CYBERCASTLE

website: http://www.cybercastlehealth.com/

Rasmus Häggkvist, Sneha Pullanoor, Ouahib Timoulali,
Subaita Rahman, Ma. Rizza Cerilles, Max Kenning

THE TEAM

Rasmus H. (Lead)
Norrbotten, Sweden

Research, Design, Outreach

Sneha P.
Mumbai, India

Design, Research, Prototyping

Ouahib T.
Kenitra, Morocco

Software dev, Encryption, Research

Subaita R.
Toronto, Canada

Software dev, Prototyping, Outreach

Ma. Rizza C.
Cavite, Philippines

Research, Market, Business

Max K.
Stockholm, Sweden

Web dev, Design, Research

PROJECT OVERVIEW

CURRENT PROBLEMS IN HEALTH CARE

- IoMT devices are easy targets for hackers
- A breach on an IoMT device without secure transportation could lead to exposed sensitive patient data
- There is no sufficient way of guaranteeing the integrity of the data being transported

STATE OF THE ART SOLUTION

- Blockchain will secure data flow between an IoMT device and relevant parties
- With well designed data architecture, breaches can be severely reduced

EXPERT EVALUATION

- 93.33% of the contacted experts agreed that our product will be useful when implemented
- The solution seems to have potential for further application in other medical areas

THE PROBLEM

PROBLEM

DATA BREACHING OF INTERNET OF MEDICAL THINGS (IOMT) IN THE HEALTHCARE SECTOR

Data breaches cost the healthcare industry approximately $5.6 billion a year and an average of one health data breach per day in 2018, and affected more than 27 million patient records (Becker's Hospital Review). In 2018, when comparing a range of work sectors that included education, healthcare, general professions, and finance, healthcare entities' portion of all breaches and security incidents was at 41 percent—the highest percentage of any sector.

Amid an aging population and rising healthcare costs in Asia, more telehealth solutions are coming to market to help doctors collect data on patients who may live in rural areas without hospitals, or elderly patients who can't travel. The addition of more IoT devices could increase the number of breaches for hospitals as most devices are not built with security in mind. It's crucial, then, for healthcare systems to understand the vulnerabilities of IoMT tools and how to protect them. One of the major security problems is that IoT devices serve as an easy gateway to access personal information, and with 420 million connected medical devices in deployment with over 60 percent exposed to some degree of risk.

BACKGROUND

WHY HEALTHCARE

Hackers tend to steal medical records because they contain a patient's full name, address history, financial information, and social security numbers—which is enough information for hackers to take out a loan or set up a line of credit under patients' names, according to Computerworld. Some hackers sell personal information on the dark web. Buyers might use the information to create fake IDs to purchase medical equipment or drugs, or to file a false insurance claim. Furthermore, access to personal information could lead to Identity theft which leads to fraud. In addition to this, bank accounts can be accessed.

But for most hospitals, it is not economically feasible for them to invest into better secured devices. Most organizations are trying to finance and prioritize many different areas, hence deciding between security or a new MRI machine, for instance, can be hard, which can make devices on a network easy targets for outside actors.

HOW IOT COMES INTO PLAY WITH DATA BREACHES

Continuous glucose monitors (CGMs) generate a substantial amount of data by collecting interstitial glucose readings every 5 minutes, which is an indicator of the patient’s blood glucose (BG). Patients with diabetes have an extremely high need for secure information flow to display glucose information and sync with health records at hospitals when sensor and actuator information is transmitted wirelessly through connected devices. The FDA is concerned that, due to cybersecurity vulnerabilities identified in the device, someone other than a patient, caregiver or health care provider could potentially connect wirelessly to a nearby CGM and access medical records.

OUR SOLUTION

HYPOTHESIS

PREVENT THE USE OF CGMS AS A GATEWAY BY TRANSPORTING MEDICAL DATA USING BLOCKCHAIN

We expect that integrating Blockchain on the IoMT for the users of Continuous Glucose Monitoring (CGM) will provide a safe, simple, and secure delivery of information between the clients. With the rise of a global pandemic, it shows how important at-home monitoring can be when it comes to saving lives and mitigating hospital surges. With our solution, we can ensure the user's trust that their data is safe and secure with the rise and need of a remote monitoring system to be used in homes and hospitals.

METHODS

LITERATURE BASED RESEARCH:

We brainstorm ideas for our blockchain system, to research relevant cybersecurity and medical literature and studies such as:

- Comparison of encryption methods
- Cloud-based storage systems
- Predictive ML algorithms to prevent future attacks

OUTREACH BASED RESEARCH:

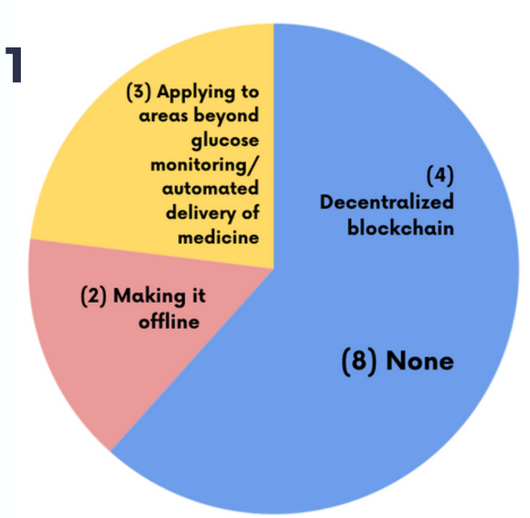
We reached out to a variety of experts across the globe in the field of cybersecurity and blockchain to gather advice for our solution by:

