Smart e-Health Security and Safety Monitoring with Machine Learning Services

W. Liu
School of Science and Technology
GGC

E.K. Park
Associate Provost for Research
NCCU

U. Krieger
Computer Science in Communication and Networks
Otto-Friedrich University Bamberg

S.S. Zhu
Department of Computer Science
Shantou University

Abstract— **This research provides security and safety extensions to a blockchain based solution whose target is e-health. The Advanced Blockchain platform is extended with intelligent monitoring for security and machine learning for detecting patient treatment medication safety issues. For the reasons of stringent HIPAA, HITECH, EU-GDPR and other regional regulations dictating security, safety and privacy requirements, the e-Health blockchains have to cover mandatory disclosure of violations or enforcements of policies during transaction flows involving healthcare. Our service solution further provides the benefits of resolving the abnormal flows of a medical treatment process, providing accountability of the service providers, enabling a trust health information environment for institutions to handle medication safely, giving patients a better safety guarantee, and enabling the authorities to supervise the security and safety of e-Health blockchains. The capabilities can be generalized to support a uniform smart solution across industry in a variety of blockchain applications.**

Keywords- e-Health Blockchain; Accountability Solution; Security Monitoring; Intelligent Analytics; Machine Learning

I. INTRODUCTION

The purpose of our e-Health monitoring program is to provide accountability to improve patient safety, decrease costs, and address the complexity of challenging e-Health problems in security, reliability, efficiency and flexibility. In the past [1,2,3] e-Health devices were mainly managed in a local system by an operational personal with direct control but with minimum sharing or remote automations. As new monitoring technologies are emerging in hardware (e.g., IoT for Health [4]) and in information delivery (e.g., Blockchain for Health [5]), new monitoring requirements bring evolutionary paradigms into the network of any unique healthcare devices embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data in blockchains. The Advanced Block-Chain (ABC) approach for e-Health [6] was a permissioned-based solution designed from scratch to meet the increasing demands in healthcare growth as well as in the new form of social interactive norms between patients and health service providers, which could revolutionize the e-Health industry with greater efficiency by eliminating many of the intermediates as we know them today.

The security and safety extension to e-Health stems from considerations that previous developments lack effective means to achieve security at the e-Health blockchain level, and they do not adequately address the patient safety in medication errors or over treatments. It turns out that the monitoring of new e-Health flows becomes a new challenge not only in numbers but also in upcoming social interactive norms. Social-distancing is very likely to further increase in adaption of e-Health technological services to control the costs while meeting demands. Recent advancements in e-Health research [7~11] have enabled interoperable and scalable networking, applications, and services for effective sharing of electronic health records, flexible data representation, and more efficient services that access such health data. As new technologies emerge in socially decentralized paradigm in life-essential applications, the blockchain interconnection of health services and devices have also emerged. These new e-Health activities outside the traditional healthcare systems are becoming able to inter-operate in the existing Internet infrastructure, which in turn further suggests the potential upgrade of the overall e-Health monitoring middleware service architecture solutions.

Furthermore, the new integrated view of data chains with security and service delivery cannot be easily addressed by the traditional e-Health audit as classical solutions are more focused on the needs of clinical/hospital/lab usages. To provide a patient centric service with new e-Health blockchains with diverse edge medical services, a new solution direction is necessary to allow the society to move towards on-line practices. Thus, it is imperative to expand the emerging advanced blockchains for e-Health with security and safety controls.

We present our intelligent monitoring service that provides administration functions for security and safety in rolling out e-Health blockchain level services. We also use machine learning, for evidence-based audit, real time assimilation, and automatic back-tracing of medications at the application service layer. This paper is organized as follows. In section II, we describe our overall e-Health blockchain architecture evolutions from the various phases of e-Health interconnection models starting from the basic digital healthcare movement to the new dimensional health blockchains. In section III we explain the intelligent monitoring in the context of e-Health service blockchains. In section IV, we layout the machine learning mechanism to

detect medication safety at the application as well as regulatory conformance. The final section V concludes with a summary of our contributions.

II. E-HEALTH BLOCKCHAIN ARCHITECTURE

We have experienced rapid changes in an e-Health technological solution for interconnection services. While the fundamental DHC (Digital Health Care) architecture [7] originated from the Service Layer solution over networked e-Health systems, the detailed designs have evolved from network interoperability solutions and e-Health security framework to cloud-computing and as well as fast development platforms [8~11]. Recently e-Health blockchains also emerged as open and distributed ledgers [12] can record e-Health transactions and flows efficiently and in a verifiable-and-permanent way. With appropriate monitoring, the permissioned e-Health "ledger" [13] itself can also be programmed to trigger safety and security transactions automatically. Since the initial successful implementations, the design of a public ledger has been the inspiration for financial transactions as well as in applications such as automatic legal services, insurance processing, supply chain tracking of merchandize, and upcoming healthcare services. All are yet to solve the security and safety monitoring problem, especially during life-critical situations.

