Sağlık Sistemleri için IoT & Akıllı Sözleşme Kuralı Tabanlı Güvenli İletişim Tasarısı

Aslı Kul[1], Eda Nur Azin[1],Oğulcan Özdemir[1], Serap Sahin[1]
[1]Izmir Institute of Technology, Computer Engineering, Turkey
{aslikul, edaazin, ogulcanozdemir, serapsahin}@iyte.edu.tr

Özet. Nesnelerin İnterneti (IoT) gelişimini sürdüren yeni bir teknolojidir. IoT sensör cihazlarının kullanım amaçlarından biri de kritik bir alan olan tıbbi sağlık sistemlerinde hasta koşullarını izlemektir. Tıbbi cihazların, sensörlerin, uygulamaların entegrasyonu, dijital servisler ve ilgili verilerin gizliliği, doğruluğu ve kullanılabilirliği açısından kritik öneme sahiptir. Bu bildiride, IoT tabanlı sağlık sistemi yapısı tasarlanmış ve çeşitli saldırı türlerine karşı sistemin kullanılabilirliği test edilmiş Bockchain temelli akıllı sözleşme yapısının IoT sistemlerine entegre edilmesiyle sistemin davranışları Calvin ve Etherium Frameworkleri kullanılarak simüle edilmeye çalışılmıştır.

Anahtar Kelimeler*:* Nesnelerin interneti, güvenlik, gizlilik, blok zinciri, akıllı sözleşmeler, very gizliliği, sensor iletişimi, sağlık, ataklar.

IoT - Smart Contract Rule Based Secure Communication Scheme for Healthcare System

Aslı Kul[1], Eda Nur Azin[1],Oğulcan Özdemir[1], Serap Sahin[1]
[1]Izmir Institute of Technology, Computer Engineering, Turkey
{aslikul, edaazin, ogulcanozdemir, serapsahin}@iyte.edu.tr

Abstract. The Internet of Things (IoT) is a new technology that its expansion increases. One of the using purposes of sensor devices is to monitor patient conditions in a critical area as medical healthcare systems. The integration of medical devices, sensors, applications have critical importance from the point of privacy and correctness and availability of digital services and related data. In this paper, an IoT backbone healthcare system was designed and tested its service availability with against frequent security attack types and a Blockchain based smart contract structure is also integrated with IoT systems and behaviors of whole system were tried to simulate by Calvin and Etherium Frameworks.

Keywords*:* Internet of things, security, privacy, blockchain, smart contracts, data privacy, sensor communication, medical, healthcare, attacks.

1 Introduction

The Internet of Things is a technology that consists of millions of physical devices worldwide to connect and transmit data to each other through the Internet. It is expected to increase its expansion to be usable in critical areas such as healthcare system or medical industry. Currently, sensor devices based on patient monitoring systems are being used in hospitals. Making these devices cooperation with the Internet of Things (IoT) devices, provides controlling strength and brings advantages of using IoT which are easy monitoring, sharing, and increased usability of collecting data to analyses. Besides that, healthcare purposes IoT system devices contain important patient data with sensitive contents. While the IoT creates a more effective and useful smart world, the work on its security and privacy has increased importance due to the fact that they are designed as lightweight devices and current security approaches are not enough for it.To provide secure IoT systems, different level security measures such as using encryption, secure protocols etc. are used but to manage IoT devices using central authority is one of the other main important problems.

On the other side, Blockchain (BC) is the other popular research area and it consists of time-stamped series of immutable records of data that is managed by the cluster of computers not owned by any single entity. Those key attributes of Blockchain; Peer-To-Peer, Distributed, Cryptographically Secured, Add-Only, Consensus makes it better than traditional approaches. Researches are going on IoT security with the idea that "Integrating Blockchain technology with IoT" can eliminate some security deficiencies.

In this paper, our aim is to provide a secure and smart IoT system for a hospital with integration of Blockchain technology. For this purpose, we design a schema and develop a system using the Digital Certificate scheme and smart contract structure. To prove the system, we develop a simulation environment and test it for some possible attacks.