- Conducting outreach to people for their feedback regarding medical and cybersecurity aspects. The survey garnered answers from professionals, professors and (2) NYAS Junior Academy mentors.
- Sending an online survey to professors and industry professionals related to the field of technology or medical science

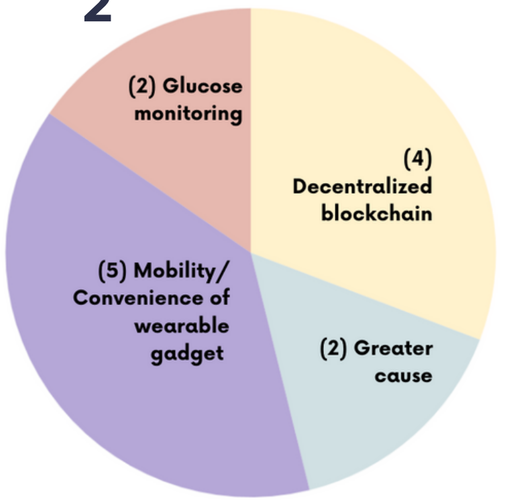
FEEDBACK SURVEY:

1. **What aspects of this solution were most useful or valuable?**
2. **How would you improve our solution? Any comments or suggestions?**
3. **Do you see yourself/someone you know using our final product?**

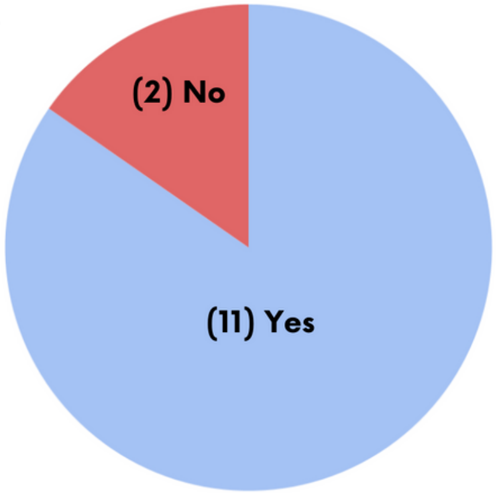
1



2



3



ADVISORY BOARD SUGGESTIONS

EVA BRUKETA

MD STUDENT AT QUEEN'S UNIVERSITY

- importance of a clear and simple user interface
- doctors' and patients' need for accurate, secure, and real-time data
- the small and quick changes can have a substantial impact when continuously monitoring glucose vitals

OLIVIA STANDISH

PROGRAM LEAD AND INCUBATOR AT THE DMZ

- suggests assumption maps, run-maps, and questionnaires
- researching on market validation and competition
- contacting the experts on insurance to clarify the industry and patients
- getting a clear view of the aspects of practical glucose monitoring

BALAJI GOPALAN

CEO, AND CO-FOUNDER OF MEDSTACK

- to understand the problem at hand in the medical community and the laws and rules that apply for each country
- to focus our business strategy towards insurance companies because they are interested in digital health
- to minimize insurance claims and reduce clients susceptible to disease

GABRIEL ZOSA

ICT AND CYBERSECURITY CONSULTANT

- building the product as a humanitarian project to lessen legal issues and build trust.
- biometrics (facial recognition) has fewer loopholes than RFID Cards
- to balance security and liberty as well as silent marketing towards insurance companies as to not attract attention from hackers

SOLUTION

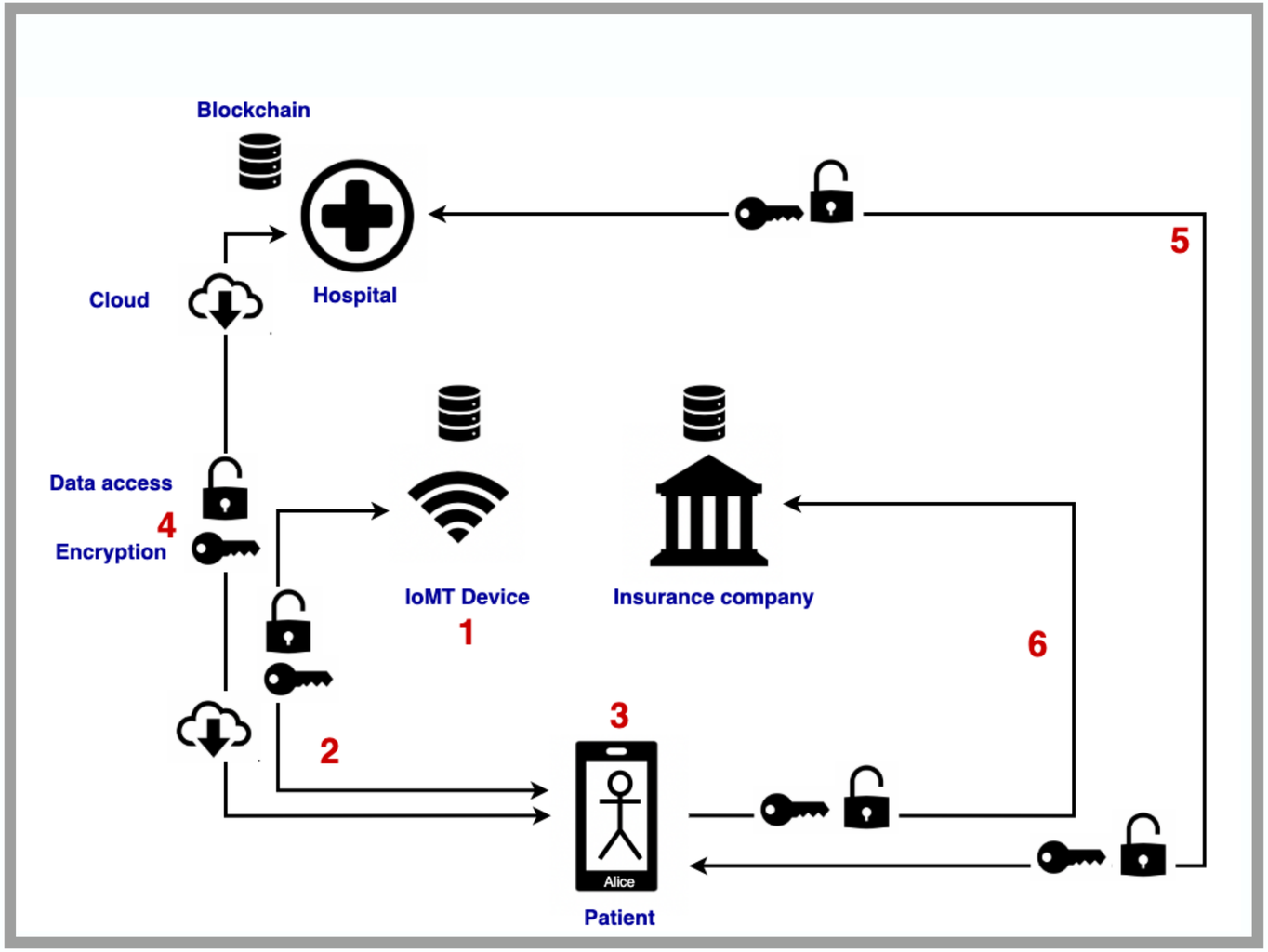
Our solution uses ethereum blockchain to record transactions of when medical records have been accessed, and by whom. The blockchain will store whether it has been accurately verified, or if a breach has occurred.

