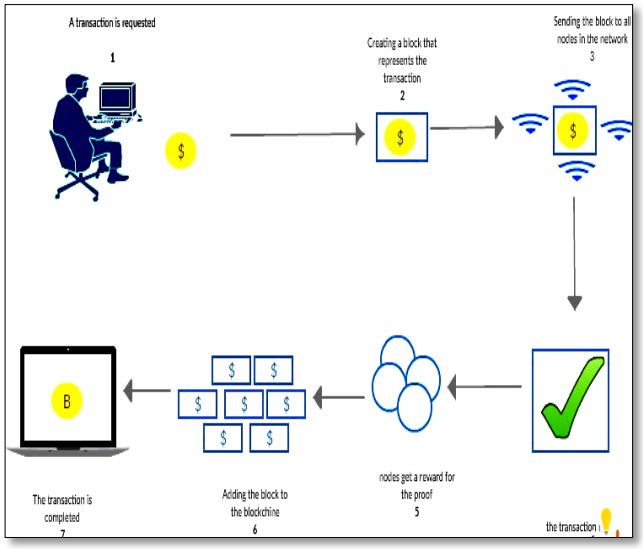

Figure 2: Illustration of Blockchain Transactions

III. RELATED WORK

Great work have been done the context to blockchain and security. [1] Targeted the main issue in health care service which is the execution time as it is the main concern in this kind of environment. The research proposed using cloud services with Swarm Optimization (PSO), and Parallel Particle Swarm Optimization (PPSO) techniques. Furthermore, the study had carried on two sub-experiments. The first was a comparative test between the two techniques that resulted in finding out that PPSO exceeds its peer in three criteria, which are speed, efficiency and execution time. This had led to the second subtest in the study that introduced the usage of PPSO in CloudSim package to solve task scheduling issues. In this research the proposed intelligent model consisted of five components which are: the devices of the stakeholders (Smartphone, Tablet, PC etc.), tasks (requests) of the stakeholders such as telemedicine, electronic records, diseases diagnosis etc., the application layer, smart home network and finally the gateway of the homes. In this model, the network administrator is in charge of applying the PPSO technique. While performing the comparative study, several findings were recorded and have been used to prove the research argument which was declaring that PPSO is a better optimization algorithm than PSO in the cloud computing environments. Furthermore, several relationships had been confirmed such as the positive relationship between the number of particles and execution time in both PSO and PPSO. Also, the negative relationship between the proposed PPSO with the increase of the number of processors with waiting time, turnaround time, CPU utilization, resources utilization, and make-span. Another very interesting research had been carried out by [2] which introduces the internet of things and its applications. It presents important applications that IoT field covered which are Smart home, Wearable's, Smart cities, and machine to machine communication (M2M) by connected cars, IoT in agriculture and Healthcare. Smart cities are one of the most important applications in IoT. Furthermore, it discusses the different elements of a smart city such as smart education, smart government, and smart home. Each element in the smart city is an internet of thing application so it has a model that creates it. Some security challenges that face smart cities are discussed such as Confidentiality and integrity compromise, Eavesdropping, Data loss, and Availability compromise. The big challenge of smart cities is how to protect the sensor's data from being stolen or modified. This research developed a new method based on encryption and encoding processes to solve the problems of security and privacy. The main components of the proposed system are microcontroller kit, temperature sensor breadboard, and electric cable. The first benefit of the proposed system is that the encryption key in both the client and the server is embedded in ESP8266 hardware modules. In addition, the website is hosted on these modules to secure the system from any hacker. It is impossible to hack the hardware because a hacker needs human to open his malicious software and then becomes a victim but the system doesn't let any person to control it. The second benefit is the ability to combine both encryption and encoding data to make hacking a very hard and tedious job. [3] Proposed a hybrid model for predicting Chronic Kidney Diseases (CKD) for residents of smarts cities using Linear Regression (LR) to identify the influencing factors on CKD, and Neural Network (NN) to predict CKD. This hybrid approach resulted in 97.8% accuracy rate which was superior to its other peer models by 64%. The model consists of four parts which are: the devices of the stakeholders (Smartphone, Tablet, PC and etc), cloud agent which is responsible to manage the tasks between the

