# Trust Modeling for Blockchain-based Wearable Data Market

Mohammad Jabed Morshed Chowdhury*, Md Sadek Ferdous†‡, Kamanashis Biswas§,
Niaz Chowdhury¶, A S M Kayes*, Paul Watters*, Alex Ng*
*La Trobe University, Victoria, Australia.
†Shahjalal University of Science and Technology, Sylhet, Bangladesh.
‡Imperial College London, London, UK.
§Australian Catholic University, NSW and Griffith Univeristy, QLD, Australia.
¶Open University, Milton Keynes, UK

***Abstract*—Wearable devices continuously produce physiological data that can provide individuals critical information about their daily routine or fitness level in combination with their smartphones without requiring manual calculations or maintaining log-books. Real-time participant-generated data can enable large scale observational studies of health conditions, provide better insights into medical conditions of individuals and streamline clinical trial processes in medical research. However, privacy is a major concern for health data and there can be a lack of trust among different parties in the health data collection process. In addition, individuals often do not have sufficient control over the sharing of their data from the wearable devices. The lack of control, trust and privacy are key barriers to research participants being prepared to share their personal data from wearable devices. In this work, we propose a trust model to overcome the trust deficit among different parties. Then, we present a reference system architecture, rooted on the developed trust model, that provides incentive for individuals to securely share their health data through a data marketplace. By encouraging individuals to share their real-time health data, researchers will have access to large data sets at low cost.**

***Index Terms*—Wearable Data, Data Sharing, Data Market, Health Research, Trust**

## I. Introduction

Many individuals are willing to share their data for medical research. According to [1], nine-out-of-ten patients with access to their health data are willing to share that data to support research. However, recruiting sufficient numbers of suitable participants in research studies is both time-consuming and expensive. For example, given the strict qualification criteria imposed by the researchers, only about 5% of candidates eventually constitute the group participating in clinical trials [2]. Long recruitment phases prolong the execution of trials, thus increasing the time it takes for theories to be tested and innovative new medicines to be studied and approved. In addition, patients often have to travel long distances to participate in those trials. However, the proliferation of the health and fitness related wearable devices has opened up new opportunities to connect the patients with the researchers. If suitable systems and protocols can be built to bridge these two communities, it might be possible to acquire a large volume of research data at low cost. Therefore, there is an urgent need of a common trusted platform through which wearable device owners can easily share their data with the researchers. In addition, they would be able to specify *what* subsets of their data can be shared, *when* it can be shared, and the type of researchers *with whom* it can be shared (e.g. they might be okay to share their data with universities but not with drug companies). Similarly, researchers also need to search for potential research subjects whose data are of interest. Although many individuals are motivated to share their data for the common human good, many others may be prompted to do so if there is a financial incentive to share their data [3]. Therefore, this platform should include a "data market" that incentivises individuals to share their data and facilitates the matching of researchers with suitable subjects.

However, there are a number of challenges to design such systems and protocols for a research data market. Since remote data owners and researchers are unknown to each other, there is always a lack of trust in market-mediated relationships. Therefore, mechanisms need to be established to build trust by ensuring that all parties abide by their obligations in the transactional contract. This trust needs to run both ways.

On one hand, the data owners want to ensure that their privacy is maintained and their information is only used for specified research purposes. Privacy is typically assured through anonymization [4], [5]. According to a survey [6], 85% of respondents perceive privacy concerns as a major barrier to sharing health information. It is clear that collected data may be used to extract or infer sensitive information about users' private lives, habits, activities and relations, which all refer to individuals' privacy [7]. About half of the respondents were either concerned or very concerned about the re-identication of their anonymized health and medical information. If data were irreversibly anonymized, 71% of respondents were willing to share their data with researchers.

Researchers, on the other hand, need to be ensured that the data they purchase is in fact coming from *bona fide* monitoring devices worn by subjects whose profile matches cohort requirements. The provision of payment for data itself creates an incentive for people to try and game a system by spoofing data generation. A financially motivated marketplace for real-time health data could be counter-productive to establishing trust. However, any platform developed to enable such data market-

place must build trust among different parties. In this paper, we propose a trust model to encapsulate the trust assumptions between the entities and enable the implementation of trust building mechanism. Then, we evaluate the risk of building such system using the DREAD (Damage, Reproducibility, Exploitability, Affected-users, Disoverability) model.