Alerts will be stored on the blockchain while user data will be stored on a biometric-secured off-chain server connected via IPFS to prevent server crash and safely distributed data. The solution guarantees the transferred data has not been tampered with and provides no pathway for hackers to access the personal data at the hospital from the IoMT.

STEPS

Here follows an explanation for the flow of data for patient Alice.

1. Alice's IOT device will continuously provide glucose data throughout the day, which is then sent via NFC (near-field communication) to her phone.
2. The data sent by the IoMT device is encrypted via oracle encryption and recorded on the blockchain. This data will then be sent to the patient's IPFS servers for temporary storage.
3. Alice wants to view her glucose data. She uses her private key to decrypt her data and access it. Additionally, her request will be recorded on the blockchain.
4. Once a week, or by request, encrypted privately stored data will be uploaded to the hospital servers via the cloud. That transaction will also be recorded on the blockchain. Our app will require consent from Alice to send information over the cloud to the off-chain database of the hospital that includes all of her EHR records. Unauthorized requests will also be stored on the blockchain and data breach alert will go off.
5. If Alice's glucose levels are unusually high, data will immediately be sent to the hospitals.
6. The insurance company gets an alert with relevant information to confirm the accident and prepare for upcoming medical expenses.



DATA ACCESS PERMISSION AND ENCRYPTION

MAIN ENCRYPTION ALGORITHMS

ORACLE ENCRYPTION ALGORITHM (OEA)

- Symmetric encryption key
- Encrypted with a master key
- Uses the encryption algorithm to encrypt and decrypt data
- Supports several industry-standard encryption and hashing algorithms, including the Advanced Encryption Standard (AES)

TRANSPARENT DATA ENCRYPTION (TDE)

- Automatic encryption of individual table columns or entire tablespaces
- When authorized users select an EHR, the data is automatically decrypted
- .Secures off-chain data regardless of theft
- Applications do not need to be modified to handle encrypted data

CHOSEN KEYS FOR EACH TRANSACTION

The patient's phone generates a symmetric encryption keys. The glucose data gets sent wirelessly to a device encrypted by the OEA. The Oracle also determines if a value meets the threshold value or not, if it does the hospital servers gets immediately notified. If not, then the data gets stored a cloud server (IPFS) to wait for further transportation to hospital off-chain storages.

Off-chain servers use TDE to encrypt and decrypt data. This provides a secure and convenient system which also is theft-proof in the unlikely case of a breach.

If the patient wants to access the data on our app, the data stored on the IPFS gets decrypted with the symmetric keys. If the doctor wants to view their records stored on the off-chain storage, they need permission from the patient to use their private key.

symmetric encryption key: type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information

CLOUD

HOW IOT DATA REACHES THE ORACLE SYSTEM

Building an API inbound/outbound oracles system will enable management of data flow from third parties. Inbound oracles bring real-world off-chain data to the blockchain (in our case glucose level data), whereas their outbound cousins do the opposite: they inform an entity outside the blockchain of an event that occurred on, we will connect this system with CGM devices or glucose monitors.

API: application programming interface is a computing interface which defines interactions between multiple software intermediaries
interoperability: ensures that doctors and specialists have the information that they need in order to provide sufficient care
REST: Representational state transfer is an architectural style that enables interoperability between computer systems through web services.

HOW THE SYSTEM INTERACTS WITH EHRS ON THE OFF-CHAIN DATABASE

The integration of data uses a robust set of universal, real-time REST APIs and a unified data model to offer read and write capabilities with any EHR without manual entry. The interoperability feature provides crucial real-time access to patient health information, including both clinical and administrative data. Data will be accessed through an inbound/outbound Oracles API system which controls the data through the blockchain network between healthcare providers and patients.

BLOCKCHAIN

WHAT IS IT?