stakeholder's devices and cloud server, Internet of Things (IoT) endpoints which delivered big data to the cloud to increase the prediction accuracy, and finally the public cloud-IoT which contains the machine learning model with the two intelligent techniques LR and NN. The intelligent model in the cloud-IoT carries on three tasks firstly, cleaning the dataset, secondly, analyzing the data by determining the impact factors by LR which showed that from the twenty-four factors the researchers gathered only thirteen had an effect on CKD, and finally NN was implemented using the thirteen factors as its inputs to predict CKD. A case study was conducted using Windows Azure as a cloud to implement the LR and NN with three CKD cases, from these three cases, two without CKD (NOCKD), and one with CKD. The findings of the experiment for the two NOCKD were 0.99992 and 0.99998, while the CKD got 0.00004 probabilities with a scaling of 1 for NOCKD and 0 for CKD. Current big health care analytics challenges along with the solutions have been discussed in [4]. The main challenges related to electronic medical records (EMR) are high-dimensionality, irregularity, missing and corrupted data, noise, sparsity, and bias. Regarding high dimensionality, it occurs when more parameters are associated with noise and sparsity issues. As a solution for high dimensionality, feature selection techniques such as wrapper methods and filter methods, and feature extraction as linear and nonlinear techniques are used. For irregularity issue, it appears when records are scattered with uneven spans. It is solved using some techniques as baseline features and data transformation (Markov). Furthermore, the paper describes various pre-processing techniques for healthcare data including data annotation, data cleansing, data integration, and data visualization. It also presents several efficient applications and services for healthcare analytics such as clustering, phenotyping, disease progression modeling, statistical regression methods, machine learning method, deep learning method, the image data analysis, mobile healthcare, the environment monitoring, and disease detection. Moreover, it proposes a solution that predicts diseases based on the integration of different types of data. The proposed system collects heterogeneous data from various resources such as sensors, EHR, and users. The system was developed using the Hadoop map reduce. A new layer was added between the Hadoop cluster and data resource. A new approach based on self-organizing multi-agent systems (So-MAS) for modeling and engineering future self-adaptive LCCIs of smart cities had been proposed by [5], which states that large complex critical infrastructures (LCCI), which are complex industrial networks used in advanced countries to control and monitor critical infrastructures such as smart grids and water distribution. So-MAS are multi-agent systems (MAS) that can dynamically and autonomously reorganize themselves to adopt the dynamic changes of the work environment. A novel MAS organizational model called NOSHAPE was adopted in the proposed approach to provide a way to dynamically reorganize the provided large-scale MAS to coordinate agents' interactions and to enable the MAS to adapt the dynamic changes of the environment. The adopted development process of the proposed approach includes three phases, which are analysis, design, and implementation phases. Further, performance evaluation has been conducted based on a simulation environment that presents how the proposed approach is able to deal with the dynamic unanticipated work environment behaviors. The proposed approach achieved up to 47% of performance improvement compared to conventional organizational techniques in MAS. A comparative analysis of the techniques used for facial expression recognition (FER) is presented by [6]. The analysis is based on local binary patterns using various variants such as multi-scale LBP, center-symmetric LBP. Furthermore, the paper proposes a framework for FER which includes four consecutive modules: preprocessing, feature extraction, dimensionality reduction, and classification. For preprocessing, it involves face detection, cropping, normalization, and contrast enhancement. Regarding the feature extraction module, it consists of retrieval of LBP feature and its variants. Dimensionality reduction step uses PCA for a reduction in size of extracted features. Finally, SVM classifier was used for recognizing facial expressions such as smile, sad, surprise, anger, fear, disgust and neutral. The experimental results indicate high recognition accuracy of LBP and its variants on various datasets (JAFFE, CK+, Yale). The results reveal the usefulness of LBP in FER. As a future step, different combinations of LBP will be used to evaluate its effectiveness in improving recognition accuracy. [7] Introduces blockchain to solve the security issues in the Internet of Medical Things (IoMT). In this proposed approach the targeted issues are the centralized cloud used in any Internet of Things (IoT) systems from data privacy and security, as past literature had shown that cloud cannot be completely trusted due to its weak point as data in it can be altered. Moreover, another problem in IoT environment systems is the data leakage from the numerous and varieties of devices used to monitor and collect needed data. The architecture of the proposed system consists of five main parties which are the doctors, body sensors, caretakers, real-time observation statistics and the diagnostics labs. Starting from the doctors who are presented in the system to observe the patients and advise them if any changes in their health that may occur, which will be collected from the sensors on their bodies that alert the doctors when changes occur. Then, there are the caretakers of the patient having the liberty to view his history, and then there is a clinic for real-time observation of the patients and generating statistical reports. In this blockchain based system, the patient record can be viewed by every member of his network. Another party in this system is the diagnostics labs who are in-charge for generating the electronic records and adding them on the blockchain. Some of big data challenges and opportunities in the field of healthcare informatics have been heightened in [8], which provides an illustration of big data and some of its characteristics such as velocity, volume, variety, veracity, value, variability, and visualization. Moreover, the paper presents an overview of cloud computing, its advantages, and disadvantages. Furthermore, it provides a detailed description of some of big data processing and analytics tools such as Hadoop and Spark. With respect to Hadoop, its definition, characteristics, clients, and the four main components in the framework with a description of their architecture were covered. For Spark, a brief description of the primary concepts that support how it works including Resilient Distributed Dataset (RDD) and Spark Machine Learning Library (MLlib) was presented. It also presents a review of big data and data mining in health informatics including the use of Ambient Assisted Living (AAL) and