The paper is organized in five sections: In Section 2, the proposed solution is described to offer security and privacy in IoT based medical industry. Then Section 3 presents implementation results and analysis. In Section 4, some related projects with the security of IoT healthcare systems and their solutions are examined. Section 5 purposes possible future security needs, challenges and perspectives in IoT based healthcare system to conclude in this project paper.

2 Proposed System

The medical purpose secure IOT environment is created for a hospital in this project. The system is built upon 3-layer architecture from bottom to up as shown in Figure 1.

1. **IOT Layer:** In the IoT layer, there are medical IOT devices which consist of EEG, EMG, ECG, glucose monitoring (CGM), insulin pen, temperature sensors, etc. They just collect data and send these data to collectors.

2. **Collector Layer:** Collectors are head clusters. They collect data from devices and defined for each patient in a room. Collectors are used by an Id card for each patient. Data for each patient is signed by Digital Signature Algorithm- DSA when transferring collected data from the collectors to data storage at the application layer.
3. **Application Layer** (Cloud, Db, Web Server, etc)**:** The application layer hosts top-level devices for the medical data storage in cloud or web service. Also besides it gives service to users as client agents with mobile phones, tablets, and personal computers.
4. **Certification Authority:** The certification authority fulfills identification requirement with Public Key Infrastructure-PKI scheme [2] in the system which will be using secure communication between devices in the network. Also ensuring safe initialization vector for the smart contract deployment, which binding identity of authorized system user to smart contract base administration properties.
5. **Ethereum - Smart Contracts:** The smart contracts provide safe and distributed control over data flow in the network with PKI scheme.
   Moreover, three layers share management, authentication, authorization, access control and secure communication properties [1] over the Calvin framework

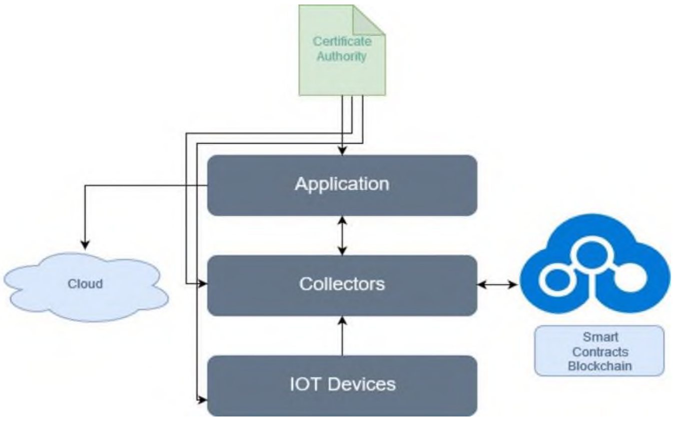


Fig. 1. General components of the proposed solution.

2.1 System Design

Scenerio. In this solution every device and users in the network have public certificates used to identify their role and capabilities in the system. Devices and all entities have the pre-installed certificate before deploying in the system signed by Certificate Authority-CA, which are verified by the ministry of health.

All employees of hospital can use this system by registering to the system and they have id card that enabled by PKI scheme as built in. Each device is defined with related rules to a collector by admin. After the initialization of the device the hospitalization of patient, his/ her admission and verification and registration on the system is done by authorized person. Health data of patients is collected via IoT devices, and send to the collectors.

A smart contract holds rules for each specific device to verify received data content of IoT devices whether having permission to send those types of data to upper layers or not.The smart contracts are distributed to each collector and application layer devices, so all of them have replicas of it. With a smart contract, the device data structure is validated based on the sender device or group id of the sender certificate. IoT layer devices only send data and do not hold smart contract information. If collectors verified the data according to define rules, it sends them to the database to record otherwise it does not accept it. As shown at Figure 2. While data is sending to the cloud it is signed with private key of patient, thus the identification of the source of received data is provided.