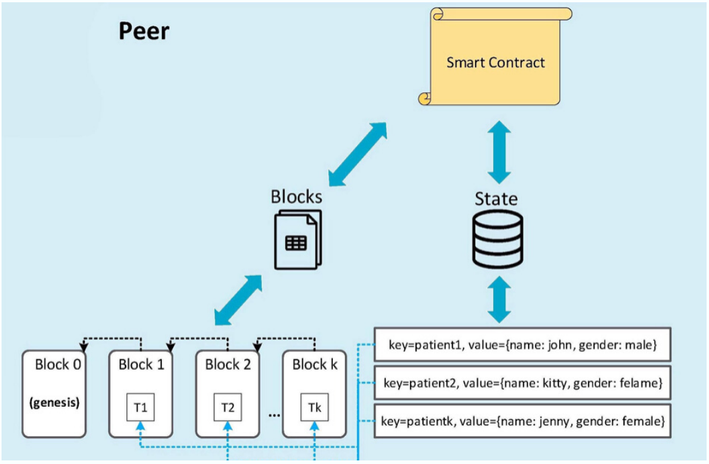
In the Blockchain, all transactions are logged. The register includes information on the date, time, participants, and amount of every transaction. Each node in the network has a full copy of the Blockchain and on the basis of cryptographic principles, the transactions are verified by Ether-miners, who maintain the ledger without being able to see the information being transported.

These principles also ensure that these nodes automatically and continuously agree regarding the current state of the ledger and every transaction in it. If anyone attempts to corrupt a transaction, the nodes will not reach a consensus and, hence, will refuse to incorporate the transaction into the Blockchain.

Ledger: a file of transactions - like a bank ledger
Ethereum: open source, public, blockchain-based distributed computing platform and operating system featuring smart contract functionality
Ether: the cryptocurrency generated by the Ethereum platform as a reward to mining individual blocks and is the only currency accepted in the payment of transaction fees

SMART CONTRACT

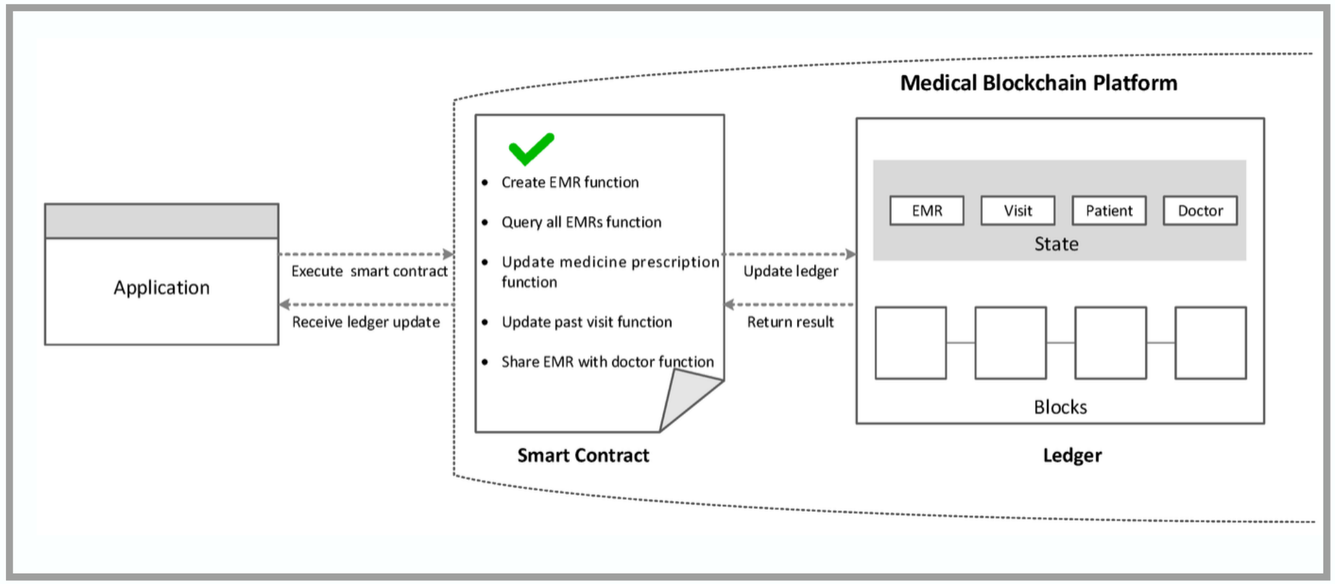
The smart contract functions as a trusted distributed application that gains its trust from the blockchain and the underlying consensus among the peers.



Smart contracts executed in an order–execute blockchain architecture must be deterministic in order to reach consensus among all of the peers. In principle, smart contracts used in these platforms are written in a non-standard, or domain-specific language (such as Solidity) so that non-deterministic operations can be eliminated.
The application running on the smart contract receives the transaction and runs different kinds of queries and updates, in turn, appends the transaction in the blocks and updates the ledger state. In the end, the ledger updating result is returned to the application as the response.

HOW BLOCKCHAIN IS IMPLEMENTED INTO THE SYSTEM

- Our system is built on a permission-less network that requires all blocks to reach a common agreement about a single data value or a single state of the network (state of the network is the data the blockchain currently holds) to ensure that a transaction is a valid transaction
- Our diagram below presents a graphical description of our blockchain architecture, where the medical blockchain preserves a complete up to date history of all transactions of medical data exchange, and failed authentication transactions



- Off-chain storage records would hold the EMR, visits, prescriptions, billing, and IoT data, which would follow an individual user for life
- The application is the doctor’s dashboard or the patient's phone and interacts with the blockchain to record any transactions being made (more detail can be seen in the prototype section).
- The end user (patient, doctor, nurse, admin, insurer etc) can submit transactional proposals to the blockchain network through the application to invoke services like the addition of IOT data onto the EMR. viewing medical data, appointments for alerts, and billing information