Among the many functions, of a continuously scalable universal exchange for current and future e-Health, are the dealing with data originating from diverse sources in multiple formats: HL7 messages, Lab LOINC codes, ICD codes, e-Prescribe as well as corresponding signatures from the e-Health service providers and/or the patients acknowledging the acceptance of care. All are further woven into multiple dimensional blockchains as illustrated in Figure 1 [6].

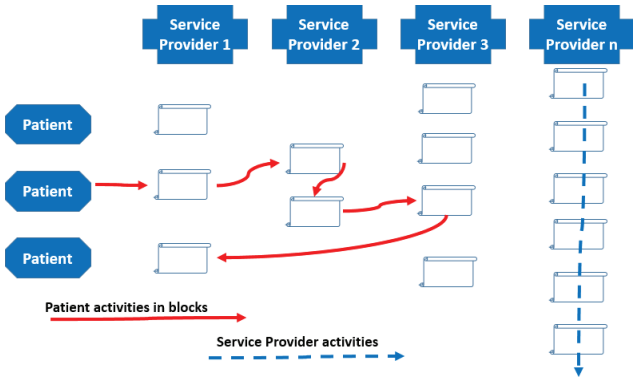

Figure 1. e-Health Service Advanced Block-Chains

Healthcare service providers (SPs) apply digitization of fast e-Health resources and publish available records during the transfer of ownership in handling patient cares, so cares can be conducted at a speed more in line with the pace of doing e-business when adopting the new blockchain model. Each of the blocks has to be signed by all involved parties before posting. All blocks are validated by the e-Health blockchain protocol. When sharing information for research or epidemic discovery, a multiple dimensional blockchain becomes conceivable when we add regulatory processing flows and other conformance requirements.

AI (artificial intelligence) and ML (machine learnings) integration are the keys for our extension to address those regulatory mandates in security of the e-Health blockchains as well as the conformance to the safety of medications at the applications. Patient-initiated chains formulate the information equivalent to the currently know EHR (Electronic Health Records) yet in a totally different format (i.e., in the e-Health block format with additional block ID and initiating parties' digital signatures). On the vertical processing threads are the e-Health blocks as processed by the service providers for their rendered treatment services. Each block has to be signed by all involving parties before being posted. And they are validated by the e-Health blockchain protocol [6,7], under which blockchain e-Health engines provide health-specific logic(s) to trigger smart transactions defined as a proven treatment procedure flows with maximal automation in mind. The AI machine learnings are integrated with the blockchain technology for decision making and collaboration. Specifically, as illustrated in Figure 2, the possible imbedding points are Cluster access, Stream access, and Security managers.

The Intelligent ML processing details will be reflected in Flow logic with both Meta data elements as guides as well as Blocking filters for security checks. Advanced processing methods are required for

1) controlling and maintaining data integrity, provenance, security, privacy and reliability;

2) providing trustworthy patient identification and authentication and access control protocols; and

3) maintaining sensitivity to legal and ethical issues associated with universally accessible e-Health data.

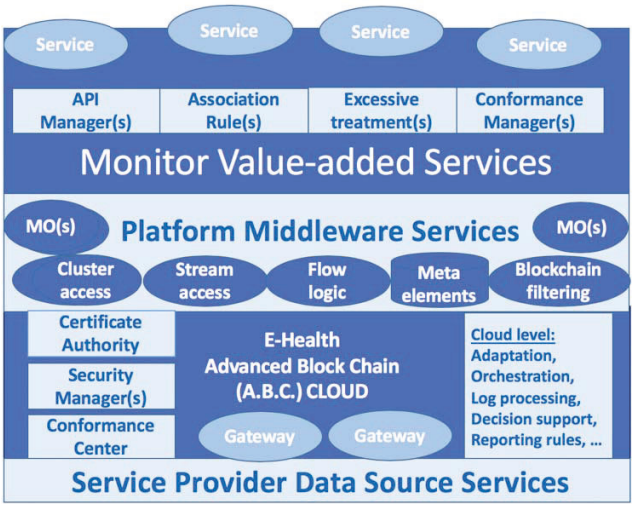

Figure 2. e-Health Blockchain Monitorting Architecture

Pertinent details of the new security intelligent monitoring and ML level medication safety are discussed

in the next two sections. Other baseline functions of the e-Health advanced blockchain can be referenced in [6].