Remote Patients Monitoring (RPM) models. The paper presents the efficiency of using (AALs) and big data analytics in monitoring the health status of the patients by providing a case study for monitoring patients suffering from one of the chronic diseases. The case study involved three patients having various types of blood pressure disorders (hypertension, hypotension, and norm tension). The study employed the Intelligent Hybrid Context-Aware Model for Patients Under-Supervision at Homes (IHCAF-PUSH) and various algorithms to classify the patient health status into four states: normal, warning, alert, and emergency. The experimental results revealed that the Decision tree (J48) and Naïve Bayer has obtained the highest classification accuracy. [32] Explains that in the current technological era, everything revolves around technology and technology rotates around cloud applications and communication over the internet. Security of data and associated applications is of great importance which can result into drastic results if there is any negligence from programs over the security issues, SDLC cycle and other important factors related to software development and management leads to vulnerabilities in technologies. [33] Describes that Social media usage and popularity of various social media apps (such as Facebook, Twitter, LinkedIn, Instagram, YouTube, My space etc. information sharing through social media has created vulnerabilities and cyber threats which eventually put privacy of personal information of end users which need to be addressed professionally.

IV. USE OF BLOCKCHAIN IN SERVICES

Nowadays, blockchain technology is incorporated in various domains due to its compelling benefits in improving systems efficiency, transparency, and safety. A wide range of domains is utilizing the blockchain approach including health, financial, business, governmental, and educational domains. Following table 1 provides examples of some blockchain-based applications.

Table 1: Blockchain domains and applications

Domain	Application	Description	Examples
Health	Medical record management	Storing health care data and manage medical records.	Guardtime's KSI
	Insurance claim process	Verifying the claim transactions to support health care financing tasks (ie, health plan claims), such as preauthorization payment	Fast Healthcare Interoperability Resources
Financial	Crypto-currencies	Providing a secure environment for financial transactions with the need for the third party	- Bitcoin - Ripple - Litecoin - Monero
	Securities issuance, trading and settlement	Companies issue shares directly and without third party association, trade shares in the secondary market, and tackle securities settlement	NASDAQ private
Governmental	Voting Systems	Storing individuals' votes under a secure, cryptographic hash-appear environment	- Voting system by the Danish political party - Local Community Voting system in South Korea
Education	Accreditors and validators	Storing students data and providing accreditation, and validation for academic achievements	Framework by National University of La Plata (UNLP) that verifies students' academic achievements