PROTOTYPES: SOFTWARE

CODE:

- Transactions processor functions (Figure 1) are written in JavaScript as part of a smart contract. The structure of transaction processor functions includes decorators and metadata that updates the EMR record transaction in the registry (Table 1), and then emits an event.
- Using queries, data can be easily extracted from the blockchain network, queries contain a description and a statement (Figure 2). We can use the queries to return all EMRs or specific EMRs with an identity parameter such as record identity and patient identity.

```
/**
* Share the patient record with doctor
* @param {composers.healthrecords.shareRecordWithDoctor} record - the shareRecord transaction
* @transaction
*/
async function shareRecordWithDoctor(record) {
    //payBill.patient.balanceDue -= payBill.bill.amount;
    return getAssetRegistry('composers.healthrecords.PatientRecord')
        .then(function(assetRegistry){
        record.patientRecord.doctor = record.doctorId;
        console.log(record.patientRecord.doctor);
        let factory = getFactory();
        let shareRecordEvent = factory.newEvent('composers.healthrecords', 'shareRecordWithDoctorNotification');
        shareRecordEvent.patientRecord = record.patientRecord;
        emit(shareRecordEvent);
        return assetRegistry.update(record.patientRecord);
    })
    .catch(function (error) {
    // Add optional error handling here.
    });
}
```

```
/**
 * Queries for EMR blockchain business network
 */

query selectHealthRecords {
  description: "Select all health records"
  statement:
      SELECT composers.healthrecords.PatientRecord
}

query selectHealthRecordByPatientRecordID {
  description: "Select health record by record ID"
  statement:
      SELECT composers.healthrecords.PatientRecord
          WHERE (PatientRecordID == _$PatientRecordID)
}

query selectHealthRecordByOwner {
  description: "Select health record based on their owner"
  statement:
      SELECT composers.healthrecords.PatientRecord
          WHERE (patient == _$patient)
}
```

Figure 1

Component	Type	Role
Share record with doctor	Transaction	Set the record access permissio
Update past visits	Transaction	Update the past visit array in record (date, proce
Update appointment	Transaction	Update the specific appointment (
Send bill	Transaction	Send the bill info to a specific pat
Pay bill	Transaction	Pay the bill to a specific money p
Share record with doctor notification	Event	Inform that the record is shared with the s
Update past visits notification	Event	Inform that the past visit info is updated by th
Update appointment notification	Event	Inform that the appointment is updated by the
Send bill notification	Event	Inform that the bill is sent to the specif
Pay bill notification	Event	Inform that the bill is paid by the speci

Table 1

PROTOTYPES: MVP AND MOCKUPS

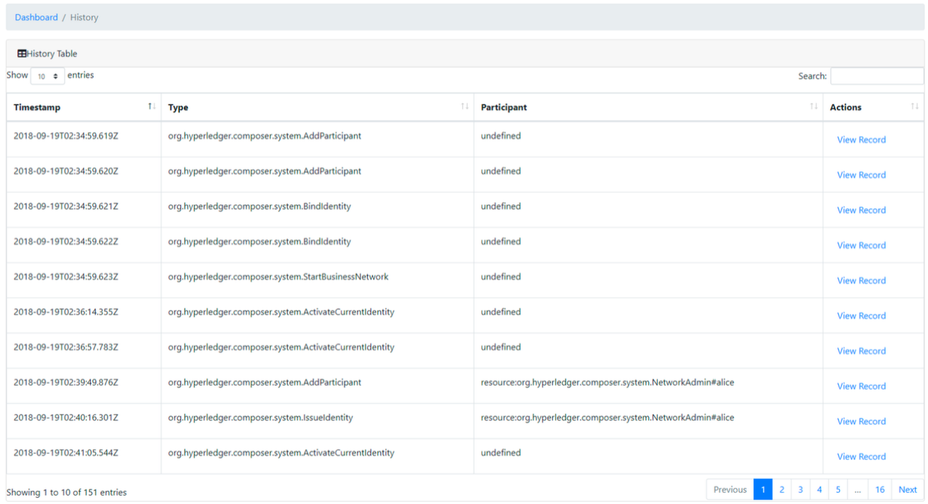


Figure 2

Figure 2 represents the snapshot of transaction history including timestamp, type, and participant. Timestamp is an unalterable blockchain ledger record time indicating when the transaction was processed. “Type” presents the transaction type and “participant” represents the user who submits the transaction.

For example, If Alice wants to access her glucose data on her phone that would be recorded as a transaction, and the participant would be NetworkAdmin (Alice) and the type would be IssueIdentityFor her to give consent to her phone to upload her information to hospital servers, the type of transaction would be AddParticipant

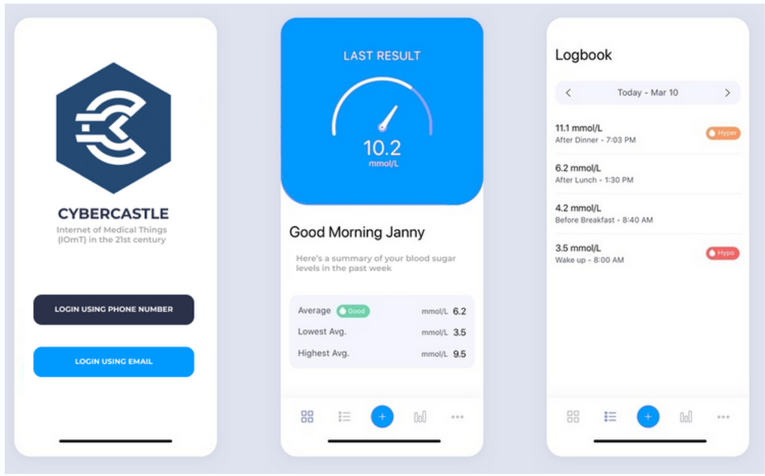


Figure 3

Figure 3 shows the app component showing a login screen as well as Alice’s glucose data when requested