III. E-HEALTH INTELLIGENT MONITORING APPROACH

In the context of e-Health, all treatment flows have to be secure and safe. Traditionally, those processes are in batch (non-realtime activities) in most of hospitals and clinics today. With e-Health blockchain solutions, the treatment flows are contained inside the communication sequences. And instant monitoring and real-time intervention will revolutionize the healthcare effectiveness in terms of prevention of over-prescription of medicine, deviation of commonly cure flows, and other costly duplication of medical tests. The monitoring capability enables the blockchain flow conformance as well as detection/report capabilities.

Our e-Health security-and-safety framework fits a variety of use cases by providing an easy to set up, extensible, and affordable solution. The development is extended from the Advanced Block-Chain [6] for e-Health, with the creative extension to offer an accountable monitoring solution for real-time healthcare teams in present actions-management as well as for regulatory bodies in future audits. It is a solution with virtualized blockchain logging service technology with automatic scaling and resilience of all monitoring services. In order to fit the growing blockchain industry, our designs integrate commodity servers into the cluster to enhance the ease of setup and maintainability on already existing infrastructures. Therefore, we distribute services on computing nodes while utilizing well-known cloud computing platforms. In addition, we can grow our service architecture when the service orchestration is dynamically provisioned to reflect future health paradigms.

A. Blockchain Interception Layers

These are enabled by monitoring the key clusters as well as by plugging into the massive streaming of e-Health blockchain data containing a number of measurements: identity related traffic, the healthcare service accounts, platform and communication operational measurements, provision of performance monitoring events at the interface to blockchains, as well as content level data capture that are further processed at the e-Heath block layer.

Managed Objects (MOs) are instantiated to capture the corresponding care information flows. Once a MO is entered in the database and the accounts are updated, the records cannot be altered, because they are linked to every transaction record that involves a particular flow. Various computational algorithms and approaches are deployed to ensure that recordings in the database are permanent, chronologically ordered, and available to all others on the monitoring network. To scale up the MO repository, the MO databased will be migrated to big data security service [11,12].

Streams of e-Health blockchains supply a publish-abstraction blockchain infrastructure. A stream consists of a list of stream items and is identified by a unique name. A big data service can handle continuous streams each of which may comprise multiple megabytes in size. To read items from a stream, an intercept service has to subscribe to that stream which in turn is pushed from the physical cluster from the e-Health blockchain. This big data service identifies the underlying (blockchain) transaction that initialized the stream and then scans all subsequent blocks for transactions that add items from that stream.

As such the e-Health blockchain interception consists of three layers: the physical access protocol to the clusters, the service protocol for stream processing, and the operational management protocol for governing formatted monitoring information in terms of MO protocols.

B. e-Health Block Capture

Besides the above strategically placed interceptions at the communication stream network, massive harvests of e-Health blocks will allow content level monitoring and reverse-engineering of ICD (International Code of Disease) code sets (and the flow sequences of codes). As the patient IDs are not visible in any e-Health blockchains, a subscription to meta data elements service is required to interact with real Health Information Systems in clinics, medical labs and hospitals. And the monitoring service subscription environment has on-demand interactive scenarios that can be easily expanded with the immersive cloud importer.

The meta elements supply the data block capture templates and are further supply a new abstraction to encapsulate the mundane medications. To guarantee desired exchangeability between compatible systems, every e-Health block reading service converts its received data into a more universal format utilizing the JavaScript Object Notation (JSON) format, where a combination of masked patient_id and service_id forms a unique identifier for every transaction per “flow” in a sequence of e-Health blocks:

```
{   "eHealth_Flow_id": 1,
    “block_id”:  [
        "masked_p_id":   detail omitted,
        “service_provider_id”: detail omitted,
        “auto_block_id”: detail omitted,
     ]
    "type": treatment_id,
    "treatments": [ name: …, value: …,   { notes }   ]
    “flows”:  detail documentation flows omitted
}
```

A medical treatment flow should provide e-Health data optimized for vital signs information, medication allergy alerts, disease diagnosis code set(s), medication, lab results, and personalized medicine tied-in to a specific patient cure flow as prescribed in an accepted cure procedure. When integrated into the e-Health intelligent monitoring system, active polls in sampling or passive (conformance) event-triggers are recorded when security level thresholds are detected.

Additional filtering pools allow customization of the specific criteria in selecting the meta data, various disease codes and treatment procedures. One utmost filtering criteria is in matching the treatments and prescriptions to the correct patients, thus generating security alarms when data are

tempered or irregular vital signs are off. Once provisioned, those instances of the filters and provision rules are consistently formed in the MO format again.