With respect to the healthcare domain, several applications and ongoing systems are utilizing blockchain for improving medical record management, enhancing the insurance claim process, and accelerating clinical research [10]. Adopting blockchain for storing patient's health record data and managing of medical records will enable patients to control access to their healthcare data. This will eliminate the need to acquiring copies of the healthcare data or sending data to another healthcare provider [11]. Numerous companies are involved in adopting blockchain technology such as Healthcare Data Gateways [12] Fatcom[13] and others [14, 15, 16]. Guardtime, a well-known company, is using a blockchain-based system to secure 1 million health records in Estonia [17]. It is worth noting that, due to the transparency and immutability of blockchain technology, it is used in some of the governmental services. For example, a Danish political party deployed the first blockchain voting application for internal elections in which every vote is recorded in a secure environment and stakeholders can participate and observe other votes [18]. South Korea, for instance, employed blockchain technology in a local voting system for community funding which enables stockholders to vote on initiatives and community aid [19]. In the financial domain, numerous applications have been introduced for employing blockchain technology. One of the most popular blockchain-based application in the financial area is cryptocurrency. It guarantees a secure environment for financial transactions in virtual currencies such as Bitcoin, Ripple, Litecoin, and Monoro. Various blockchain applications are related to stock markets services such as securities exchange, smart contracts, trading and settlement, and payments and remittance. Generally, these applications aim to simplify and speed up the traditional process. For instance, Nasdaq Private Market, a private investor, has adopted blockchain to reduce the usual trading time from four days to 10 min [20]. Even in the educational domain, blockchain technology is used in different scenarios. Several educational institutions have adopted blockchain for various problems. For example, the National University of La Plata (UNLP) developed a blockchain-based framework that verifies students' academic achievements and accordingly issues the diploma. In 2015, a school in San Frasisco started to utilized blockchain in order to assist employers to validate the academic credentials. [21].

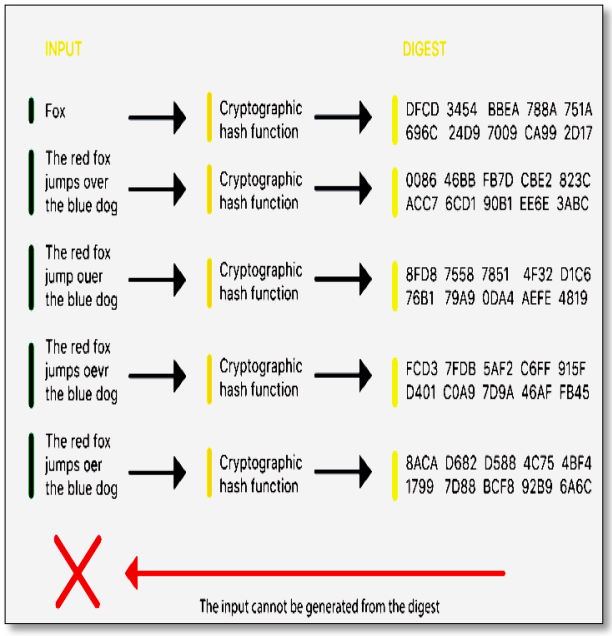

Figure 3: Cryptographic Hash function Generation [31]

V. PROBLEMS AND DEFICIENCIES

Every IoT system in smart cities must guarantee the confidentiality, integrity, and availability of the services. Confidentiality refers to making sure that only the authorized user/s can read the message. Integrity is achieved when the sent message is received at the destination without any modification, and availability means that all services and data are available when they are needed. In an IoT environment, blockchain is expected to play a significant role in the security of IoT devices. In this section, we discuss and summarize some of the problems and deficiencies of secure communication in IoT in Smart Cities and potential blockchain's solution. [27, 28]

a) Identity of Things (IDoT):

The Identity of Things (IDoT) is a method involves assigning unique identifiers (UID) with associated metadata to devices so they can connect and communicate effectively over the Internet. (IDoT) for IoT address a number of challenging problems in secure manner. One main problem is ownership and identity relationships of IoT devices. Ownership of a device changes through the lifetime of the device from the manufacturer, supplier, retailer, and consumer. The consumer ownership of an IoT device can be changed or revoked, if the device gets resold, decommissioned, or compromised. Controlling of attributes and relationships of an IoT device is another problem. Attributes of a device involve manufacturer, make, type, serial number, deployment GPS coordinates, location, etc. Apart from attributes, capabilities, and features, IoT devices have relationships. IoT relationships may contain device to human, device-to-device, or device-to-service. Blockchain has the ability to solve these problems by providing trustworthy and authorized identity registration and ownership tracking. TrustChain technique is used to enable trusted transactions using blockchain while maintaining integrity. Blockchain can register and give identity to connected IoT devices, with a set of attributes and complex relationships that can be uploaded and stored on the blockchain-distributed ledger. Additionally, trustworthy decentralized management, and tracking at every point in the supply chain of an IoT device is provided by blockchain [27].

