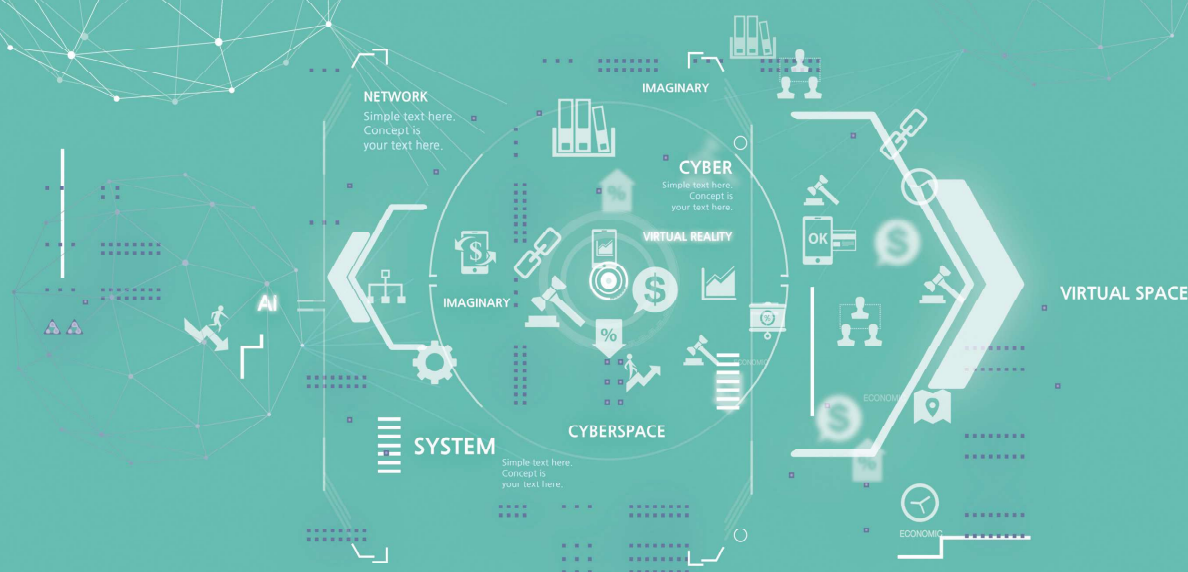




2019 International Conference on Platform Technology and Service

28-30 January, 2019, Jeju, Korea

PlatCon-19

Proceedings

IEEE Catalog Number : CFP19B77-ART (Xplore)
ISBN : 978-1-7281-1288-6 (Xplore)
IEEE Catalog Number : CFP19B77-CDR (CD-ROM)
ISBN : 978-1-7281-1287-9 (CD-ROM)

KSI Based Sensitive Data Integrity Validation Method for Precision Medicine System	115
<i>Deuk-Hun Kim; Jeong-Seok Jo; Jin Kwak</i>	

Optimized Power Consumption Model for Multiplication in Galois Field of AES	120
<i>Ju Hwan Kim; Boyeon Sim; Dong-Guk Han</i>	

Security Engineering for Secure Information Systems

A Design of a Tax Prediction System Based on Artificial Neural Networks	123
<i>Sung-Bong Jang</i>	

A Study on Smart City Security Policy Based on Blockchain in 5G Age	127
<i>Jong-ho Noh; Hun-yeong Kwon</i>	

Security Requirements for Cloud-based C4I Security Architecture	131
<i>Jahoon Koo; Young-Gab Kim</i>	

Deception Tree Model for Cyber Operation	135
<i>Chang-Wook Park; Young-Gab Kim</i>	

Analysis of IoT Platform Security: A Survey	139
<i>JinYong YU; Young-Gab Kim</i>	

Interoperable OAuth 2.0 Framework	144
<i>Se-Ra Oh; Young-Gab Kim</i>	

Efficient Vulnerability Management Process in the Military	149
<i>Seungjin Baek; Young-Gab Kim</i>	

KSI based Sensitive Data Integrity Validation Method for Precision Medicine System

Deuk-Hun Kim
ISAA Lab, Dept. of Computer
Engineering
Ajou University
Suwon-si, Republic of Korea
dhkim.isaa@gmail.com

Jeong-Seok Jo
ISAA Lab, Dept. of Computer
Engineering
Ajou University
Suwon-si, Republic of Korea
jsjo.isaa@gmail.com

Jin Kwak
Dept. of Cyber Security
Ajou University
Suwon-si, Republic of Korea
security@ajou.ac.kr

Abstract—Interest in precision medicine in the medical field is increasing through the United States ‘Precision Medicine Initiative’ announced in 2015. Accordingly, a method for secure and efficient provide of precision medicine services has been continuously studied. Recently, a survey by consulting company shows the importance of verification the integrity of data in decision making is increasing in the analysis of sensitive data of big data size that a key component of precision medicine. Therefore, in this paper, we study integrity validation method of sensitive data by applying signature technology called KSI in precision medicine system.