The structure of the paper is as follows. In section II, we discuss background and related works. Section III explains the functional requirements for the data sharing framework. A trust model encapsulating trust assumptions and trust building mechanisms is defined in section IV. In section V, we present the proposed system architecture. Section VI evaluates and compares the proposed model with a traditional system using the DREAD model. Finally, section VII concludes the paper.

## II. Background and Related Work

### A. Wearable Data in Medical Research

The use of wearable devices in medical research has become a new prospect. While challenges such as stability and biocompatibility are major concerns, their potential value in managing chronic diseases cannot be ignored in addition to maintaining regular fitness records [8]. Several promising wearables have emerged from some reputed companies. Litmus Health, a clinical data science platform providing research infrastructure for real-life data, has recently identified 15 wearable devices including ActiGraph, Fitbit Icon and Garmin Vivomove and argued that these devices have huge potential in the pharma and healthcare industry for providing quality data [9].

Despite the enormous potential of these devices, they are not free from scepticism. The fact is that the development of wearable devices is made by bioengineers who seem to be more interested in performance than privacy and security issues of the devices. It is only a matter of time when the consequences of overlooking these problems will be exposed, and many companies will not be able to sustain that aftereffect. Therefore, collaboration with researchers from the computing and mathematical domain becomes an utmost necessity [10].

### B. Digital Data Markets

It is anticipated that the value of the data marketplace will be around $3.6 trillion, and approximately 4.38 Zettabytes of data will be traded every year [11]. Some of these marketplaces are powered by blockchain technology while many are still classical centralized data centres. **Datapace** [12] is a blockchain-based data marketplace that uses Hyperledger Fabric, an open-source permissioned blockchain platform [13]. The use of hyperledger fabric can be a strength when it operates in a real consortium environment, however, due to the restrictive nature, unwanted entities may not get access to it. If one single entity remains responsible for maintaining all nodes, this strength becomes an Achilles heel and may absorb many of the benefits that blockchain could potentially offer.

One of the renowned public ledgers is IOTA [14] that acts as a marketplace for IoT data. IOTA is designed based on the objective of processing unlimited transactions at a given time. While doing so, it does not charge the participating entities for making transactions instead makes the use of the community who help each other to verify the transactions. Since the launch of IOTA, its founders have the vision to make it a marketplace for IoT data, although it has not seen much success yet.

Another similar blockchain-based platform is Moeco. This platform is not a true marketplace in nature since it enables sellers to sell their data to the buyers acting as a middleman and processes the payment on their behalf [15].

On the other hand, Dawex [16] is an example of a classical marketplace where buyers can discover and buy data of various types such as IoT data collected through wearables. It works as the *eBay for data* where one can have a virtual store and sell either live or historical data to the potential buyers.

### C. Trust Management in Medical Research Data Collection

A core requirement of scientific research is that empirical evidence is social and established rather than impersonal and neutral [17]. Numerical data is not to be trusted instinctively, but to be considered as a likely outcome of the social practice [18]. As such, the trust management of medical data is two folds – first, the participants must trust the system and feel safe in sharing their data, and second, the research community needs to be convinced that the collected data is unbiased and established enough to back the decision researchers have been reaching upon [19].

Trust management in the medical marketplace is still a grey area. The Nobel Laureate economist Kenneth Arrow described the system as an entity characterized by uncertainty in 1967. Numerous initiatives have been taken ever since, but the situation did not significantly change [20]. It is, therefore, likely that if we are to establish trust in this domain, an approach entirely out of the box will be needed. Amongst the existing technology, blockchain technology looks like the most suited candidate to be that out of the box strategy.

## III. Requirement Analysis Based on a Scenario

Let's say, Ms Marry is an alzheimer patient. Due to her medical conditions, her movement is limited and she wears a medical device to monitor her health condition. She has heard about a medical research team who recruits alzheimer patients for their research. She is interested to share/sell her data with the research team. However, she is worried about her privacy. On the other hand, a medical research team is investigating alzheimer. They need data from suitable alzheimer patients to conduct and validate their research work. The research team is even happy to pay for the data of alzheimer patients. By analysing the scenario presented here, we have formulated the following functional requirements

**Data Marketplace (Req 1):** Ms Marry and the medical research team both need a match making mechanism to communicate. A data marketplace (DM) would facilitate both parties where Ms Marry can sell/share her health data from the comport of her home and the research team can have access to both historical and real-time data. Monetization of the data will influence many of the patients like Ms Marry to share

their data and earn some extra dollars. However, individuals may wish to donate their data for common human good.