C. Immersive Block Importer

It is the immersive block importer [14,15] layer that allows writing code, performing live exploitations, configuring servers, and doing analysis & performance indicators in order to scale up and down of the MO repository clusters. Another key function is to support Application Programming Interfaces (APIs) for future new monitoring services and applications. As such, an API manager exposes the monitoring security services all the way up to the application users for development applications.

The monitoring platform to support this importer layer has to accommodate the block capture design as well. We have considered the design options of Docker Swarm vs. Kubernetes. While the Docker Swarm could meet prototyping and rapid development of the e-Health monitoring services with ease of usage, at the end we decided on our architecture design to incorporate Kubernetes (K8) for microservices and streaming. In addition, Kubernetes has a much richer feature set because it offers by default advanced operation services, such as service monitoring, centralized logging and a dashboard. One major drawback is the complicated setup process from adopting the complex system.

D. Data Analytics with End-to-End Logic

Health service flows and deviations are detected and flagged because of end-to-end logics in monitoring and logging deployments. Again, those end-to-end logics are formulated in meta data to prevent the different health service providers from becoming autonomous healthcare delivery islands with their own arbitrary standards and billing levels. These metadata, which cover treatment side-effects, complications, medication conflicts and infections or return-rates, also become a part of the overall health service flow activities.

The key function beyond security monitoring is to supply end-to-end data integrity analysis and authorization audits, the summary results are reported as the analytics outcomes with customized presentation. All the reporting flows enable a central security manager to ensure security of healthcare processing when data are transmitted via the blockchains. While at the same time, security manager of those flows authenticate the validity of the authorities who are tapping into global data collection that un turn enable the government agencies to formulate the cost effectiveness of care procedures that involve a large number of medical services.

IV. E-HEALTH MCHINE LEARNING FOR SAFETY OF PATIENT MEDICATIONS

As the core e-Health systems are relatively stable, rapid growth comes from future blockchain information flows as well as applications to the monitoring application. Another new feature is in our application of ML into medication safety in e-Health to perform treatment detection issues. One key issue, among many, is in excessive medicine overly prescribed and overly used. The solution also related to enhanced end-to-end treatment flows order to achieve safety during care.

1) Construction of Disease Association Rules

Due to the differences in the experience and technical levels of different doctors, some doctors might give a wrong diagnosis. It could be constructed by a disease diagnostic model via the relationship between the patient symptoms and disease to determine the abnormal condition of the wrong treatment. Among them, the key method used was the association rule of the unsupervised learning method. The specific modeling steps are as follows:

Step 1: Find the historical medical history of the relevant disease as a training set and establish a medical diagnosis (aka "transaction") list with set $\{S_i\}$ being the symptoms and set $\{D_j\}$ being possible diseases.

Step 2: Generate a frequent item set using the Apriori algorithm which is a machine learning technique. The specific process is to set the minimum support (s) and the minimum confidence (c), scan the data set of the treatment data list table, and generate a candidate rule item set $\{S\}=>\{D\}$ The support item count of the candidate item set is compared with the minimum support count to generate a frequent item set F_1. The algorithm continues to use the progressive link and pruning steps until the final frequent item set F_k is generated.

Step 3: The frequent item set eventually generates an association rule e.g., $\{S\ldots\}=>\{D_j\}$. The specific process is to generate a non-void subset of the final frequent item set F_k by determining whether the support is greater than the minimum confidence. As such, an association rule can be generated for a particular disease type D to be derived from a subset of symptoms S, and finally well-established doctor diagnostic results are compared for accuracy of the associations.

2) Excessive Treatment Discovery Application

After extracting data analytics from the e-Health blockchains to form association rules, the next step is to perform auto detection of Over-Medication that is the main manifestation of excessive treatment. Our approach is to apply a drug similarity comparison model and extend it to the similarity between new prescription and the best expert prescription to examine whether it is over-medicated with a new prescription.

Step 1: A direct comparison may not be straightforward for the e-Health blockchain procured treatment flow data, as drugs of various names could perform similar (or have the same) functions. The application should first check whether any new prescription drugs (or treatment steps) that are incompatible with the disease; if yes, it is judged that the prescription is wrong and invalid; otherwise continue to Step 2 next.

Step 2: When and if there is similarity among the drugs between two treatments, a single treatment is compared to an optimal (classical) treatment. If the treatment under audit is a

super set of the optimal treatment, it can be flagged out as a possible over-medication. Otherwise, the similarity of new and existing subscriptions cannot be judged by the drug name at this time, and continue to Step 3 next.