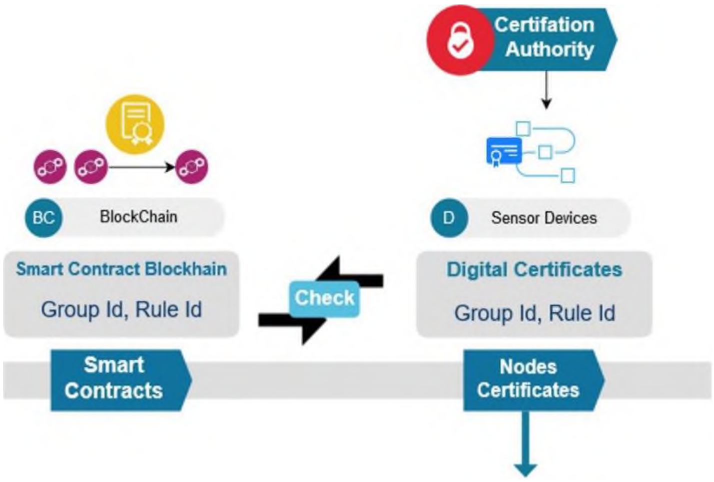


Fig. 2. Group & Rule ID checking while sending data from devices to collectors

Use Cases Requirements. The following use cases and requirements are defined to clearly explain proposed solution.

Actors: IoT Device, Collectors, Certificate Authority, Doctors, Nurses, Patients, Ministry of Health

1. **Rule Policy Definition:** In proposed solution rules are placed in a smart contract. They define which device group can send which type of data. For this purpose each rule is defined as a unique Id and stored as a table entity in the cloud, each contract contains rules against a specific device or group of devices.
2. **Device Registration:** The IoT, collector, and application layer devices are registered to the system to be able to collect and send patients' data from IoT devices and send these data from IoT devices to the collectors.
3. **Patient Registration:** The system gives Id to the hospitalized patient.The given room or defined department for the patient such as the intensive care unit or the

others are recorded to the system as a department, room and bed Id and associated with each other, together with the patient Id and device's Id.

4. **Smart Contract Installation:** The initial chain is started by the authorized system user (admin) with the deployment of rule manager that is a smart contract. Each device has rule policy either dependent for its id or affiliated subgroups such as group, room or floor id. The smart contract also known as a rule manager.the smart contract and each rule contract is only deployed by admin, rule manager smart contracts have a unique feature.They hold and call the registered rule contracts.The rule contracts are specific for their purpose and every rule control against deployed contracts are added as a log to the transaction records.
5. **Certificate Distribution:** Certificates are distributed while registration phase alongside with smart contract client node installation. They contain the necessary extension fields for identification and rule control management and all nodes use certificates to establish a secure communication channel. HTTPS underlying SSL/TLS handshake protocol, the Ministry of health verifies the trustability of the certification authority. In addition, the group ids in the smart contracts and certifications meet the id specifications in x509 standards.
6. **Get Data from Patient:** The main reason to collect data with IoT from patients is to improve the diagnosis and treatment process. The proposed solution implementation combine IoT device data signed with patients' smart identification card which has a built-in PKI scheme [2] with patient's previous data.
7. **Data Collection from Devices*:*** In this solution, data are collected from the IoT devices then send to the collectors by using secure protocol that meets TLS requirements. After successful TLS handshake, device group ID is extracted from IoT certificate by collector and used to find smart contract that holds rules for specific device group. If the data content is approved, the data are sent to the cloud to save data to the database over a secure channel by using the collector certificate.
8. **Save Data to DB:** For the data collected from patients, the hash value is generated by the collectors. Private keys on patients' smart cards are used to sign the hash of the data and then it is sent to the server to save data with their hashes (digital signatures). The database does not accept the data without the hash value of it and check the integrity and identity of the data by verification digital signature process.
9. **Access Patient Data:** The system use a secure communication channel to take the patient's data from the cloud server.

Securiy Requirements And Solutions. For proposed solution in order to offer authentication and identification requirements of the system, the SSL/TLS certificate on PKI scheme was used. In a network, transactions cannot take place without the capacity to digitally identify people and machines in a reliable way. Public Key Infrastructure (PKI) is responsible for offering services required for establishing trusted digital communications [3]. Figure 3 shows that scheme.