b) Authentication and Integrity

In IoT security, an authentication mechanism is a process of ensuring that message has not been modified while in the transition to make sure integrity of data, the receiving party is also able to verify the source of the message. To secure communication in IoT in smart cities, the authentication is highly required. This environment has a problem for defining a standard global protocol for authentication in IoT. A suitable implementation of authentication results in a trustworthy environment that ensures secure communication in IOT of smart cities. Blockchain solves the problem of authentication and integrity of transmitted data by connecting IoT devices to the blockchain network that makes transmitted data cryptographically proofed and signed by the true sender, which holds a unique public key and GUID. Besides, all transactions processes made on IoT devices are recorded on the blockchain network and tracked securely and efficiently. [27]

c) Data Privacy, Confidentiality and Integrity

As IoT data transmitted over multiple hops in a network, proper encryption methods are required for ensuring the confidentiality and integrity of data. The data stored on IOT devices are vulnerable to privacy violation by compromising nodes in a network. One of the significant blockchain's solutions for this problem is a smart contract protocol that provides decentralized authentication rules and offers single and multi-party authentication to an IoT Device. Furthermore, smart contracts provide a more effective authorization access rules to connected IoT devices with fewer complexity methods compared with traditional authorization protocols. Additionally, data privacy can be also ensured by using smart contracts technology, which set the access rules, conditions, and time to allow certain individual or group of users or machines to own, control, or have access to transmitted data. The smart contracts control and manage who has the right to update, upgrade, patch the IoT software or hardware, reset the IoT device, provision of new key pairs, initiate a service or repair request, change ownership, and provision or re-provision of the device. [27]

d) Cybersecurity of Communications

Different IoT communication technologies and protocols used to connect the smart device such as HTTP, MQTT, CoAP, or XMPP, or even protocols related to routing as those of RPL and 6LoWPAN, are not secure. For secure communication, protocols have to be wrapped within other security protocols such as DTLS or TLS. [27] Blockchain potentially resolves the problems by using the public key infrastructure (PKI) to authenticate and authorize parties and encrypt their communications. The keys can be used for protection of user information, the confidentiality of data, authentication data and authorization to the network. This can help combat some of the security threats such as Man-in-the-middle attacks when secure communication protocols are implemented on the blockchain. [30].

VI. CONCLUSION AND FUTURE WORK

Based on our findings during this research we can conclude that use of blockchain is going to be a must job for any cloud/internet based services, as blockchain provides a temper-prove feature as it records every transmission in the digital communication which allows the saved data to be viewed publicly with no alteration risk, accomplishing decentralized agreement base. Since health information of

any person is very personal stuff which cannot be shared publically so there is a great need to address secrecy of individual health records. Since blockchain was primarily designed for small data (bitcoins) to store and process so there was no issue related to data storage due to size and nature of this data while on the other hand storing health information systems consisted of huge information where the stored data are enormous, sensitive and it also needs further study to keep track of patient condition. It should be dealt by storing data in the traditional database due to huge quantity and privacy of data and to track this hash references should be stored in the blockchain which allows an authenticated access to the database keeping its authenticity intact. Future research can be conducted to explore option related to increase the processing capacity of IOT devices to properly implement and ensure security and privacy.

VII. REFERENCES

[1] Abdelaziz, A., Salama, A. S., & Riad, A. M. (2019). A Swarm Intelligence Model for Enhancing Health Care Services in Smart Cities Applications. In Security in Smart Cities: Models, Applications, and Challenges (pp. 71-91)

[2] Farahat, I. S., Tolba, A. S., Elhoseny, M., & Eladrosy, W. (2019). Data Security and Challenges in Smart Cities. InSecurity in Smart Cities: Models, Applications, and Challenges(pp. 117-142).

[3] A. S., Riad, A. M., & Mahmoud, A. N. (2019). A Machine Learning Model for Predicting of Chronic Kidney Disease Based Internet of Things and Cloud Computing in Smart Cities. In Security in Smart Cities: Models, Applications, and Challenges (pp. 93-114).

[4] Ismail, A., Shehab, A., & El-Henawy, I. M. (2019). Healthcare Analysis in Smart Big Data Analytics: Reviews, Challenges and Recommendations. In *Security in Smart Cities: Models, Applications, and Challenges* (pp. 27-45)

[5] Abbas, H., Shaheen, S., & Amin, M. (2019). Engineering Large Complex Critical Infrastructures of Future Smart Cities as Self-adaptive Systems. In Security in Smart Cities: Models, Applications, and Challenges (pp. 143-170).

