Blockchain-Secured Health Wearables in Smart Homes Utilising Raspberry Pi Web of Things Gateways

Solomon Hopewell Kembo
Department of Computer Engineering
University of Zimbabwe
solomonkembo@gmail.com

Patience Mpofu
Department of Computer Engineering
University of Zimbabwe
mampopatie@gmail.com

Brighton Tafadzwa Mukorera
Cryptosine PBC
bmukorera@gmail.com

Saulo Jacques
Hacking Ecology
saulo@hackingecology.com

Abstract

Owing to the large-scale public health crisis arising from the Coronavirus Disease 2019 (COVID-19), the global health system could not adequately deal with the entirety of infections. Consequently, improvisations meant to complement the healthcare systems in remedying the pandemic emerged. “Hospital-at-home” improvisations include the use of wearable technology to triage patients within households before consulting the health institutions. The wearable devices collect physiological and activity data in order to detect or predict the prevalence of the disease.

Unfortunately, Do-It-Yourself health improvisations expose citizens to security vulnerabilities and interoperability challenges. This study proposes the adaptation of a prototype developed prior to the pandemic in securing smart homes and to interoperate health wearable devices used in detecting the prevalence of COVID-19 before symptoms manifest. Focus is placed on: 1) Integration of wearables from different vendors to ensure interoperability using the Mozilla WebThings gateway on Raspberry Pi; 2) Use of Hyperledger Fabric Blockchain to secure the data and allow for implementation of legal restrictions through software. The proposed user-centric wearables architecture enhances data privacy through edge and fog computing, whilst opening up Smart Homes to General Data and Protection Regulations (GDPR)-inspired “data portability” and personal data monetization opportunities.

Keywords
Wearables, COVID-19, Web of Things, Blockchain, Single Board Computers

1 Introduction

The emergence of COVID-19 in Wuhan in December 2019 crippled the global health system as evidenced by incidences of infected patients, shortages of hospital wards, artificial ventilators and face masks. World Health Organisation (WHO) guidelines to isolate or quarantine COVID-19 infected or exposed individuals respectively, heightened the need for remote health monitoring alternatives. As a way to respond to the need for remote healthcare models, numerous IoT innovations including wearable devices, drones, robots, IoT buttons and smartphone applications are being explored to fight COVID-19 at different phases of the pandemic including, early diagnosis, quarantine time and after recovery (Nasajpour *et al.*, 2020). IoT-powered wearable devices present an affordable physiological and biochemical parameters remote monitoring alternative. This alternative has the potential to complement current health facilities and effectively deal with logistical challenges associated with mass testing.

The global wearables market is dominated by four firms namely: Fitbit, Apple, Garmin and Xiaomi. These market leaders utilize ecosystems that are vertically integrated which results in vendor lock-in, thus limiting the option of selecting different devices from a variety of vendors. Situations in which consumers are able to buy different devices from different vendors using closed, proprietary protocols may result in challenges in interoperating the gadgets.

In the global south, which is characterised by low disposable income, cost is a determining factor when acquiring technology. However, the desire to buy low-cost devices usually leads consumers to purchasing equipment from untrustworthy vendors. In addition to the security vulnerabilities associated with buying low priced devices, consumers will also encounter interoperability challenges as most low technology vendors do not utilise universal standards when developing their products.

Ordinarily, a smart home IoT architecture is comprised of sensing and actuation devices as well as wearables that are connected within a local home network through a gateway. A gateway, which connects the local devices to the fog or cloud network, is a good point to implement security and interoperability of IoT devices within households.

Recently, Blockchain technology has been implemented in varying use cases beyond the cryptocurrency. One such use case is in providing an effective security layer on the top of data management infrastructures. Another security related use case is the use of private Blockchain to prove whether installed devices are not invading consumers' privacy by sending unauthorised information from the local network. Raspberry Pi single board computer is an inexpensive IoT gateway alternative that can be used to interoperate devices through software. It is a useful candidate to host private Blockchain in implementing the security use cases as well as to execute smart contracts.

There is therefore a need to develop a Blockchain-secured IoT application that will connect health wearables that collect data in order to help detect the prevalence of COVID-19 before symptoms appear. Such a system must allow for the interoperability whilst identifying incidences of security violations that involve invading owners' privacy.

1.1 Objectives

The specific objectives of the study include:

i. To develop a system architecture that will ensure personal medical data collected within a Smart Home is secured through customizable privacy settings and implements data portability.

ii. To customize an Internet of Things platform that is able to connect and collect data from health wearable devices within households.

iii. To utilize the Mozilla WebThings to interoperate numerous wearable gadgets using a Raspberry Pi as gateway.

iv. To record data collected by the IoT gateway on a private Blockchain allowing for implementation of legal restrictions in smart contracts.