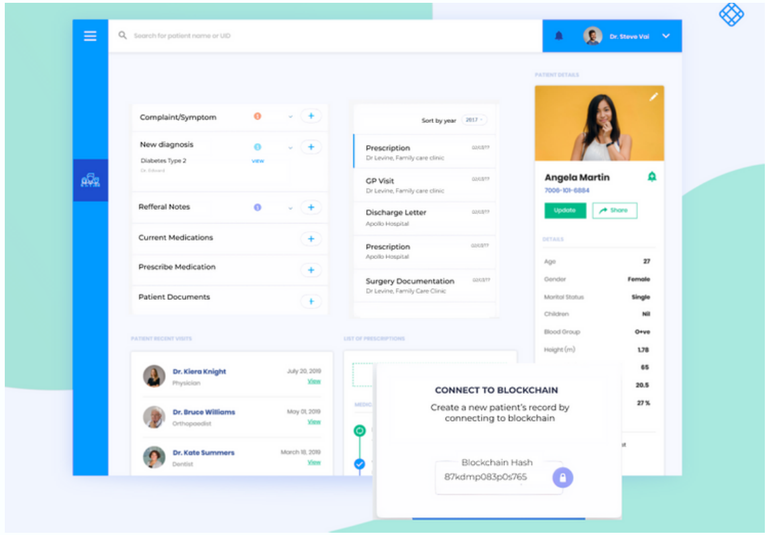


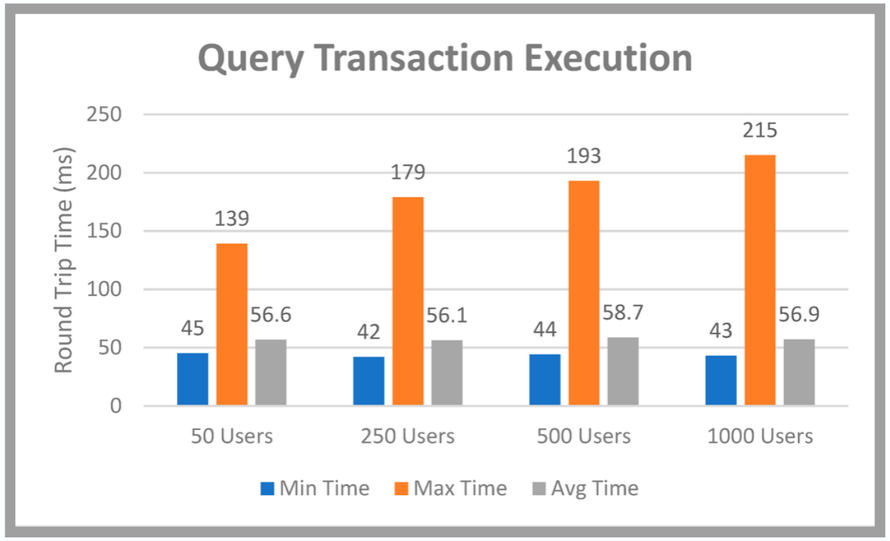
Figure 4

Figure 4 represents the snapshot of Alice’s Doctor EMR dashboard that provides a portal to access a certain piece of the EMR, the dashboard also provides an entry that shows the detailed information of a specific transaction.

PROTOTYPES: TESTING

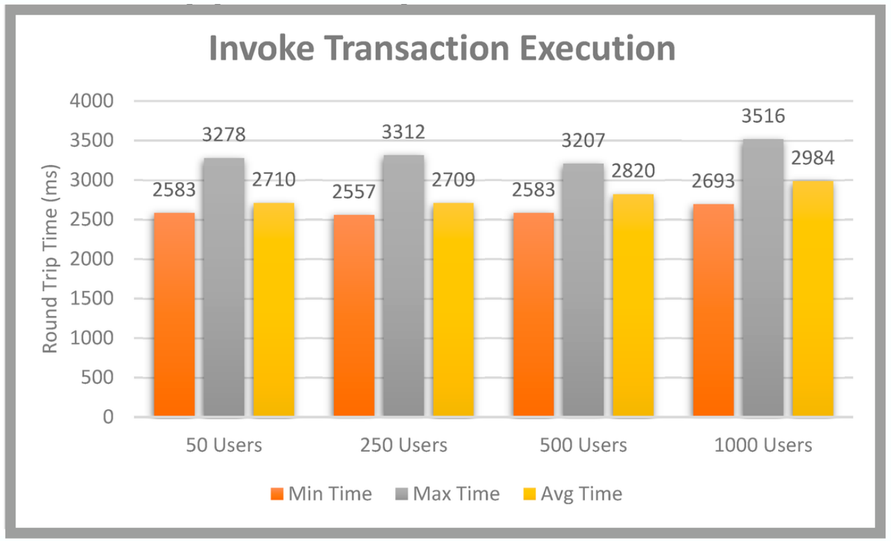
The experimental test was carried out by evaluating the transaction round-trip time in the blockchain network (the time that a transaction request takes to be sent plus the length of time it takes for an acknowledgement to be received by the web client). Two cases were performed.

First Case



It is the round-trip time spent on performing query transactions The round-trip time slow grows with the increase of user requests. However, the increase is at such a relatively small level that it can be ignored since it has no direct impact on user experience.