**Privacy Preserving Data Sharing (Req 2):** Wearable devices continuously produce health data. This time-series data can be exploited to compromise the privacy of the individuals. Therefore, the individuals want a strong privacy preservation mechanism in place while data is shared with the researchers. This mechanism ensures that the researchers can work with the shared data but won't be able to identify whose data it is.

**Fine Grained Access Control (Req 3):** The individuals need control on who, when and how long the researchers can access their data [21]. Therefore, a fine grained access control mechanism is vital.

**Trust/Transparency on the System (Req 4):** The data produced by the wearable devices are private and real-time. The individuals need to fully trust the system that 'what it said it will do'. Traditional centralized systems do not provide transparency of the data flow and access.

## IV. Trust Model

The notion of trust plays a crucial role in designing a privacy-preserving platform for sharing health data. In fact, we expect trust to be the inherent property that will bind together all involved entities and provide the underlying confidence to interact with each other using the proposed platform. In this section, we present our trust analysis.

### A. Trust Semantics

Trust is essentially a directional relationship between two entities, a trustor and a trustee, where a trustor trusts a trustee within a *scope* with respect to perform a certain *action*. An action is the function that the trustor expects the trustee to perform. Optionally, an action may have a qualitative modifier which implies the quality of the action.

A scope in a trust relationship signifies the specific purpose or context into which that trust relationship is valid. Trust can be of two types: Direct Trust (*DT*) and Indirect Trust (*IT*) [22]. A direct trust is established based on first hand experience and evidence, whereas, an indirect trust, also known as *Transitive Trust*, is established by referrals from one or more intermediate third parties. There is a notion of *Mutual Trust* which exhibits a bi-directional trust relationship with the same trust type, scope and action between the corresponding entities. In such case, both entities can act as the trustor and the trustee.

Trust often exhibits the transitivity property [23]: if an entity *A* trusts another entity *B* and *B* trusts another entity *C*, a trust relation can be derived between *A* and *C*. To derive such a transitive trust relation, the trust scope and the action must be same. A trust with a single scope can be defined as an atomic trust. A compound trust can be defined as the combined trust of several different atomic trusts where the trust direction and action between a trustor and trustee will remain same.

### B. Notations

Next, we introduce the notations to be used in our trust model. We use $E$ to denote the set of entities. The elements of $E$ are the entities (data subjects, data brokers and so on) in our data model. We use the notation $DS$ to represent the set of data subjects, $DCUST$ for the set of data custodians, $DB$ for the set of data brokers, $BC$ to denote a singleton set of a blockchain consortium and $DCON$ to represent the set of data consumers. Thus,

$$E \triangleq \langle DS \cup DCUST \cup DB \cup BC \cup DCON \rangle$$

As explained above, we consider two types of trust: direct trust ($DT$) and indirect trust ($IT$). Therefore, $T \triangleq \langle DT, IT \rangle$ where $T$ represents the set of trust types.

We use $S$ for the set of trust scopes. Different trust scopes can be defined depending on the trust requirements. We consider the following trust scope elements of set $S$:

$$S \triangleq \langle DATA \cup POL \cup PAYMENT \rangle$$

where, $DATA$ represents the trust scope with respect to data, $POL$ represents the trust scope with respect to policy, and $PAYMENT$ denotes the trust scope corresponding to payment.

Different application domains will have require different actions. In the scope of this article, we consider the following actions with their corresponding notation: $STO$ (Storage Action), $SHA$ (Sharing Action), $TRN$ (Transaction Action), $MGT$ (Management Action), $ENF$ (Enforcement Action), $MAT$ (Data matchmaking action), $ANON$ (Anonymization action). The notation $A$ is used to denote the set of actions which can be defined in the following way:

$$A \triangleq \langle STO \cup SHA \cup TRN \cup MGT \cup ENF \cup MAT \cup ANON \rangle$$

Optionally, some actions might have qualitative modifiers. We indicates the set of modifiers with $M$. The modifier considered in this article is presented as follows along with its notation: $ACCU$ (*accuracy* of a certain action) $SECU$ (*security* of a certain action), $CON$ (*consent* for an action), and $AUD$ (*auditing* for an action).

### C. Model

In essence a trust model represents the trust relationship between different entities in a scope limited to the corresponding application. The relationship is represented using a notation which embodies all the components of a trust relationship. In this work, we utilize the trust modelling framework presented in [24].