2 Literature Review

A non-exhaustive list of conventional diagnostic tools to detect COVID-19 include next generation sequencing, quantitative reverse transcription-polymerase chain reaction (rRT-PCR), Point of care testing (POCT), vitro diagnostics (IVDs) (Kumar *et al.*, 2020). A major obstacle of these diagnostic tools is the requirement to meet qualified health personnel within health facilities, which is currently a challenge given the lack of capacity of the existing health infrastructure. Another challenge of conventional COVID-19 detection methods is the lack of accuracy as reflected by numerous cases of false-positive results (Surkova, Nikolayevskyy and Drobniewski, 2020) . Whilst mass testing for COVID-19 became a necessity during the public health crisis, costs prevented developing countries from sustainably testing citizens (Songok, 2020) . According to (Radin *et al.*, 2020) collecting and collating physiological and activity data within a population has the potential to enhance the timeliness and accuracy of public health interventions.

2.1 Web of Things Architectures and Integration Patterns

The Web of Things (WoT) paradigm is an attempt to solve scalability and interoperability challenges of IoT by employing the Web as the application layer of IoT. Since IoT devices exist in different form factors and processing capabilities, integration of IoT devices into the Web requires different integration architectures. As standardization efforts of WoT continue to evolve and mature three integration patterns that define where to implement the Web Application Programming Interface (API) in order to connect IoT devices to the Web, have emerged. The three patterns include direct integration pattern, gateway integration pattern and the cloud integration pattern (Dominique Guinard;Trifa Vlad, 2016, p. 175 – 213)

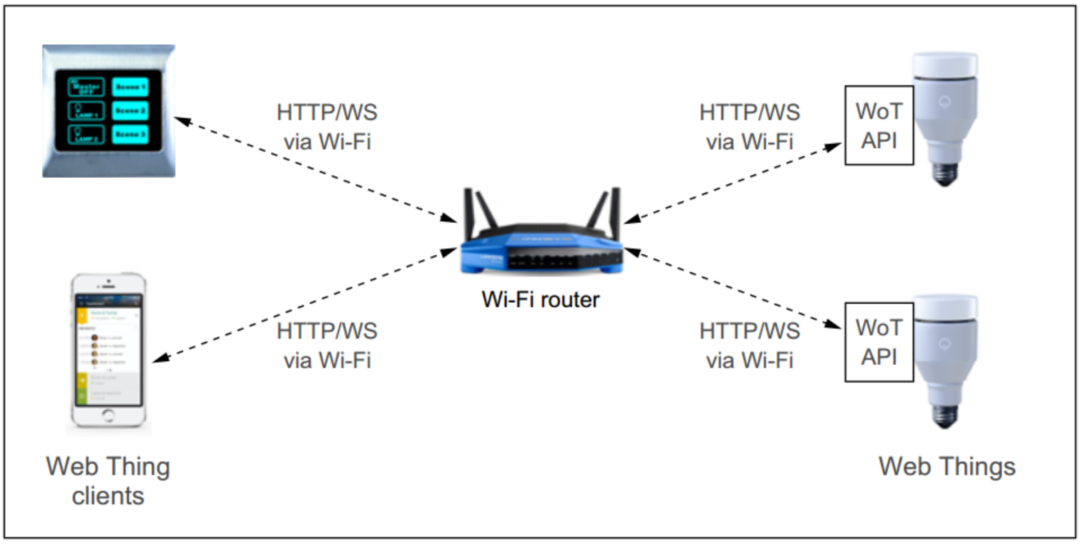

Figure 1: Direct Integration Pattern. The pattern is suitable for Smart Home use cases in which devices are not battery-powered and low-latency is important. Nodes are accessible through Internet protocols and they host web servers. Reprinted from Building the Web of Things (1st ed., p.177), by D. Guinard and V. Trifa, 2016, Manning. Copyright http://model.webofthings.io.