Keywords—Precision Medicine System, Keyless Signatures Infrastructure, Medical Security, Data Validation, Cloud-based Precision Medicine Center

I. INTRODUCTION

In recent years, cloud technology has been widely used in various fields to quickly and accurately analyze and utilize information based on big data. In this way, researches focusing on forecasting through big data in various fields are actively being carried out.

Among the many field of research that began is the ongoing an advanced perspective of healthcare services in the field of healthcare by the ‘Precision Medicine Initiative(PMI)’[1], which was announced in the United States in January 2015.

In the Republic of Korea, precision medicine is defined as “optimal personalized medicine that improves treatment effects and lowers side effects by integrating and analyzing health-related data such as medical record, genetic information, and lifelog” and has been selected as a leading field of the fourth industrial revolution[2].

However, according to a recent Accenture surveys, 89% of the top management of medical institutions responded that data integrity is an important issue in decision making when analyzing sensitive data of big data size[3]. In other words, to construct a precision medicine system, more secure and efficient methods of sensitive data of big data size should be continuously studied and applied.

In this paper, we review the outline of precision medicine system and KSI that can be applied to the precision medicine in Chapter 2, analyze the sensitive data flow according to the precision medicine configuration entities and examine the integrity validation method by applying KSI in Chapter 3. Finally, conclusions are made in Chapter 4.

II. RELATED WORKS

A. Precision Medicine Systems

Precision medicine provides a comprehensive analysis of information on a big data scale such as individual genetic characteristics, occupation, living environment, and dietary habits, and then provides optimal treatment suitable for individuals.

The PMI of the National Institute of Health(NIH) defines precision medicine as follows - Precision medicine is “an emerging approach for disease treatment and prevention that takes into account individual variability in genes, environment, and lifestyle for each person.” It is in contrast to a one-size-fits-all approach, in which disease treatment and prevention strategies are developed for the average person, with less consideration for the differences between individuals[4].

The components of precision medicine are population cohort, medical record of medical institutions, genetic information, medical big data of public institutions, mobile health care and big data analysis and security technology.

However, in order to secure construct a precision medicine system composed of a complex system of various factors, a security and efficiency approach is needed.

- Whether the data was generated from a trusted subject
- Whether the data is forged or not
- Efficiency of data processing on big data size
- Scope of data disclosure

In order to satisfy such a condition, hash tree characteristics can be utilized in terms of efficiency and, authentication and digital signatures characteristics can be utilized in terms of security.

Applying the Keyless Signatures Infrastructure(KSI) method[5], published by A. Buldas et al. in 2013, can provide a way to use sensitive data of big data size in precision medicine.

B. Keyless Signatures Infrastructure

Keyless Signatures Infrastructure(KSI)[5] is a technology developed by Estonian security firm Guard Time, which is an alternative to the existing Public Key Infrastructure(PKI) signature.

Keyless does not mean that the encryption key is not used during signature generation. This means that we still need a key in authentication, but we can create and verify a trusted signature without the need to keep the key confidential.

The signer identification and integrity protection functions are performed separately from keyless signatures and are implemented with multiple signatures. This signature process for the data is as follows:

Step 1. Hashing

The data to be signed is hashed, and the hash value is used to represent the data in the remaining processes.

Step 2. Aggregation

A global temporary hash tree for each round is created to represent all the data signed during the per round.

Step 3. Publication

The root hash value of the aggregation tree by per round is collected as a permanent hash tree called a hash calendar, and the root hash value of the tree is issued to the trust anchor.

An infrastructure is needed to perform this signature process. The infrastructure is a hierarchical structure of an aggregation server that creates a global hash tree per round through collaboration, and is composed of an aggregation network, a core cluster, and a gateway.