According to that model, a trust relationship of trust type $t$ between a trustor $e_1$ and trustee $e_2$ having a trust scope of $s \in S$ for a particular action $a \in A$ with an optional modifier $m \in M$ is denoted with the following notation:

$$e_1 \xrightarrow[a\,.\,m]{t\,:\,s} e_2$$

If there are two trustors $(e_1, e_2)$ having the similar trust relationship with a trustee $(e_3)$ with the same trust type, scope and action, then we can combine these two relationships using the following notation:

$$e_1, e_2 \xrightarrow[a\,.\,m]{t\,:\,s} e_3$$

Similarly, if a trustor ($e_1$) having the similar trust relationship with two trustees ($e_2$ and $e_3$) with the same trust type, scope and action, then we can combine these two relationships using the following notation:

$$e_1 \xrightarrow[a\,.\,m]{t\,:\,s} e_2, e_3$$

Next, we explore different trust relationships for the proposed platform:

TR-1 A data subject ($ds \in DS$) trusts that a data custodian ($dcust \in DCUST$) will store data originating from wearable devices in a secure fashion. This relationship can be modelled in the following way:

$$ds \xrightarrow[STO\,.\,SECU]{DT\,:\,DATA} dcust$$

TR-2 A data subject ($ds \in DS$) trusts that a data custodian ($dcust \in DCUST$) will share their personal data only with their consent. This relationship can be modelled in the following way:

$$ds \xrightarrow[SHA\,.\,CON]{DT\,:\,DATA} dcust$$

TR-3 A data subject ($ds \in DS$) and a data consumer ($dcon \in DCON$) both trust that a data broker ($db \in DB$) will match-make policies between them and a data consumer. This relationship can be modelled in the following way:

$$ds, dcon \xrightarrow[MAT]{DT\,:\,POL} db$$

TR-4 A data subject ($ds \in DS$) and a data consumer ($dcon \in DCON$) both trust that a data broker ($db \in DB$) will allow the management of policies for them. This relationship can be modelled in the following way:

$$ds, dcon \xrightarrow[MGT]{DT\,:\,POL} db$$

TR-5 Both a data subject ($ds \in DS$) and a data consumer ($dcon \in DCON$) both trust that a data broker ($db \in DB$) will enable the transaction of payments. This relationship can be modelled in the following way:

$$ds, dcon \xrightarrow[TRN]{DT\,:\,PAYMENT} db$$

TR-6 Both a data subject ($ds \in DS$) and a data custodian ($dcust \in DCUST$) trust that the blockchain consortium ($bc \in BC$) enforces the corresponding policies. This relationship can be modelled in the following way:

$$ds, dcust \xrightarrow[ENF]{DT\,:\,POL} bc$$

TR-7 A data consumer ($dcon \in DCON$) trusts that both the data subject ($ds \in DS$) and the data custodian ($dcust \in DCUST$) share accurate data. This relationship is modelled in the following way:

$$dcon \xrightarrow[SHA\,.\,ACCU]{DT\,:\,DATA} ds, dcust$$

TR-8 Both a data subject ($ds \in DS$) and a data consumer ($dcon \in DCON$) trust that the blockchain consortium ($bc \in BC$) shares data in an auditable fashion. This relationship can be modelled in the following way:

$$ds, dcon \xrightarrow[SHA\,.\,AUD]{DT\,:\,DATA} bc$$

TR-9 A data subject ($ds \in DS$) trusts that the blockchain consortium ($bc \in BC$) provides data anonymization service. This relationship can be modelled as follows:

$$ds \xrightarrow[ANON]{DT\,:\,DATA} bc$$

## V. System Architecture for Data Market

Fig. 1 shows the system architecture to achieve privacy preserving health data sharing from wearable devices. The system architecture has the following building blocks: i) Data Subject, ii) Data Consumer, iii) Data Custodian, iv) Data Broker/Data Marketplace, and v) Blockchain Consortium Module. Each of them is described below.

**1. Data Subjects:** DSs are the individual patients who want to share and/or sell their data produced by wearable devices. A DS has the following functionalities:

- Register to the marketplace with their preferences. They can define if they want that their data should not be used for any particular purpose such as military.
- Register with the blockchain consortium to have their own crypto-wallet and access to the blockchain.
- Facilitate data collection from their wearable devices as accurately as possible (satisfying *TR-7*).
- Define the data sharing policy to be used for match-making services.
- Authorize the blockchain consortium to fetch the data.