[6] Nigam, S., Singh, R., & Misra, A. K. (2019). Local Binary Patterns Based Facial Expression Recognition for Efficient Smart Applications. In Security in Smart Cities: Models, Applications, and Challenges (pp. 297-322)

[7] Diawar, N., Rizwan, M., Ahmad, F., & Akram, S. (2019). Blockchain: Securing the Internet of Medical Things (IoMT). INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 10(1), 82-89.

[8] Hassan, M. K., El Desouky, A. I., Elghamrawy, S. M., & Sarhan, A. M. (2019). Big Data Challenges and Opportunities in Healthcare Informatics and Smart Hospitals. In Security in Smart Cities: Models, Applications, and Challenges (pp. 3-26)

[9] Abdelaziz, A., Salama, A. S., & Riad, A. M. (2019). A Swarm Intelligence Model for Enhancing Health Care Services in Smart Cities Applications. In Security in Smart Cities: Models, Applications, and Challenges (pp. 71-91)

[10] Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220.

[11] Ivan, D. (2016, August). Moving toward a blockchain-based method for the secure storage of patient records. In ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST.

[12] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems, 40(10), 218.

[13] Snow, P., Deery, B., Kirby, P., & Johnston, D. (2015). Factom ledger by consensus.

[14] Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2018). Blockchain-based medical records secure storage and medical service framework. Journal of medical systems, 43(1), 5.

[15] Prakash, R. (2016). Adoption of blockchain to enable the scalability and adoption of accountable care. In ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST.

[16] Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (2016). A blockchain-based approach to health information exchange networks. In Proc. NIST Workshop Blockchain Healthcare (Vol. 1, pp. 1-10).

[17] Williams-Grut O. Estonia is Using the Technology Behind Bitcoin to Secure 1 Million Health Records. Business Insider Inc. http://www.businessinsider.com/guardtime-estonian-health-records-industrial-blockchainbitcoin-2016-3. Accessed December 20, 2016.

[18] Millet, J. (2014). Danish Political Party May Be First to Use Block Chain For Internal Voting. NewsBTC. 22 April. Retrieved from http://www.newsbtc.com/2014/04/22/danish-political-party-may-first-use-block-chain-internal-voting/

[19] Ojo, A., & Adebayo, S. (2017). Blockchain as a next generation government information infrastructure: a review of initiatives in D5 countries. In Government 3.0–Next Generation Government Technology Infrastructure and Services (pp. 283-298). Springer, Cham.

[20] Yoo, S. (2017). Blockchain based financial case analysis and its implications. Asia Pacific Journal of Innovation and Entrepreneurship, 11(3), 312-321.

[21] Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. IEEE Access, 6, 5112-5127.

[22] Marc, P. (2016). Blockchain technology: Principles and applications (No. halshs-01231205).

[23] Guardtime. Guardtime Industrial Blockchain. https://guardtime.com/. Accessed February 20, 2019.

[24] HL7.org. Fast Healthcare Interoperability Resources (FHIR). https://www.hl7.org/fhir/. Accessed February 15, 2017.

[25] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[26] Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., & Brooks, R. (2016, December). A

brief survey of cryptocurrency systems. In 2016 14th annual conference on privacy, security and trust (PST) (pp. 745-752). IEEE.

[27] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395-411.

[28] Biswas, K., & Muthukkumarasamy, V. (2016, December). Securing smart cities using blockchain technology. In 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS) (pp. 1392-1393). IEEE.

[29] Yakubov, A., Shbair, W., Wallbom, A., & Sanda, D. (2018). A blockchain-based PKI management framework. In The First IEEE/IFIP International Workshop on Managing and Managed by

[30] Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018, Tapei, Tawain 23-27 April 2018.

[32] https://commons.wikimedia.org/wiki/File:Hash_function.svg

[33] Shahbaz Pervez, Malik Misbah, Humaira Yaqub, Mahjabeena, "Protective Measures For Security & Privacy In Cyber Era Of Cloud Computing", "IEEE International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing " 28-29 January 2018, Villore district Tamil Nado India.

[34] Shahbaz Pervez, Mahjabeena, Humaira Yaqub, Malik Misbah, "Optimal Use Of C4I for Securing Cloud & Social Network User's Privacy", "IEEE International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing (EECCMC)" 28-29 January 2018, Villore district Tamil Nado India.