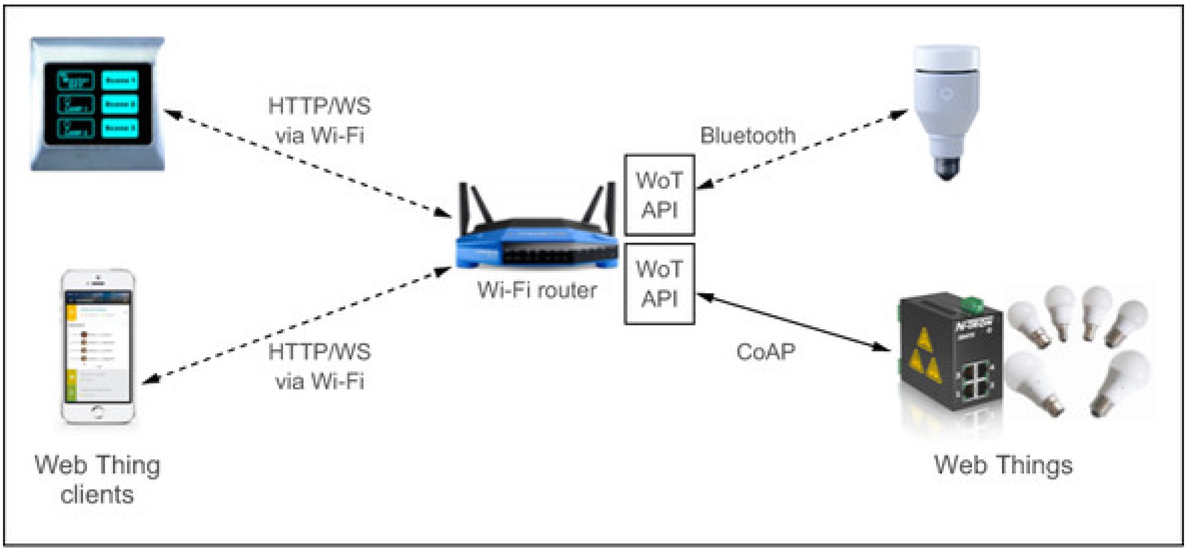

Figure 2: Gateway Integration Pattern. This architecture is suitable for nodes that utilize low-power protocols including Bluetooth and ZigBee. Devices are accessible through WoT gateways that expose devices' functionality and translate messages from constrained protocols such as CoAP that utilises UDP, into HTTP. Reprinted from Building the Web of Things (1st ed., p.195), by D. Guinard and V. Trifa, 2016, Manning. Copyright http://model.webofthings.io.

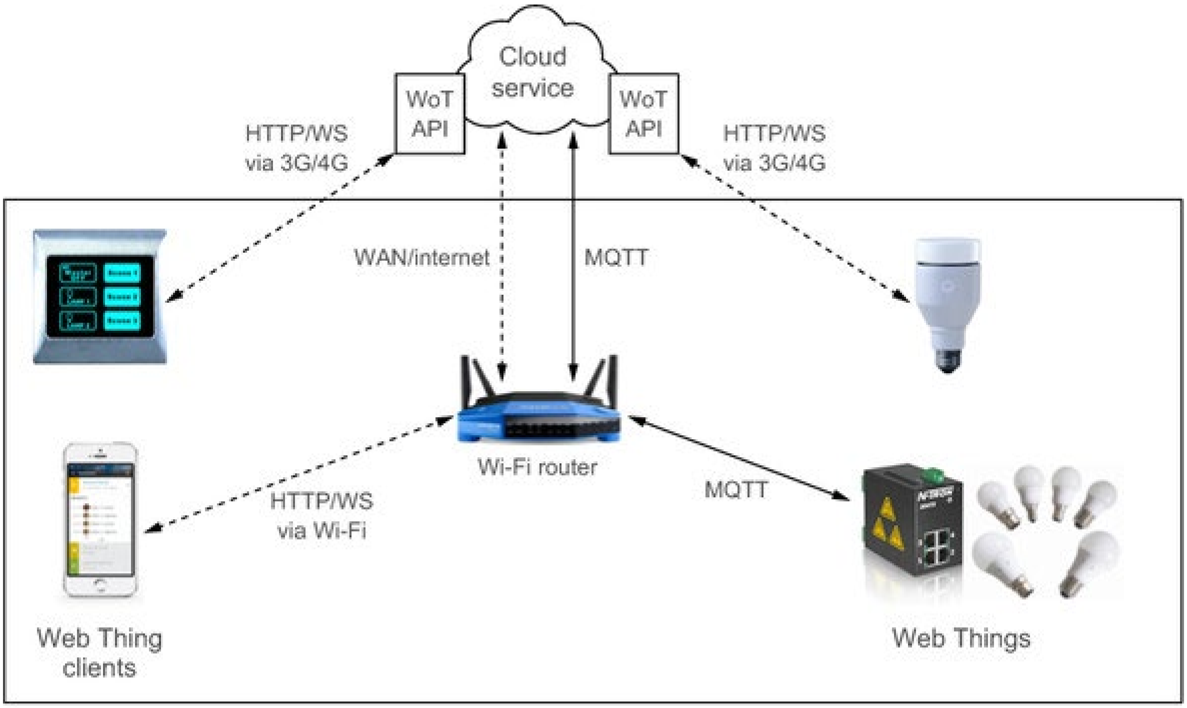

Figure 3: Cloud Integration. This pattern is an extension of the Gateway Integration Pattern suited for use cases with scalable data storage and processing requirements. Devices access the remote cloud gateway through the Internet. Reprinted from Building the Web of Things (1st ed., p.199), by D. Guinard and V. Trifa, 2016, Manning. Copyright http://model.webofthings.io.

2.2 Wearables for Early Presymptomatic and Asymptomatic Detection of COVID19

Persons infected by the highly contagious Severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV-2), the virus that causes COVID-19, can generally be classified into five categories: asymptomatic, mild, moderate, severe and critical. Asymptomatic persons, though infected with the virus, never exhibit the symptoms. Asymptomatic SARS-CoV-2 patients pose huge challenge as they can infect others unknowingly. A study (Oran and Topol, 2020) approximates asymptomatic persons accounting for 40% to 45% of SARS-CoV-2 infections. Presymptomatic patients, who do not initially show signs of COVID-19 even though infected, also risk spreading the virus benignly.