In our project rule-based data transformation was set up between layers with using certificates and X509 infrastructure. Certificates include device id, group id for different device types in their extension fields. Each Device id consists of 96 bits electronic product code. Grup id defines device types and collectors so the system is protected against false data injection. All Ids are queried from Rule Authority.

Communication security between all layers such as IoT to collectors and application is provided by the HTTPs protocol with underlying SSL/TLS certificates. Https provides secure communication and confidentiality at a network. Data is sent by HTTPS that is secured via Transport Layer Security protocol (TLS), which provides three key layers of protection.

1. **Encryption:** Encrypting the exchanged data to keep it secure from eavesdroppers. That means that while the user is accessing network, nobody can "listen" to the conversation.
2. **Data integrity:** Data cannot be modified or corrupted during transfer, intentionally or otherwise, without being detected.
3. **Authentication:** Proves that users communicate on network. It protects against men-in-the-middle-attacks and builds user trust, which translates into other business benefits.

Attacks and Prevention. Some IOT devices and IOT network of attacks that may be encountered are listed below. Through the use of certificate authentication and Rule-based approach those types of attacks are prevented for all layers in this system. At IoT layer, false data injection, sinkhole attack, and reply attacks are prevented by rule authority system underlying smart contract infrastructure [12]. Communication channels security is providing by HTTPs underlying the SSL/TLS certificate scheme.

1. **Spoofing Attack:** In the IoT sensor network, IP spoofing is a common way to use while attacking the network. In this project requester identification from a unique X509 based certificate system protects the IoT network from this type of attack.
2. **Node Capture Attacks*:*** Wireless Device Networks may be assortment of sensors with restricted resources that collaborate so as to attain a standard goal. The proposed system has a smart contract based rule control on data over the network which distributed to each collector. Once data arrived to the collector, smart contract id is extracted from sender certificate and data is checked with appropriate smart contract.
3. **Sinkhole Attack:** Sinkhole attack is a corporate executive attack that was an entrant compromise a node within the network and launches an attack. In proposed system sinkholes are named as collectors. Even if one of the collectors is compromised, system also has rule policy control at the application layer.
4. **Replay Attack:** A replay attack is an attack on victimization of the safety protocol. The proposed system does not allow processing of this type of unlegitimate requests by the checking of timestamp within each request.
5. **False Data Injection*:*** Due to their comparatively tiny sizes and unattended operations; sensing of IoT nodes has a high risk of being captured and compromised. False sensing reports is injected through compromised nodes, which might cause not solely false alarms, however additionally the depletion of restricted energy resource during a battery power-driven network. False data injection types of attacks are intercept by using the IoT-Blockchain based infrastructure.

3 Experiment and Analysis

3.1 Used Technology

The technologies used to set up the targeted system can be listed as written.

1. **Calvin Framework**: Ericsson Calvin framework [1] is used for convenient and reliable environment to develop and manage runtime IoT devices and networks and abstracts the hardware and network dependency.
2. **Digital Certificate:** Digital certificate scheme widely common security solution for digital identity problem. This leads to generating a trust chain among certificate authority to its certified branches to trusted entities
3. **Smart Contract:** Smart Contract is a self-employed software agent that ensures to be run in certain predetermined actions and provide a digital agreement structure that does not need any intermediate carry out contract procedure.
4. **Ethereum:** Distributed application scheme forge opposed to hindrance, deception, and intervention from a third party and it is also Turing complete language runs over Blockchain provide the environment for developers who build up and publish distributed applications.
5. **Solidity:** Solidity is an object-oriented programming language that uses for smart contracts development.
6. **Note:** Remix Ethereum IDE [7], web3 library and GETH (go implementation ethereum) [6] are used for smart contract side simulation, development, and deployment.

3.2 Simulation Setup

In this simulation, there are 3 nodes that represent the initialization smart contract chain in the boot node, collector node that first rule control phase and storage node for storing data. IoT sensor devices placed under collector since its data only pass through the collector.