1) Aggregation Network

a) An aggregator is a component that constructs a hash tree from the request being sent and forwards the root hash value to the parent aggregator. When a response is received, the response is transmitted to the sub-aggregator.

b) Each Aggregator has a reserved spot in the hash tree, so it can prove the server involved when generating a particular signature token.

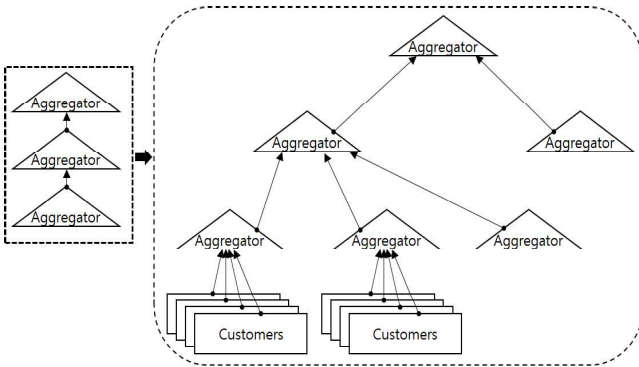


Fig. 1. Aggregation network

2) Core Cluster

a) It is composed of top-level aggregators per round, which generates hash calendars and distributes and synchronizes them through the aggregation network.

b) It is stored and distributed on the verification server through the archiving and cache layer to ensure integrity of the hash value of the hash calendar. Also, the root of the intermediate aggregate tree is stored only in the associated signature token.

c) The gateway copies the calendar copy from the cache server using the HTTP protocol and uses it to verify the signature token.

3) Gateway

a) It acts as a protocol adapter, accepting the application's request and delivering to the specified aggregator.

b) At the gateway node, the first level of aggregation occurs, and the extender to validate the signature token.

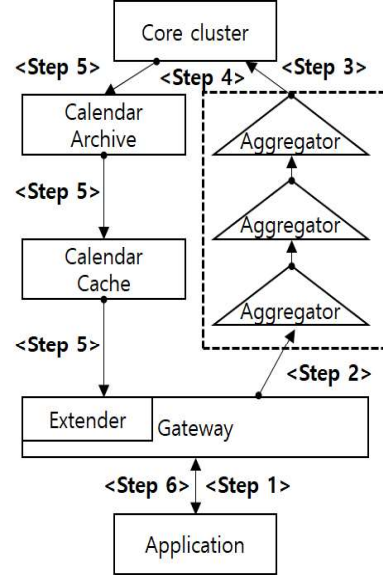


Fig. 2. Keyless signatures infrastructure

The process shown in Figure 2 is as follows:

Step 1. The application computes a hash of the data to be signed and sends a request to the gateway that services the user.

Step 2. The gateway aggregates the received requests during the round and sends the request to the upstream aggregation cluster to request the highest hash value.

Step 3. Requests are aggregated through aggregators of several layers and globally unique top-level hash values are generated by the core cluster.

Step 4. Responses composed of verifiable hash tree paths are sent back through the aggregation layer.

Step 5. The top hash values for each round are collected into a hash calendar archiving layer and distributed to extender services deployed with the gateway host through the calendar cache layer.

Step 6. The application utilizes the Extender service for signature verification.

C. Analyze the Risk of Integrity Infringement of Sensitive Data

Precision medicine system require sensitive data for each person. In this case, if the integrity characteristic of the sensitive data can not be verified, the reliability of the processed data is reduced. In other words, it can not normally provide precision medicine services.

The following are cases where the integrity infringement of sensitive data.

- Sensitive data may be falsified by attackers or unauthorized entities while sensitive data is being collected by each entity in precision medicine system.
- Sensitive data may be falsified by attackers in handling and managing data on big data scale in cloud-based data center.

Thus, there is a need to improve the security of precision medicine system through authentication and integrity verification during sensitive data collection and processing.

III. PROPOSED METHOD

A. Precision Medicine Data Flow

Figure 3 compares the sensitive data collected by each entity by the components of precision medicine mentioned in the related works in Section 2.A.