Numerous research initiatives had been exploring the use of wearables in digital health before the COVID-19 pandemic surfaced. One institution leading efforts in precision medicine is the Stanford Healthcare Innovation Lab. With more than six hundred and ninety three (693) publications, the innovation lab pioneered the multi-omic, longitudinal baseline profiling approach to healthcare, deriving precision medicine from both biology and data science. In one study (Li *et al.*, 2017) forty adults were tracked through wearable technology to obtain genomic and biochemical clues into disease and health. Big data evidenced by 250 000 bodily measurements per person, per day was able to detect early infections from changes in heart rate. Over a period of two years the study morphed into a more rigorous evaluation of seven of the wearables. One volunteer had the sensors strapped to his wrist, belt, shirt and finger, continuously measuring his steps, physical activity, calories, heart rate, skin temperature, sleep, blood oxygen, exposure to radiation, and weight. In one incident the volunteer was able to proactively detect changes in heart rate and consulted a physician who assisted in dealing with a Lyme infection.
Challenges associated with identifying early asymptomatic and presymptomatic persons, inadequate healthcare coupled with inadequate infrastructure and high health costs have necessitated the need for remote healthcare and detection methods that use different types of wearable computing.

Numerous COVID-19 studies are using different types of wearables from multiple vendors to measure physiological parameters associated with the disease. Wearable vendors and brands including Fitbit, Oura, Apple, WHOOP, Beurer, AIO, Garmin, VivaLNK sell gadgets ranging from $30 up to $579 (Seshadri *et al.*, 2020). Whilst the most comprehensive studies are combining high end technology and big data, other studies are employing simple technology including pulse oximeters (Zhuo *et al.*, 2020) to detect potential infections.

2.3 Wearable Computing Security Vulnerabilities

A typical wearable computing architecture is characterised by the devices' data moving across short, unlicensed Body Area Networks (BAN) and Personal Area Networks (PAN) to a monitoring hub within the patient's home. The monitoring hub will in turn offload data to a broadband network which then routes it to a third party cloud analytics provider for further processing. Processing of data within the cloud is made necessary by the fact that most wearables are constrained in terms of memory and processing power. The constrained form factor and battery size of wearable devices means there are fewer options to implement standard security on normal computing platforms.

Whilst prominent wearables brands including Fitbit, Garmin, Apple, Xiaomi and Samsung provide some decent level of security safeguards, these gadgets are beyond the reach of most citizens in developing countries. Global south citizens end up settling for wearable clones and counterfeits that suit their pockets. Clones and counterfeits provide an avenue for security vulnerabilities to be exploited (Mark M. Tehranipoor, 2017) According to (Young, 2019) the healthcare sector has been affected by counterfeit device manufacturers that abuse the medical community's universal barcode, the Unique Device ID (UDI). Unscrupulous device manufacturers mislead the medical community by attaching UDI values of newer devices on old devices compromising the security of the devices. Vulnerabilities arise when, for example, a newer patch is applied to an older device leading to potential incidents of bricking the device, opening up vulnerabilities and malfunctioning of the device.

Table 1: Security Vulnerabilities of Mobile Devices. Threats related to wearable and mobile devices to the likelihood of occurrence (Franklin et al., 2020) :

Threat Event	Vulnerability	Category	Threat Source	Severity	Likelihood
Sensitive information is intercepted from a mobile device	Lack of confidentiality protection or poor cryptography	Confidentiality	Adversarial	EMS: Moderate Fire: Low LE: High	High
Accidental disclosure of information via a shared device or resource	Lack of properly implemented access controls	Confidentiality	Accidental	EMS: Low Fire: Low LE: Mod	Mod
Individual accesses information and services via a lost or stolen public safety device	Lack of physical access control, lack of user authentication to device	Confidentiality	Adversarial, Human error	EMS: Mod Fire: Low LE: High	Mod
Pre-installed spyware on device accesses sensitive data	Lack of supply chain controls	Confidentiality	Adversarial	EMS: Mod Fire: Low LE: High	Low
A denial of service or other technical attack, blocks communications	Protocol not designed to withstand jamming attacks, lack of available spectrum	Availability	Adversarial, Accidental	EMS: High Fire: High LE: High	Mod

A denial of service or other technical attack, blocks communications	Protocol not designed to withstand jamming attacks, lack of available spectrum	Availability	Adversarial, Accidental	EMS: High Fire: High LE: High	Mod

EMS: Emergency Medical Service; Fire: Fire Service; LE: Law Enforcement

The table 1 shows that the most prevalent security threat to wearables and mobile devices is confidentiality and the likelihood is mostly high. Whilst confidentiality is a duty of the producer it is closely related to privacy which is the consumer's "right to be let alone". Enforcing confidentiality requirements to certified wearable device manufacturers is made possible through regulations such as European Union's General Data Protection Regulation (GDPR). However countries in the Global South are yet to have robust public policy that protects citizens using IoT and wearable devices, similar to GDPR. Consequently consumers of wearable devices in developing societies have easier access to uncertified alternatives, and therefore need tools that ensure they are in control of their own private settings when they purchase cloned, uncertified wearables within unregulated jurisdictions in the Global South.