**2. Data Consumer:** DCONs are the researchers from both public (e.g., researchers from public university) and private (e.g., researchers employed by the private companies) sectors. A DCON has the following functionalities:

- Register to the blockchain consortium. The consortium is responsible to conduct proper background checking of the data consumers before allowing them in the network.
- Register with the marketplace to be able to search for their suitable data donors.
- Access anonymized data from the blockchain consortium.
- Pay for the accessed data.

**3. Data Custodian:** DCUSTs are the wearable device service providers, such as FitBit, apple watch etc. These service providers sell wearable devices and allow the individuals to access their data via cloud-based resources and services [25], [26]. They also allow the DSs to share their data via mobile or web APIs. A DCUST has the following functionalities:

- Collect data subject's data via wearable devices as accurately as possible (satisfying *TR-7*).
- Store the data securely (satisfying *TR-1*).
- Allows data subjects to share their data with consent (satisfying *TR-2*).

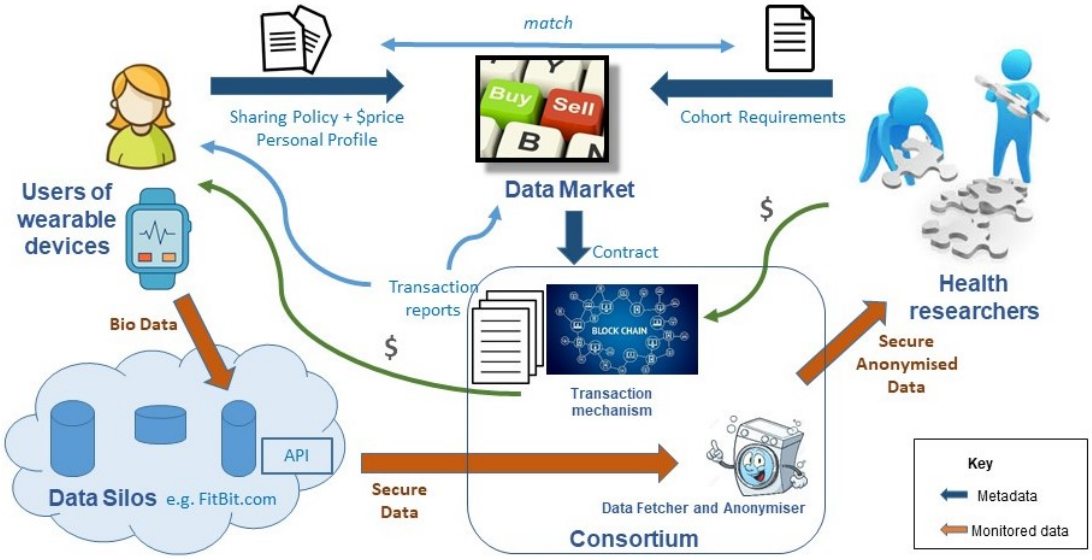


Fig. 1: Proposed system architecture

**4. Data Broker/Data Marketplace:** A DB also known as data marketplace is the matchmaker between the DS and the DCON. The owner of the data marketplace will usually get a commission for each sale. They will regularly run marketing campaigns to popularize their marketplace and maximize their profits. A DB has the following functionalities:

- Provide a platform for the data subject to register and data consumer to search.
- Register with the blockchain.
- Provide the match-making service between a DS and a DCON (thereby satisfying *TR-3*).
- Upload the copy of the defined data sharing policy, from a data subject and a consumer, to the blockchain (trust building mechanism) (satisfying *TR-4*).
- Receive the payment from the DCON via blockchain and pass it to a DS (satisfying *TR-5*).