Second Case

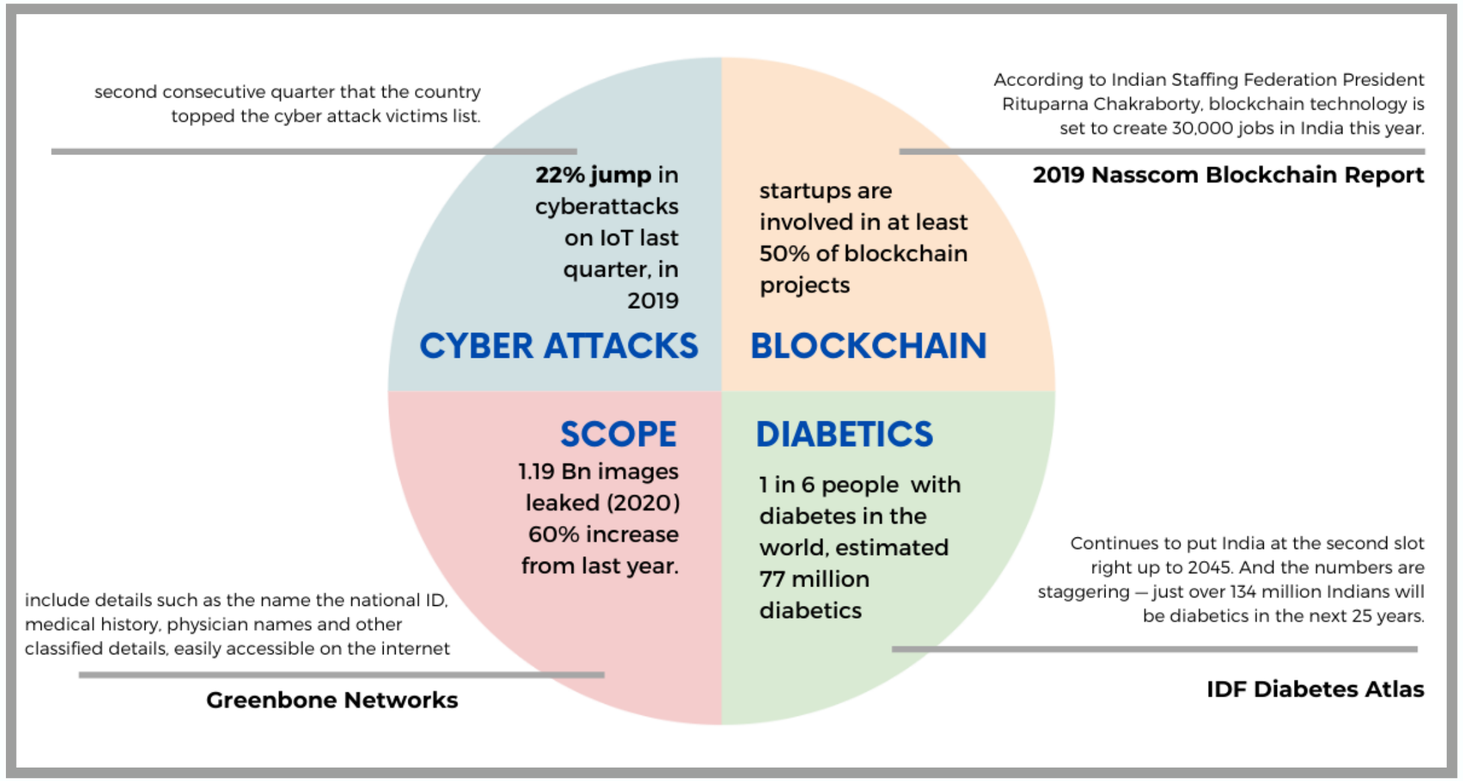


It is the time spent on performing invoke transactions. It can be seen from the graph that this spends much more time on performing transactions than the first case.

For Ethereum, the average transaction times to mine a block are around 15 seconds, however, the time cost varies significantly in terms of network environments. The average transaction execution time for our proposed network is around 3 seconds, which races far ahead than most popular blockchain platforms.

MARKET VALIDATION AND BUSINESS MODEL

TARGET COUNTRY: INDIA



American insurance companies Premera Blue Cross and Excellus Health Plan have reported cyber-attacks with data compromise of over 10 million subscribers. A cyber-attack on Anthem in February of 2015 compromised the data of 78.8 million customers.

Although India has been working on the healthcare data privacy and security bill since 2018, the bill hasn't come into effect yet. The Ministry of Health and Family Welfare placed the draft for Digital Information Security in Healthcare Act (DISHA) has an aim to secure the healthcare sector data in India, giving people complete ownership of their health data. Without proper insurance laws and enforcements in place, Indian healthcare insurance companies could face the same consequences as the US.

Having insurance companies subsidise our costs by giving subscribed users a phone plan along with IOT device, they could save billions of dollars down the drain.

SCOPE, LIMITATIONS AND FUTURE

Future Proposals

Facial recognition: One of the bigger benefits with facial login is that users are not subject to cumbersome and long processes for identity verification - it's done in a few milliseconds. Businesses will be able to sift out fraudulent accounts and ensure that only legitimate users are creating and accessing their accounts.

Machine learning algorithm to detect future attacks - We can partner with existing AI-focussed industries to help enhance our own proposal (ML can be used to automatically flag potential vulnerabilities or anomalies, and notify the appropriate managers, so they can respond quickly. It not only helps receive actionable insights on the individual device level, but in the aggregate as well, presenting a departmental and organizational overview of one's risk profile)

Limitations

- The programming codes in the smart contract and an easy programming mistake could lead to a disastrous chain of events.
- The Practical Byzantine Fault Tolerance (PBFT) algorithm used in the proposed blockchain platform can be disabled if more than a third of the peers are offline at the same time.
- The limited number of peers will result in an incident that could happen in small networks. It is essential to increase the number of peers to prevent malicious peers from occupying the whole system.