2.4 Interoperability Challenges of IoT and Wearables

As vertical IoT ecosystems represent the most common IoT model, challenges to interoperate devices from different verticals increase. Led by Standards Developing Organisations (SDOs) that include the Internet Engineering Task Force (IETF) (Morabito and Jimenez, 2020) , protocols that ensure comprehensive, interoperable and streamlined IoT stacks are under development. The original Internet protocols were not designed to work for constrained IoT devices. Newer IoT-specific protocols that include Constrained Application Protocol (CoAP), IPv6 over Low power WPAN (6LoPAN), Constrained Binary Object Representation (CBOR) are under development. Efforts are also under way to implement semantic interoperability which transparently enables devices to be discoverable through metadata (context-based) and/or device values (content-based) (Cimmino and Poveda-villalón, 2020)

The World Wide World is credited for bringing the Internet out of research institutions into the public domain as it allowed users to navigate different types of resources. The W3C (Matthias Kovatsch, Ryuichi Matsukura, Michael Lagally and Kunihiko Toumura, 2020) is developing a set of Web of Things (WoT) standards in an attempt to solve IoT interoperability issues of different platforms and application domains. WoT will enable smart devices to communicate with web applications. Mozilla developed the WebThings gateway that will integrate smart things in a vendor neutral way. WebThings provides a Representational State Transfer (REST) Application Programming Interface (API) (Mozilla, 2020) that adheres to the WoT standard. The WebThings gateway is designed for household use as it can be deployed on the Raspberry Pi single board computer.

2.5 Private Permissioned Blockchain on Single Board Computers

Blockchain is a Distributed Ledger Technology (DLT) that records transactions between two parties in an immutable and verifiable manner. The first use of blockchain was in the Bitcoin cryptocurrency. However various efforts are exploring the use of DLT technology in numerous use cases that include smart homes (Dorri *et al.*, 2017), (Xue, Xu and Zhang, 2018), (Lee *et al.*, 2020), (Khezr, Yassine and Benlamri, 2020). Additionally, the implementation of blockchain for healthcare highlights the potential of this technology to provide privacy for confidential and sensitive patient data, as already covered by studies such as (Dwivedi, Srivastava and Dhar, 2019)

Currently Raspberry Pi is used beyond its initial intended use as an educational tool. The application of Raspberry Pi in different domains has enhanced Blockchain researches who are using it to deploy private Blockchain. For instance, (Fernando, 2019) developed an Ethereum private Blockchain application running on a Raspberry Pi for a pharmaceuticals use case.

However the hype associated with Blockchain technology has discredited its usefulness in a number of situations. Technology opportunists have been criticised on several occasions for abusing DLT by turning Blockchain into a "solution looking for a problem". (Wust and Gervais, 2018) developed a methodology using a flow chart to evaluate the usefulness of certain types of Blockchain. The flow chart works by asking a series of questions that will confirm if a particular problem is best suited to be solved using. I also prescribes themost appropriate type of Blockchain (see Figure 4).

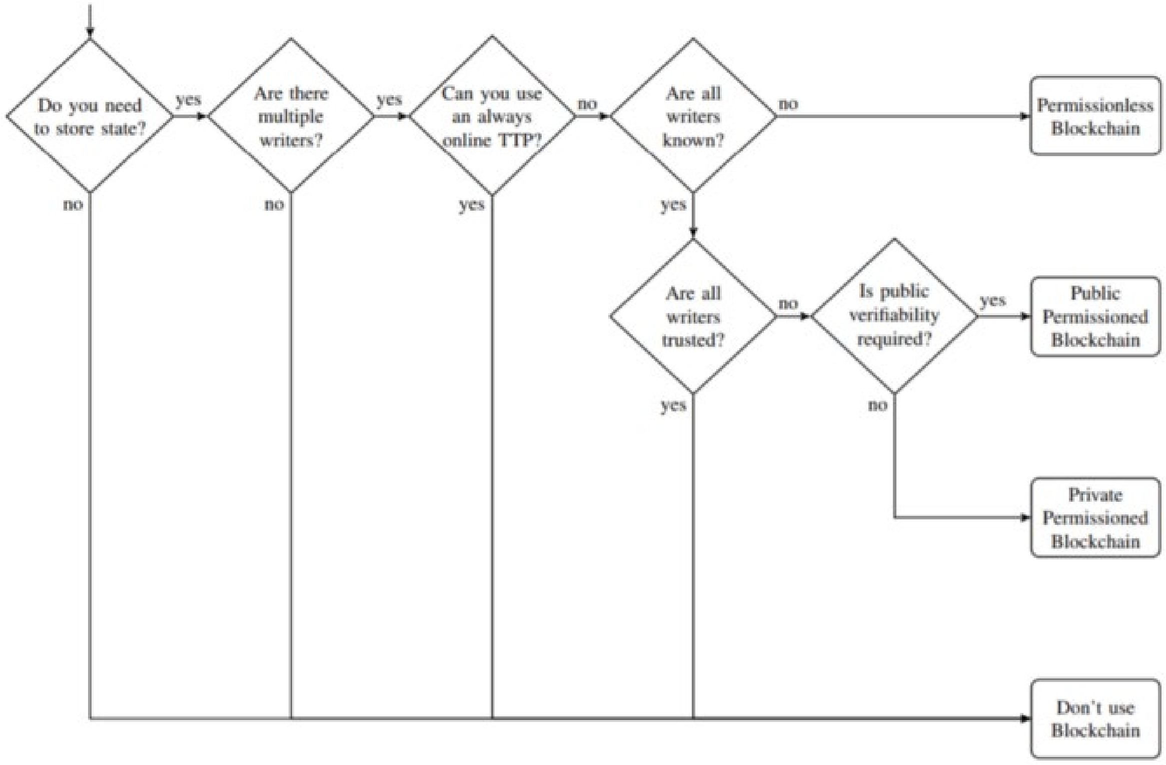
Do you need to store state?
yes
no
Are there multiple writers?
yes
no
Can you use an always online TTP?
no
yes
Are all writers known?
no
yes
Permissionless Blockchain
Are all writers trusted?
no
yes
Is public verifiability required?
yes
no
Public Permissioned Blockchain
Private Permissioned Blockchain
Don't use Blockchain