**5. Blockchain Consortium:** A BC is the team of academicians from the public university who will establish and run the blockchain network. It can be treated as research data sharing network. As no one single academic controls the network, the consensus need to be made to allow any transaction in the network. This mechanism in blockchain will prevent any malicious activities in the network as well as will work as a trust building mechanism for the overall system. The blockchain-consortium system plays very critical role in this data sharing framework. The BC has the following components and functionalities:

- *Registration:* It allows the data subjects, data consumers and the marketplace to register in the system. It provides required background checks before allowing anyone to register.
- *Policy Checking:* When blockchain is notified to access the data subject's data, it checks the data sharing policy of that particular data subject from the blockchain to ensure that data marketplace cannot make changes to the data subject's data sharing policy for their benefits.
- *Data Fetching:* During the data subject registration phase, the data subject authorizes the blockchain consortium to fetch its data when appropriate. If the data sharing policy allows (satisfying *TR-6*) then the data fetcher fetches the data from the data custodian. This architectural decision is also very vital as it ensures the data marketplace does not have any access to the wearable data. Only trusted blockchain fetcher module has access to the data. The underlying blockchain module allows the BC to record and audit every single piece of data sharing (satisfying *TR-8*)
- *Anonymizer:* This particular modules anonymize the data before releasing them to the data consumer and thereby satisfying *TR-9*.
- *Payment:* It transacts money when data is released to the data consumers according to the data sharing policy.

## VI. Evaluation

This section evaluates the effects of security threats on conventional data sharing platforms and compares the results with our proposed model using DREAD model [27]. First, we define five common security threats on healthcare system based on the KPMG report [28]. The report identifies the following security concerns and the greatest vulnerabilities in data security: malware infecting systems (67%), external attacks (65%), internal vulnerabilities (40%), device security (32%) and inadequate firewalls (27%). We choose five specific security threats in order to represent each of these categories as presented in Table I. We also briefly define the DREAD model and associate a risk score to each category of DREAD model for each threat to determine the total risk factor.

TABLE I: Five common security threats on health data

| Threat Description | Threat Target | Risk | Attack Techniques |
|---|---|---|---|
| T1: Attackers may encrypt health information and demand a ransom | Health Data | High | Malware like Ransomware |
| T2: Attackers may steal sensitive information such as login credentials | User Authentication System | Medium | Phishing Attack |
| T3: Attackers may disclose sensitive information for financial benefits | Statistical/Personal Information | Medium | Insider Attacks |
| T4: Attackers may manipulate or inject false information in the system | Wearable Devices | High | Node Compromization Attacks |
| T5: Attackers may prevent legitimate users from accessing the service | The Whole System | High | Distributed Denial of Service Attack |

### A. DREAD Model

The DREAD model is commonly used to evaluate and triage various threats by rating them on the basis of five categories: Damage (D), Reproducibility (R), Exploitability (E), Affected Users (A) and Discoverability (D). Here, we describe each of these categories in brief.

- **Damage-** Damage refers to the extent to which the system is affected by a threat. Thus, it is necessary to get the answer of- *"how bad would an attack be?"*.
- **Reproducibility-** This refers to how often the stated event can potentially occur, i.e., *"how easy it is to reproduce the attack?"*.
- **Exploitability-** Exploitability is directly related to vulnerability of a system. It determines *"how much work is required to launch an attack?"*.
- **Affected Users-** This simply measures the number of people that will be affected by an attack.
- **Discoverability-** The last category of DREAD, discoverability, is also related to vulnerability as it tries to get answer of *"how easy is it to discover the vulnerability?"*.

In the DREAD model, the threat is rated by answering the above questions and assigning a numeric value for each category. This value represents the severity of a threat for a particular category and can be expressed as follows: 1 - *low*, 2 - *medium*, 3 - *high*. First, we assign risk factors for each category of DREAD model and then we use the following range to calculate the overall risk of each threat: High (12-15), Medium (8-11), and Low (5-7). Now, by plotting and summing up the values for each threat identified in Table I, we can calculate the total risk value and determine the severity of each threat as shown in the next subsection.

### B. Risk Rating Using DREAD

For evaluation, we choose an IoT cloud based wearable ECG monitoring system that gathers ECG data using a wearable monitoring node and transmits directly to the IoT-cloud using Wi-Fi [29]. The system is divided into three parts: i) ECG sensing network, which is responsible for collecting physiological data from the body surface and transmitting them to the IoT cloud via a wireless channel, ii) IoT-cloud, which provides a number of functionalities such as data cleaning, storage, analysis and disease warning, and iii) Graphical User Interface, which is responsible for data visualization and management. In a nutshell, the ECG monitoring node collects data from human body and forwards these data to the IoT-cloud, which stores them in a database. Any user can login the IoT cloud and access the ECG data through a website or a mobile application.