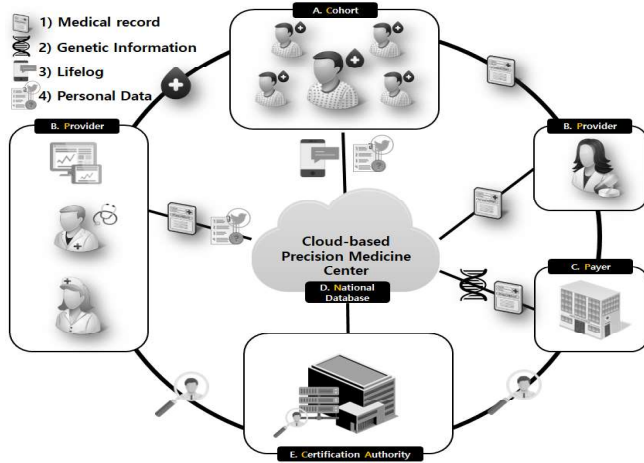


Fig. 3. Data flow in precision medicine system

1) Cohort

The subject to conduct medical consultation and questionnaire in order to receive precision medicine, and to agree with Precision Medicine Center(PMC) to provide its own genetic information, medical record and lifelog information.

2) Provider

The subject that provides medical services to the cohort group and transmit the cohort-related information to the PMC.

3) Payer

Pay the provider for the medical service, in addition, subjects who transmit past medical record and genetic information of cohort to the PMC.

4) National Database(ND)

It is a cloud-based centralized database center that receives sensitive information from each entity and

provides data that can be used in precision medicine through big data-based analysis.

5) Certification Authority(CA)

The subject that performs authentication of each entity in the precision medicine system.

Sensitive data collected from each entity is as shown in Table 1. Infringement of integrity may cause problems in the provision of processing and services for precision medicine, so it is necessary to verify the integrity of sensitive data.

TABLE I. SENSITIVE DATA ANALYSIS FOR PRECISION MEDICINE SYSTEM

Classification	Analysis
1) Medical record	Information about the prescription of each person in the cohort
2) Genetic information	DNA for each person in the cohort, information managed and provided by the cancer center and public institution
3) Lifelog	Lifestyle information of cohort collected through wearable device
4) Personal data	Others personal information such as survey results of the cohort group and SNS used in precision medicine system

B. KSI-based Integrity Validation Method of Precision Medicine System

In this section, we propose a procedure for verifying the integrity of sensitive data by applying KSI to a precision medicine system.

First, we analyze the application section for authentication and integrity verification in sensitive data collection process according to data flow for authentication and integrity verification through application of KSI in precision medicine system. The process is shown in Figure 4.

Step 1-2. Cohort groups perform mutual authentication through CA to provide life logs and personal information(such as SNS) to PMC, a cloud-based ND, and then provide data through encryption and KSI-based signature.

Step 3-5. Cohort visits the medical institution to perform the mutual authentication through the CA to provide the PMC with medical record and personal data(such as survey) among the sensitive data to be used in the precision medicine, and then performs the medical treatment and survey.

Step 6-10. The medical institution performs mutual authentication with the PMC through the CA, and provides medical record and personal data(such as survey) of the cohort group through encryption and KSI-based signature.

Step 11-13. Each patient in the cohort receives drug prescription from the pharmacist according to the prescription, the pharmacist performs mutual authentication with the PCM through the CA, and then provides the medical

record such as the patient's medication history and drug information through encryption and KSI-based signature.