Figure 4: Evaluating Appropriateness of Blockchain for specific use cases.

2.6 Summary and Synthesis

Recent work reveal different efforts to develop “Hospital-at-home” solutions utilising Smart Homes’ IoT and wearables technology to combat the COVID-19 disease (Seshadri et al., 2020; Nasajpour, M. et al., 2020). Most of the studies make use of wearable devices from the traditional ecosystems include Fitbit, Apple, Garmin and Xiaomi. Whilst these systems have guaranteed quality they are out of reach for most homes in developing communities.

In the case of homes in the global south that access average quality and inexpensive brands, there is a risk that different brands might not work together. There is need therefore to explore inexpensive ways to provide interoperability between cheap wearables beyond the current per-vendor integrations.

Incidences have been recorded in which wearable devices leak data or are used to attack other devices. Thus, Blockchain technology can address this issue, as a mechanism to monitor the traffic generated by wearables at the same time that provide tools to preserve privacy within smart homes.

3 Testbed and Adapted Architectural Design

The initial prototype was submitted as ISOC Zimbabwe's submission for 2018 Chapterthon whose theme was “IoT Security”. It consists of a Hyperledger Fabric application to record data shared by IoT gadgets within a connected home using Blockchain technology. It also has a user application (based on NodeJS), that will allow home owners to query the Blockchain for suspicious, unauthorised sharing of private data. Instructions to replicate the setup are available of the Github repository (Makerspace, 2018)

3.1 Choice of a Traditional Database or Blockchain

The first step in deploying the study objective 4, involved evaluating the most appropriate storage media for recorded data. The flowchart-based methodology developed by (Wust and Gervais, 2018) was utilised in answering questions as shown:

i. Is there need to write state?
Yes, Wearables need to record measurements and destination to write to.

ii. Are there multiple writers?
Yes, Multiple wearables will be measuring various activity, physiological and biochemical parameters.

iii. Is there an Online Trusted Third Party?
No, the system uses an offline-first paradigm

iv. Are the writers known?
Yes, every wearable added in the Smart Home will be known

v. Are the writers trusted?
No, because Zimbabwe does not have a IoT Policy that vets IoT hardware and Smart Home consumers occasionally buy unbranded, cheap wearables.

vi. Is there need for verifiability?
No, the system prioritises privacy of patient data over transparency

Answers to these questions confirmed the suitability of utilizing a private Blockchain to augment data storage for the application.

3.2 Architectural Overview

The overall system can be viewed as three subsystems namely (1) IoT; (2) Blockchain, and (3) Fog subsystems. Figure 5 represents the proposed system architecture containing the following components:

- IoT Subsystem: this layer is comprised of wearable devices, a Wazihub LoRa gateway and the WebThings gateway software. A full list of supported gateway hardware, adapter and devices is found at this resource (Mozilla, 2020). D A Wazihub LoRa gateway that supports LoRaWAN and is capable of sending and receiving messages from up to 200 devices.
- Blockchain subsystem: a permissioned distributed ledger framework implemented as a docker container. The susbsystem provides identity management, event management and smart contracts.
- Fog subsystem: a cluster of Raspberry Pis implementing k3s Kubernetes distribution that provides data aggregation services.