Scope

This project is primarily focused on developing an application for the computerization of Electronic Medical Record (EMR), monitoring the glucose of a diabetic patient, and securing the data with the implementation of blockchain in IoMT. Specifically, the development of the system covers the process of making the transmission of data:

Safe: Resolving any security vulnerabilities associated with remote patient monitoring and automating the delivery of notifications to all involved parties in compliance to HIPAA.

Simple: Tracking glucose levels measured with supported real-time patient monitoring.

Secure: Utilizing blockchain-based smart contracts to facilitate secure analysis and management of medical sensors.

Competitor's analysis

Name	Mission	Value Offer
BeatO	- manage diabetes through your smartphone.	- uses Smartphone glucometers that are extremely small making them convenient to carry and take accurate readings. All readings are saved on the app and cloud to access anytime.
PranaCare	- AI and SaaS-based platforms for lifestyle management providers who can also manage clients.	- Decentralized ledger for Patients Data Records linked using cryptography - Private Chain of Healthcare Stakeholders managing the Patient Data Records - Insurance Companies or any other Compliance Monitoring Authorities can get access to untampered Patients Data Records for Fraud Control.
PlenumData	- provides data security, data integration and data management solution	- designed for use of 'cloud native' or 'serverless' deployments. - No hardware investments required by enterprises

CONCLUSION

Data breaching has affected the trustworthiness of companies and compromised the information of customers. We recognize that healthcare systems are facing various challenges of technological and economical issues to better protect patients. The fusion of technology and healthcare may result in the threats of the confidentiality, integrity, and availability but with Cybercastle we aim to deliver a successful solution would balance liberty and security, along with an affordable and attractive product.

ACKNOWLEDGEMENT

We would like to thank our mentor Ms. Jill Gundlach for her unwavering pedagogic and systematic teaching during our time together.

Additionally, we are sincerely thankful for extensive support from following experts: Gabriel Zosa, Eva Bruketa, Balaji Gopalan, Olivia Standish. Special thanks to Nicole Becher for giving us an overview of blockchain and its key aspects.

Lastly, we would like to extend our gratitude to the New York Academy of Sciences, The Junior Academy, and S&P Global - the sponsors of this challenge.

BIBLOGRAPHY

REVIEW OF RELATED LITERATURE AND STUDIES

- Angeles, R. (2019). Blockchain-based healthcare: Three successful proof-of-concept pilots worth considering. Journal of International Technology and Information Management, 27(3), 47-83.
- Cichosz, S. L., Stausholm, M. N., Kronborg, T., Vestergaard, P., & Hejlesen, O. (2019). How to use blockchain for diabetes health care data and access management: an operational concept. Journal of diabetes science and technology, 13(2), 248-253.
- Dilawar, N., Rizwan, M., Ahmad, F., & Akram, S. (2019). Blockchain: Securing Internet of Medical Things (IoMT). Int J Adv Comput Sci Appl, 10(1).
- Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. J. Med. Syst. 2018, 42, 1302]

PROBLEM

- Dungan, K., & Verma, N. (2018). Monitoring technologies–continuous glucose monitoring, mobile technology, biomarkers of glycemic control. In Endotext [Internet]. MDText. com, Inc..
- Gabriel, M. H., Noblin, A., Rutherford, A., Walden, A., & Cortelyou-Ward, K. (2018). Data breach locations, types, and associated characteristics among US hospitals. Am J Manag Care, 24(2), 78-84.
- HIPAA Journal. (2020, February 24). January 2020 healthcare data breach report. https://www.hipaajournal.com/january-2020-healthcare-data-breach-report/
- Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we?. Bmj, 358, j3179.

TECHNICAL

- Allied Market Research. (2018). Internet of things (IoT) healthcare market to reach $136.8 Bn, globally, by 2021. Market Research Company offers Syndicate & Custom Market Research Reports with Consulting Services - Allied Market Research. https://www.alliedmarketresearch.com/press-release/internet-of-things-iot-healthcare-market.html
- Bryant, M. (2019, April 11). Healthcare again tops industries for cybersecurity attacks, data breaches. Healthcare Dive. https://www.healthcaredive.com/news/healthcare-again-tops-industries-for-cybersecurity-attacks-data-breaches/552403/CyberMDX. (2020). Clinical connectivity: Just the facts. CyberMDX Healthcare Cybersecurity. https://www.cybermdx.com/resources/clinical-connectivity-factbook-
- Faber, B., Michelet, G. C., Weidmann, N., Mukkamala, R. R., & Vatrapu, R. (2019, January). BPDIMS: A blockchain-based personal data and identity management system. In Proceedings of the 52nd Hawaii International Conference on System Sciences.

MARKET VALIDATION, SCOPE, AND LIMITATION, TARGET COUNTRY

- ETCISO India. (2019, August 10). India most attacked nation in IoT space last quarter: Report. ETCISO.in. https://ciso.economictimes.indiatimes.com/news/india-most-attacked-nation-in-iot-space-last-quarter-report/70614581
- Godse, V., Bhattacharya, M., & Ghosh, A. (2019). CYBER INSURANCE IN INDIA: Mitigating risks amid changing regulations & uncertainties. Data Security Council of India (DSCI). https://www.dsci.in/ucch/resource/download-attachment/13/Cyber%20Insurance%20in%20India
- Kannan, R. (2019, November 14). India is home to 77 million diabetics, second highest in the world. The Hindu. https://www.thehindu.com/sci-tech/health/india-has-second-largest-number-of-people-with-diabetes/article29975027.ece