TABLE II: DREAD rating of the IoT cloud based system

| Threats | D | R | E | A | D | Total | Rating |
|---|---|---|---|---|---|---|---|
| T1 | 3 | 2 | 2 | 3 | 2 | 12 | High |
| T2 | 2 | 2 | 2 | 1 | 3 | 10 | Medium |
| T3 | 3 | 1 | 2 | 3 | 1 | 10 | Medium |
| T4 | 3 | 2 | 3 | 3 | 2 | 13 | High |
| T5 | 3 | 2 | 3 | 3 | 3 | 14 | High |

Table II presents the risk rating scores for each threat in the IoT based data sharing platform. Since the IoT cloud based system doesn't employ any cryptographic schemes except user authentication, it is vulnerable to various security threats. The risks of reproducibility, exploitability and discoverability are very high due to the following reasons: i) there is a single-point-of-failure in the system, e.g., monitoring node ii) no cryptographic scheme is used to ensure data confidentiality and integrity, iii) the system depends on central servers, iv) the attackers would have full control of the system if the central server is compromised. As a consequence, the level of damage and the number of affected users would be significantly large in this system. It can also be seen that the overall impacts of security threats on IoT cloud based system is high as the average risk factor equals to 11.8.

Unlike the centralized IoT cloud based system, our proposed model uses an immutable and irrefutable distributed ledger to record medical data. The strong cryptographic schemes of blockchain technology makes it almost impossible to modify or inject data in the system. Due to the distributed nature of blockchain, the damage and affected number of users would be very minimal in the proposed system. However, reproducibility, exploitibility and discoverability of threats could be major problems in a blockchain based system that is public and contains buggy smart contracts. However, since only authenticated and verified users can participate in our consortium blockchain platform, the impacts of these threats are negligible in our proposed model. The risk rating values of the proposed system are presented in Table III. It can be seen that the risk is low for most of the common threats in the proposed system except the insider attacks. Similarly, the average risk factor equals to 6.4 which is also lower compared to the IoT based healthcare system.

TABLE III: DREAD rating of the proposed system

| Threats | D | R | E | A | D | Total | Rating |
|---|---|---|---|---|---|---|---|
| T1 | 1 | 1 | 1 | 1 | 1 | 5 | Low |
| T2 | 2 | 1 | 1 | 2 | 1 | 7 | Low |
| T3 | 2 | 1 | 2 | 2 | 1 | 8 | Medium |
| T4 | 2 | 1 | 2 | 1 | 1 | 7 | Low |
| T5 | 1 | 1 | 1 | 1 | 1 | 5 | Low |

### C. Discussion

In a nutshell, the proposed blockchain based system provides resiliency against various security threats and thus minimizes the overall risks in healthcare systems. The inherent properties of blockchain technology ensure the integrity, confidentiality and availability of information in a trustless environment. Compared to traditional data sharing systems, the proposed model is more reliable and trustworthy since there is no need of trusted third parties or intermediaries like conventional systems.

## VII. Conclusion

Data availability for health researchers is critical for sustaining the momentum of successful innovations in healthcare technology. Wearable devices allow individuals to generate and share their health related data. However, individuals are concerned about the privacy of their data. Although research has addressed privacy issues in traditional healthcare data, preserving the privacy of health data (especially for cyber-physical based streaming data) represents a blind-spot in scholarly knowledge. In this work, we have outlined the requirements for a privacy-preserving framework. We have also discussed the trust deficit between different parties in a medical data sharing framework. Finally, we have proposed a data sharing framework which can address the security requirements and build trust between individuals and the researchers. This framework will help individual patients sharing their data with prospective researchers without the risk of compromising their privacy.

## References


[1] D. M. Maslove, J. Klein, K. Brohman, and P. Martin, "Using blockchain technology to manage clinical trials data: A proof-of-concept study," *JMIR medical informatics*, vol. 6, no. 4, p. e11949, 2018.

[2] E. R. Weitzman, S. Kelemen, L. Kaci, and K. D. Mandl, "Willingness to share personal health record data for care improvement and public health: a survey of experienced personal health record users," *BMC medical informatics and decision making*, vol. 12, no. 1, p. 39, 2012.

[3] A. Rowhani-Farid, M. Allen, and A. G. Barnett, "What incentives increase data sharing in health and medical research? a systematic review," *Research integrity and peer review*, vol. 2, no. 1, p. 4, 2017.

[4] B. C. Fung, K. Wang, and S. Y. Philip, "Anonymizing classification data for privacy preservation," *IEEE transactions on knowledge and data engineering*, vol. 19, no. 5, pp. 711–725, 2007.