Environment for Security: The proposed system relies on tested and vastly used security schemes for low-level network layers, provides protection solutions against. These types of attacks require inspection on data structure, the identity of data, and data flow control.

Data structure inspection will be controlled by distributed smart contract based rules. Thus provide convenient and immanent reaction against structural attacks. Identity of data is ensured by the PKI scheme. Data flow control provisioned with the HTTPs scheme.

Environment setup for Performance: Since every component of the test environment run fully virtual on one device we can estimate performance on the real devices from the benchmark result of current IoT devices hardware capabilities. [4,5]

In perspective of IoT devices additional workload is limited to making HTTPs request to the collector. Collector wise performance split into two process lines. First, receiving requests from IoT devices then processing. (Identification of the device, rule control based on the identification of requester) Second data hash is signed by a patient smart identification card built in a PKI scheme [2]. Collectors are highly capable of this type of processing. Cloud storage stance to data processing is dependent on the performance scalability of cloud server hardware. The test environment runs on the device has i7 4700MQ Intel processor, 16Gb RAM, and 256Gb SSD hard drive.

Simulation setup steps:

First installation of proper version for mentioned frameworks. After that initializaed of Ethereum private network that uses Proof of Authority as a consensus for local machine using puppet side executable program that comes with the go-ethereum package [6].

Two sealer node added for Proof of Authority consensus model. The rule Manager smart contract is deployed to this network using Remix IDE [7] and web3 node js library.The deployed contracts are shown on Remix IDE [13].Lastly with configuration and deploying mock IoT device into Calvin runtime using Calvin GUI (Figure 3) the simulation setup was finished.

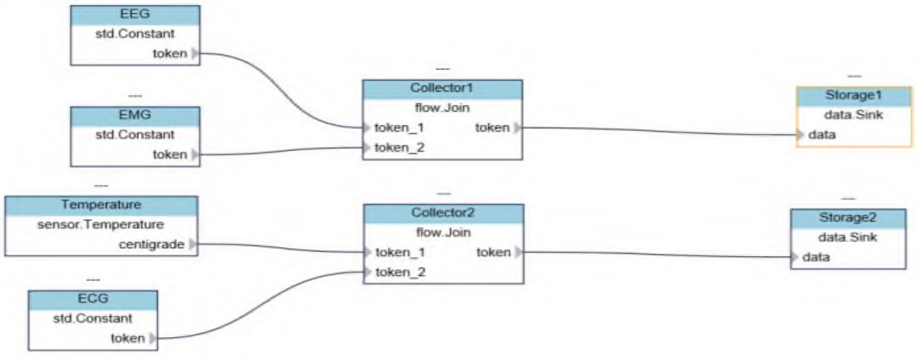


Fig. 3. Deployed mock IoT device into Calvin runtime on Calvin GUI.

3.3 Analysis

In this stage some scenarios were tested and resulted in simulation environment.

Performed Tests.

1. **Load Test on Collector:** In this test we want to measure response time for various counts of requests in the same collector at once. Approximate response time for data

store requests from IoT nodes to collector was measured. In the network configuration block mining time was set to 5 seconds. Thus leads to minimum response time to 5 seconds. Moreover, simulated collector handled specific count of requests. As shown from Figure 5 performed 10, 100 and 1000 simultaneous requests resolved in 5.72, 10.81 and 30,25 seconds consecutively.