Fig. 5. Proposed KSI-based integrity validation method in precision

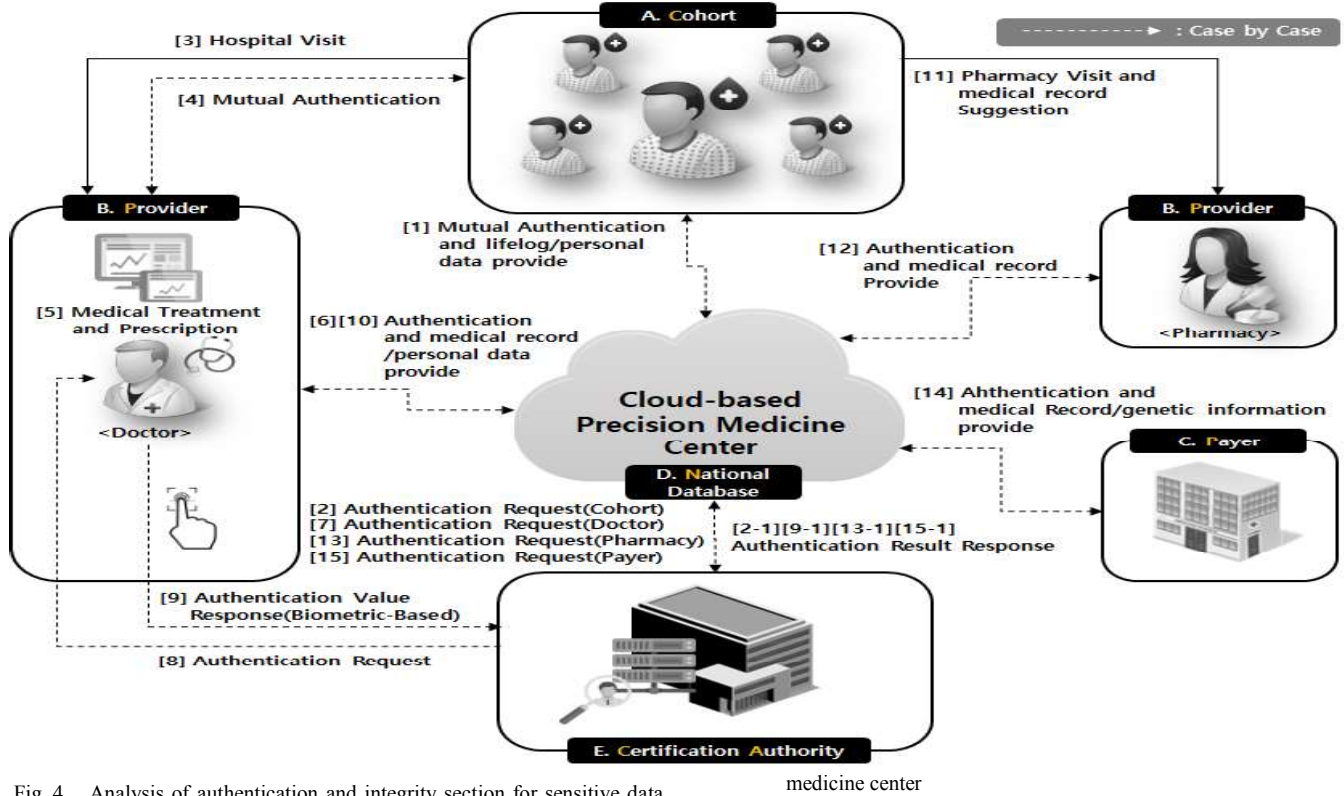


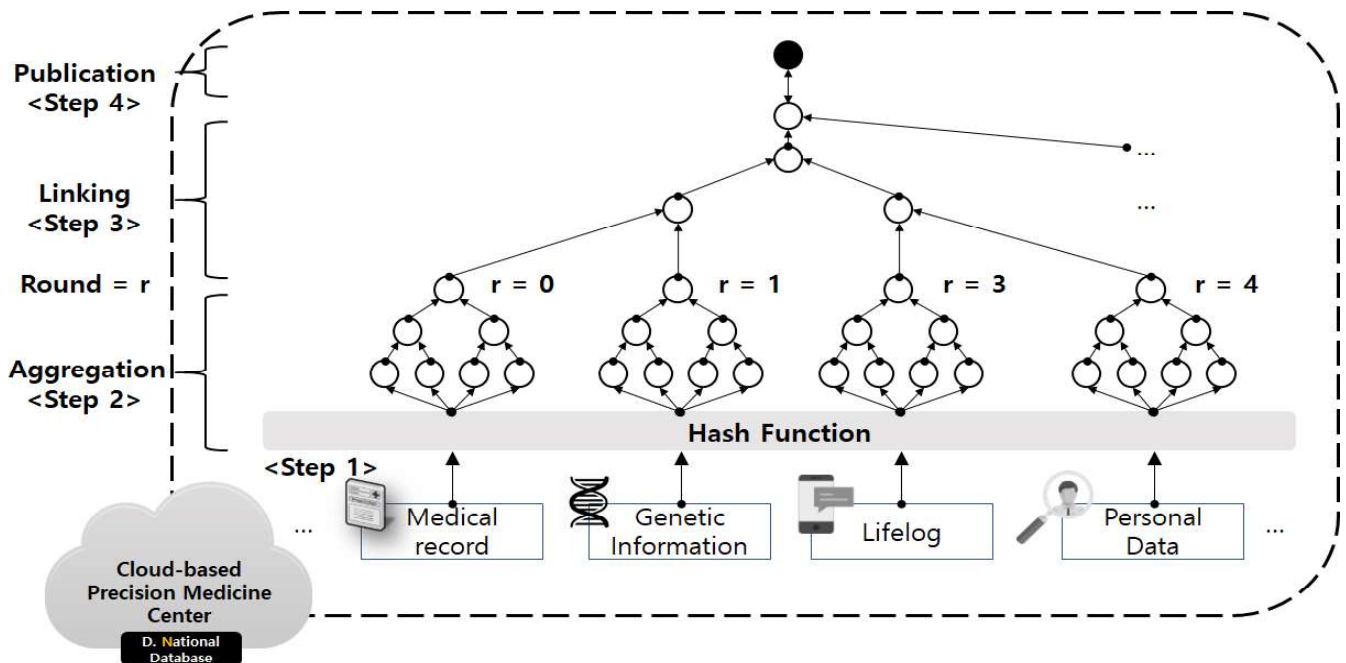
Fig. 4. Analysis of authentication and integrity section for sensitive data in precision medicine system