Step 3: In order to judge the similarity between drugs with different names, we apply the therapeutic functions via a K-Modes clustering process so that the overall similarity of the two drugs is judged. The specific calculation is to determine the "distance" of each treatment (T1, T2, etc.) while our application middleware encapsulates the capabilities. The format is in the "distance" that captures Therapeutic Functions Similarity:

	Therapeutic functions				
	fun1	fun2	fun3	fun4	...
T1 effects	0	0	1	1	...
T2 effects	1	1	0	1	...
Etc.	1	-1	0.5	0	...

The treatments are similar if they are within a pre-set threshold after totaling the weighted sum for the desired therapeutic functional set.

Step 4: Finally, the combined procedure (with T1, T2, etc.) are compared with the extracted optimal treatment for excessive medication. Otherwise, the new treatment has better therapeutic effects over the disease and excessive treatment is excluded.

At the end, the new and non-excessive treatment is to be included as a candidate for further optimal treatment model selection which is beyond the scope of this paper.

3) Regulatory Conformance

The e-Health blockchain monitoring design has to meet the stringent privacy specifications as required in HIPAA [16~18], EU-GDPR [19] and other [20] regional regulations. Through the use of IDs and permissions, patients can specify which part of e-Health record details they want others to be permitted to view when they are flowing through the e-Health blockchain service flows. Permissions can be expanded for government agencies and auditors, who may need access to more healthcare details. Having a decentralized (yet monitored) but shared data collections can serve as a single source of truth with the ability to monitor and audit healthcare practices.

4) Additional Value-added applications

Additional value-added service systems are derived from accessing the enhanced e-Health monitoring applications. For example, a supporting entity such as an insurance company may obtain identification information and extract and process the e-Health blocks as referenced by a billing block chain without the physicians to submit billing requests as in existing flows. These activities are in turn automatic because the computational logic in e-Health flows automatically trigger billing processing and payment transactions between nodes in insurance and in a doctor's office. As such, our monitoring service application engine can be further expanded to co-relate with billing expenses, resulting in consistency and constant detection. Additional value-added applications can be extended to health care research and discoveries in terms of new indications of out-breaks and effectiveness in treatments for new epidemics.

V. BENEFITS AND LIMITATIONS

The key benefits are multifaceted in extending the e-Health blockchain architecture approach to include the appropriate monitoring and application middleware. First of all the permissioned Advanced Block-Chain (A.B.C.) was previously devised from scratch, and now this innovative extension allows many flexibility and creativity without any dependency on other platforms like a Hyperledger Fabric or Quorum solutions. Instead, the solution as presented in this paper could be generalized to those other blochchains. Our solution provides automatic security monitoring (of end-to-end healthcare flows) and also preserves patient privacy and safety. Government and regulatory agencies are given additional control for audit and conformance purposes.

By embedding computational logics into the e-Health blockchain flows as well as into treatment protocols, additional remote medication endpoints could be available for monitoring service in the future. The application engine stands ready for the excessive treatment and over-medication detection, regulation compliance reporting, billing updates, alerts from treatment results and medication events. Innovative healthcare flows with additional services will eventually emerge from the new e-Health blockchain practices.

Further benefits include solving the drawbacks of the legacy information flow of a medical treatment process, providing transparency and accountability of the service providers, enabling a secure, safe and trust health information environment for institutions to monitor their own medical data, and enabling the authorities to supervise new paradigm of e-Health services.

One limitation of our solution approach, which is partly due to the nature of healthcare that demands better control, is how to allow future public extension of the functions in cloud-sourcing of general health monitoring. Yet another open problem is in smart contracts such as letting a larger community, besides those with pre-setup provisions, to interact with the interceptor APIs for the e-Health blockchain. There is also a plan to remove any MO database and migrate into a pure cloud-based solution as part of the advanced blockchain for e-Health, which will be part of our future research.

Nevertheless, the intelligent monitoring and safety application capabilities can be further generalized to support a uniform smart solution across multiple industries in a variety of blockchain applications. Our solution further provides the benefits of resolving the abnormal flows of a medical blockchain process, providing accountability of the service providers, enabling a trust e-Health information environment for institutions to handle medication safely, giving patients a better safety guarantee, and enabling the authorities to supervise the security and safety of e-Health blockchains.

VI. REFERENCES

[1] W. Liu, E.K. Park and U. Krieger, "e-Health Interconnection Infrastructure Challenges and Solutions Overview", Proceedings of IEEE HealthCom-2012, Beijing, China, October 2012.