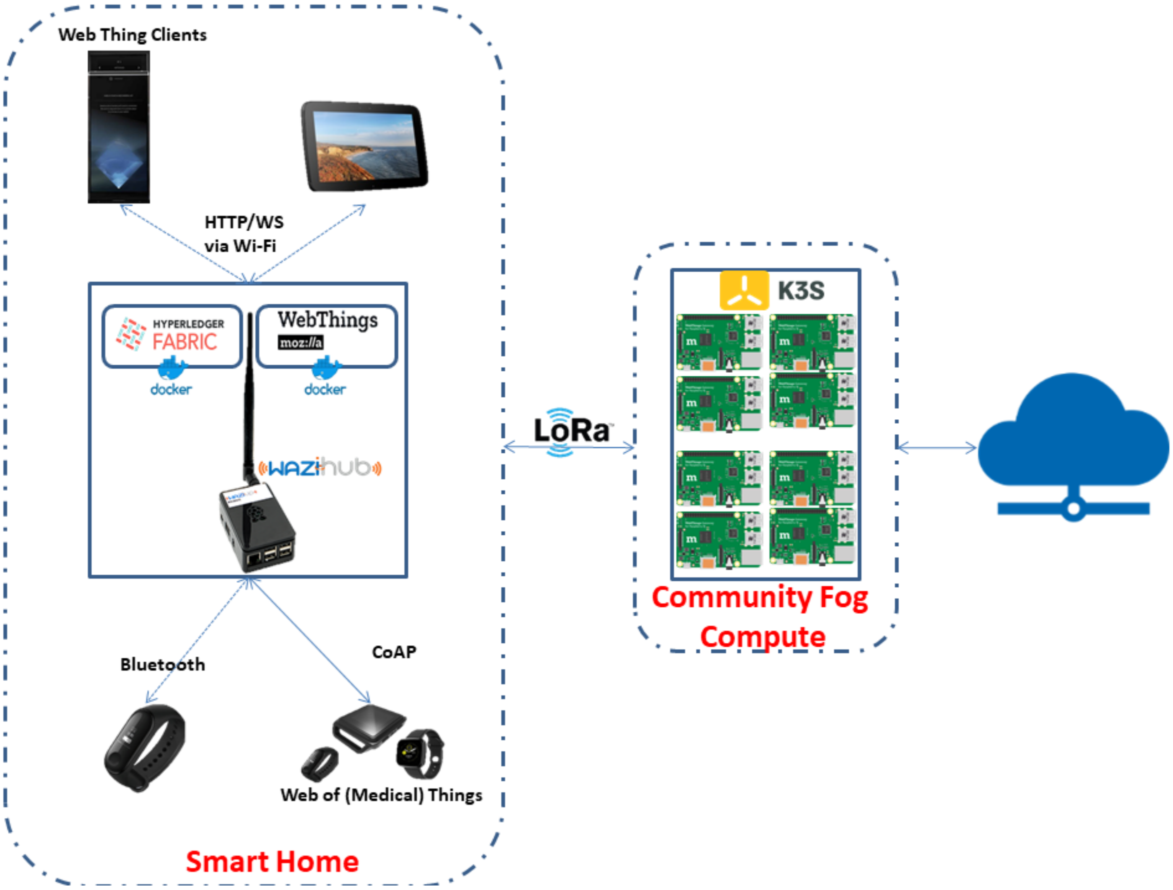

Figure 5: System Architecture

4 Conclusion

The paper presents an architecture that can be implemented to provide reliable data privacy and portability for wearables. As efforts are underway globally to contain the CoVID-19 pandemic the testbed was adapted to a smart home to explore a privacy-preserving web of things and Blockchain application. As conventional IoT and wearables solutions are out of reach, we opted for the open Mozilla WebThings as a platform able to connect a myriad of health wearables. Whilst the IoT operability is far from perfect the WebThings' open nature provides room for further customization. On the Blockchain layer, the system ensures immutable observation and the recording of all outgoing traffic. Future improvements are needed to automate the triggering of alerts on the private Blockchain. We also consider it imperative to add smart contracts to notify owners of incidences of data leaks.

References

Cimmino, A. and Poveda-villalón, M. (2020) 'eWoT : A Semantic Interoperability Approach for Heterogeneous IoT Ecosystems Based on the Web of Things'. doi: 10.3390/s20030822.

D. Guinard and V. Trifa (2016) *Building the web of things: with examples in node. js and raspberry pi: Manning Publications Co., 2016.* Manning.

Dorri, A. *et al.* (2017) 'Blockchain for IoT Security and Privacy : The Case Study of a Smart Home', (March). doi: 10.1109/PERCOMW.2017.7917634.

Dwivedi, A. D., Srivastava, G. and Dhar, S. (2019) 'A Decentralized Privacy-Preserving Healthcare', pp. 1–17. doi: 10.3390/s19020326.

Fernando, E. (2019) 'Blockchain Technology Implementation In Raspberry Pi For Private Network', (May 2020). doi: 10.1109/SIET48054.2019.8986053.

Franklin, J. M. *et al.* (2020) 'Security analysis of first responder mobile and wearable devices'. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8196.pdf.

Khezr, S., Yassine, A. and Benlamri, R. (2020) 'Blockchain for Smart Homes : Review of Current Trends and Research Challenges Blockchain for smart homes : Review of current trends and research challenges R', *Computers and Electrical Engineering*, 83(January), p. 106585. doi: 10.1016/j.compeleceng.2020.106585.

Kumar, R. *et al.* (2020) 'COVID-19 diagnostic approaches: different roads to the same destination', *VirusDisease*, 31(2), pp. 97–105. doi: 10.1007/s13337-020-00599-7.

Lee, Y. *et al.* (2020) 'A blockchain - based smart home gateway architecture for preventing data forgery', *Human-centric Computing and Information Sciences*. doi: 10.1186/s13673-020-0214-5.

Li, X. *et al.* (2017) 'Digital Health: Tracking Physiomes and Activity Using Wearable Biosensors Reveals Useful Health-Related Information', *PLoS Biology*, 15(1), pp. 1–30. doi: 10.1371/journal.pbio.2001402.

Makerspace, S. P. M. I. (2018) *Proof of Privacy*. Available at: https://github.com/st-peters-mbare-iot-makerspace/proof-of-privacy.