Step 14-15. Public institution related on medical system perform mutual authentication with the PMC through the CA to provide PMC with past medical and genetic information for each patient in the cohort group. Thereafter, medical record is provide through encryption and KSI-based signature, and the genetic information is provide through anonymization and KSI-based signature.

Second, the integrity verification process for sensitive data of big data scale processed by PMC after collection. The process is shown in Figure 5.

Step 1. In the cloud-based PMC, data is input to the KSI hash function to sign data such as medical record, genetic information, lifelog, and personal data collected from each entity constituting the precision medicine system.

Step 2. A global temporary hash tree for each round is created using the hash value in the aggregation network.



Step 3. Linking to the calendar to upstream the root hash value of the round-by-round aggregation tree.

Step 4. The top level root hash value of the tree that is up-loaded by the calendar is issued to the trust anchor to perform and validate signature and integrity verification for each sensitive data in the precision medicine system.

TABLE II. ANALYSIS OF THE SECURITY AND EFFICIENCY OF THE PROPOSED METHOD

Classification	Analysis
Whether the data was generated from a trusted subject	When collecting sensitive data from each entity, carry out entity authentication by CA and signature using KSI. In addition, since the validity of the top hash value is validated from the trust anchor, the reliability of the data is ensured.
Whether the data is forged or not	The KSI issues a signature token, which is used by the Extender to validate the data forgery by validating the signature token
Efficiency of big data-based data processing	Although the existing PKI has reduced the data processing speed by sharing each data and signature value, KSI has only improved the data processing speed of big data size by sharing the hash value of the data only.
Scope of data disclosure	Data owner can choose public scope

IV. CONCLUSIONS

In this paper, we propose a method for verifying integrity by applying KSI to the precision medicine system which is selected as the leading field of the 4th industrial revolution to secure and efficiently use sensitive data of big data scale.

Top executives working in the medical field are also aware of the importance of integrity assurance for sensitive data in realizing a precision medicine system.

In addition, KSI, which has been verified and utilized by the US Department of Defense, EU, and NATO, can be applied to a precision medical system in order to efficiently process big data, thereby improving the speed of sensitive data processing compared to the conventional PKI.

In the future, we intend to verify the security and efficiency of the proposed method through really PKI and KSI implementation after collecting data on precision medicine components

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2017R1E1A1A01075110).

REFERENCES

- [1] B. Obama, "The Precision Medicine Initiative", <https://obamawhitehouse.archives.gov/precision-medicine>, January 2015.
- [2] "Promoting 'personalized medical care' and 'securing future growth engines' through precision medicine", Ministry of Health & Welfare, August 2016.
- [3] K. Safavi, B. Kalis, "Digital Health Tech Vision 2018 – Intelligent Enterprise Unleashed", Accenture Consulting, May 2018.
- [4] "What is precision medicine?", <https://ghr.nlm.nih.gov/primer/precisionmedicine/definition>, December 2018.
- [5] A. Buldas, A. Kroonmaa and R. Laanoja, "Keyless signatures' Infrastructure: How to Build Global Distributed Hash-Trees", Nordic Conference on Secure IT Systems, Ilulissat, Greenland, pp. 313-320, October 2013.