[5] A. Kobsa and J. Schreck, "Privacy through pseudonymity in user-adaptive systems," *ACM Transactions on Internet Technology (TOIT)*, vol. 3, no. 2, pp. 149–183, 2003.

[6] E. R. Weitzman, L. Kaci, and K. D. Mandl, "Sharing medical data for health research: the early personal health record experience," *Journal of medical Internet research*, vol. 12, no. 2, p. e14, 2010.

[7] W. Zhou and S. Piramuthu, "Security/privacy of wearable fitness tracking iot devices," in *2014 9th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE, 2014, pp. 1–5.

[8] H. B. Rhodes, "Accessing and using data from wearable fitness devices," *Journal of AHIMA*, vol. 85, no. 9, pp. 48–50, 2014.

[9] L. Health, *Litmus Health Announces New End-to-End Data Science Platform for Clinical Research*, Oct. 2019, https://www.technologynetworks.com/diagnostics/product-news/litmus-health-announces-new-end-to-end-data-science-platform-for/-clinical-research-322309.

[10] M. N. Sawka and K. E. Friedl, "Emerging wearable physiological monitoring technologies and decision aids for health and performance," 2017.

[11] Accenture, *Value of data: The dawn of the data marketplace*, Oct. 2018, https://www.accenture.com/au-en/insights/high-tech/dawn-of-data-marketplace.

[12] Datapace, *Unlock the enormous value of digital data with marketplace powered by blockchain and global network of sensors.*, Oct. 2018, https://www.datapace.io/.

[13] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*. ACM, 2018, p. 30.

[14] IOTA, *IOTA White Paper*, 2015, https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf.

[15] Moeco, *Moeco Blockchain*, 2019, https://moeco.io/.

[16] Dawex, *Sell, buy and share data — Dawex*, Oct. 2018, https://www.dawex.com/en/.

[17] B. Latour and S. Woolgar, *Laboratory life: The construction of scientific facts*. Princeton University Press, 2013.

[18] T. M. Porter, *Trust in numbers: The pursuit of objectivity in science and public life*. Princeton University Press, 1996.

[19] K. Ostherr, "The medical futures lab: An applied media studies experiment in digital medical humanities," in *Applied Media Studies*. Routledge, 2017, pp. 60–78.

[20] A. Maynard and K. Bloor, "Trust and performance management in the medical marketplace," *Journal of the Royal Society of Medicine*, vol. 96, no. 11, pp. 532–539, 2003.

[21] M. Chowdhury, A. Colman, J. Han, and A. Kabir, "A policy framework for subject-driven data sharing," in *51st Hawaii International Conference on System Sciences*, 2018.

[22] U. Kylau, I. Thomas, M. Menzel, and C. Meinel, "Trust requirements in identity federation topologies," in *2009 International Conference on Advanced Information Networking and Applications*. IEEE, 2009, pp. 137–145.

[23] A. Jøsang, E. Gray, and M. Kinateder, "Simplification and analysis of transitive trust networks," *Web Intelligence and Agent Systems: An International Journal*, vol. 4, no. 2, pp. 139–161, 2006.

[24] M. S. Ferdous, G. Norman, A. Jøsang, and R. Poet, "Mathematical modelling of trust issues in federated identity management," in *IFIP International Conference on Trust Management*. Springer, Cham, 2015, pp. 13–29.

[25] A. Kayes, W. Rahayu, T. Dillon, E. Chang, and J. Han, "Context-aware access control with imprecise context characterization for cloud-based data resources," *Future Generation Computer Systems*, vol. 93, pp. 237–255, 2019.

[26] A. Kayes, W. Rahayu, and T. Dillon, "Critical situation management utilizing iot-based data resources through dynamic contextual role modeling and activation," *Computing*, pp. 1–30, 2018.

[27] O. S. Group, *Security/OSSA-Metrics*, 2019, https://wiki.openstack.org/wiki/Security/OSSA-Metrics#DREAD.

[28] KPMG, *Healthcare and Cyber Security: Increasing Threats Require Increasing Capability*, 2015, https://assets.kpmg/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf.

[29] Z. Yang, Q. Zhou, L. Lei, K. Zheng, and W. Xiang, "An iot-cloud based wearable ecg monitoring system for smart healthcare," *Journal of Medical Systems*, vol. 40, no. 12, p. 286, Oct 2016. [Online]. Available: https://doi.org/10.1007/s10916-016-0644-9