Mark M. Tehranipoor, U. G. and S. B. (2017) *Invasion of the Hardware Snatchers: Cloned Electronics Pollute the Market Fake hardware could open the door to malicious malware and critical failures*, *IEEE Spectrum*. Available at: https://spectrum.ieee.org/computing/hardware/invasion-of-the-hardware-snatchers-cloned-electronics-pollute-the-market.

Matthias Kovatsch, Ryuichi Matsukura, Michael Lagally, T. K. and Kunihiko Toumura, K. K. (2020) *Web of Things (WoT) Architecture*. Available at: https://www.w3.org/TR/2020/REC-wot-architecture-20200409/.

Morabito, R. and Jimenez, J. (2020) 'IETF Protocol Suite for the Internet of Things: Overview and Recent Advancements', *IEEE Communications Standards Magazine*, 4(2), pp. 41–49. doi: 10.1109/MCOMSTD.001.1900014.

Mozilla (2020a) *Supported Hardware*. Available at: https://github.com/WebThingsIO/wiki/wiki/Supported-Hardware.

Mozilla (2020b) 'WebThings REST API'. Available at: https://iot.mozilla.org/wot/.

Nasajpour, M. *et al.* (2020) 'Internet of Things for Current COVID-19 and Future Pandemics: An Exploratory Study'. Available at: http://arxiv.org/abs/2007.11147.

Oran, D. P. and Topol, E. J. (2020) 'Prevalence of Asymptomatic SARS-CoV-2 Infection : A Narrative Review', *Annals of internal medicine*, 173(5), pp. 362–367. doi: 10.7326/M20-3012.

Radin, J. M. *et al.* (2020) 'Harnessing wearable device data to improve state-level real-time surveillance of influenza-like illness in the USA: a population-based study', *The Lancet Digital Health*, 2(2), pp. e85–e93. doi: 10.1016/S2589-7500(19)30222-5.

Seshadri, D. R. *et al.* (2020) 'Wearable Sensors for COVID-19: A Call to Action to Harness Our Digital Infrastructure for Remote Patient Monitoring and Virtual Assessments', *Frontiers in Digital Health*, 2(December 2019), pp. 1–11. doi: 10.3389/fdgth.2020.00008.

Songok, E. (2020) 'A locally sustainable approach to COVID-19 testing in Africa', *The Lancet Microbe*, 1(5), p. e197. doi: 10.1016/s2666-5247(20)30118-x.

Surkova, E., Nikolayevskyy, V. and Drobniewski, F. (2020) 'False-positive COVID-19 results: hidden problems and costs', *The Lancet Respiratory Medicine*, 2(20), pp. 19–20. doi: 10.1016/s2213-2600(20)30453-7.

Wust, K. and Gervais, A. (2018) 'Do you need a blockchain?', *Proceedings - 2018 Crypto Valley Conference on Blockchain Technology, CVCBT 2018*, (i), pp. 45–54. doi: 10.1109/CVCBT.2018.00011.

Xue, J., Xu, C. and Zhang, Y. (2018) 'Private Blockchain-Based Secure Access Control for Smart Home Systems', 12(12), pp. 6057–6078.

Young, G. (2019) *Cybersecurity Leaders Are Talking A Lot About Counterfeit Devices*, *Simply Security*. Available at: https://blog.trendmicro.com/cybersecurity-leaders-are-talking-a-lot-about-counterfeit-devices/.

Zhuo, K. *et al.* (2020) 'Stress and sleep: A survey based on wearable sleep trackers among medical and nursing staff in Wuhan during the COVID-19 pandemic', *General Psychiatry*, 33(3), pp. 1–6. doi: 10.1136/gpsych-2020-100260.

Biography

Solomon H. Kembo is a lecturer in the Department of Computer Engineering at the University of Zimbabwe. He is also the founder of St Peters Mbare IoT Makerspace, a community project empowering youths from disadvantaged communities to explore open technology in solving their local problems. His current research work focuses on decentralised architectures and technologies targeted at digitally excluded and unconnected communities including edge and fog computing. He is also involved with IoT interoperability efforts as a member of Internet Research Task Force's Work on IoT Semantic/Hypermedia Interoperability (WISHI).

Patience Mpofu is a lecturer in the Department of Computer Engineering at the University of Zimbabwe. She is also an instructor at founder of St Peters IoT Makerspace, a community project empowering youths from disadvantaged communities to explore open technology in solving their local problems.

Brighton T. Mukorera has extensive experience in Blockchain platforms integrations Bitcoin, Ethereum, Waves and Hyperledger. A former Lead Engineer at Golix, a crypto currency exchange, he is currently doing research in the use of Blockchain for decentralized education platforms**.** He runs a start-up that operates a Gaming and Design Studio with a vision to promote development of Africa-centric games and animations. The start-up tells African stories through games.

Saulo Jacques has a PhD in ecosystem ecology with experimental research testing the impact of climate changes on the microbial community and the nutrient cycle. Former member of Aquatic Ecology Lab of Federal University of Rio de Janeiro and from the Bromeliad Working Group of the University of British Columbia currently is the research officer of Hacking Ecology, a group of developers and researchers building open source and decentralized tools for environmental research and community science.