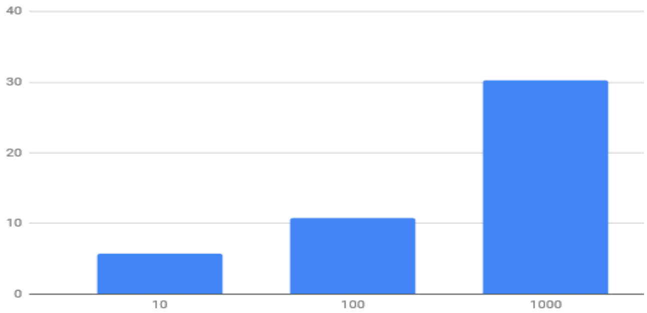


Fig. 4. Request / Response count

2. **Secure Communication Test:** We used openSSL [8] to generate certificates for authority and X509 certificates for IoT nodes, and collectors. Afterwards, certificate authority signed generated certificates for IoT devices and collector nodes. During the tests, simulated collector verified sender IoT nodes' certificates with challenge against certificate authority trust chain control. We observed that If the sender's supplied certificate was not in trust chain of certificate authority this request was rejected by simulated collector as expected. The simuşated nodes deny unsecure HTTP request by default.
3. **Using certificate extension field to interact rule smart contract:** In this test, we checked whether our system successfully extracts requester IoT node group identifier from supplied certificate X509 extension field. Thus leads to acquire trusted information about the identified sender with non repudiation property. Then performed smart contract tests shows that proper smart contract transaction committed based on group identifier.
4. **False data injection attack control:** To test against this type of attack, one of the simulated IoT nodes acted as compromised and sent false data to the simulated collector. Subsequently, the collector verified compromised node certificate. Then, commited new rule smart contract transaction with supplied group identifier in certificate. Therefore, the result of transaction was negative. Thus, proposed system prevents false data to transmitted cloud-storage.
5. **Ethereum Private Network Initialization:** In system preparation phase, we conducted a test deployed collector and cloud-storage nodes properly bootstrapped their blockchain miners. For that one bootnode was deployed to test environment act as negotiator. Simulated collector and cloud-storage were used as sealer nodes. Afterwards, we identify two sealer nodes start to negotiate block mine phase synchronously in nodes' transaction logs.

6. **Deploying Rule Smart Contract:** To test this scenario we generated ethereum private account as authorized system user and deployed it as private network with one bootnode, one sealar, one transaction node. Then deploy smart contract with authorized account to ethereum private network using geth command line tools. Subsequently, we observed that deployed smart contract acknowledged with nodes in private network.

4 Related Works

How to implement IoT in secure way and what are intended solutions' positive and negative sides were investigated in many different prior works. Some of the related studies are explained and compared to our study.

In [9], they suggested a framework called "Privacy Protector", which aims to give protection for patient's privacy, and protected data collection in IoT based healthcare applications because there are attacks against patients' data such as collusion attacks and data leakage and destruction attacks. The framework has two main properties: (i) the secret sharing uses Slepian Wolf coding based secret sharing (SW-SSS) in an attempt to optimize the secret share size, (ii) the other one is share repairing if the data loss or compromise. To apply these properties, they collect data from IoT devices to a communication service provider (CSP). CSP uses the SW-SSS scheme to forward data. In our approach, we use the collectors instead of CSPs for collecting patients' data. In the case of loss or compromise of the data, CSP creates and shares the data again. Doing lots of calculations are required, when we think about lots of the devices sending the data to the collector. To avoid additional computation to repair data, we define rules for the device groups, and according to the rules we control the behavior of the devices. In this way, we prevent data loss or corrupted data.

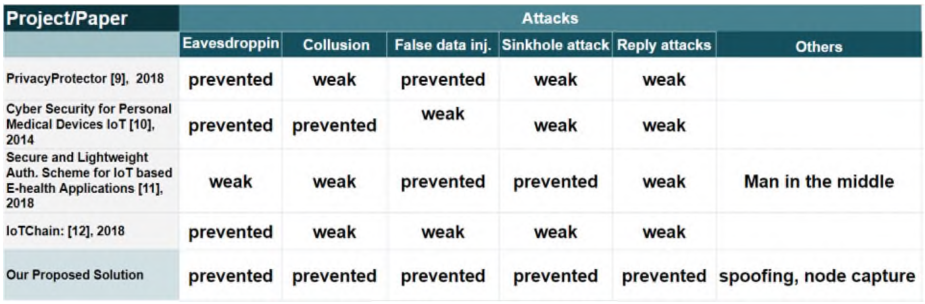
And the other focus area of mentioned project is while storing data, the mentioned project provides data storage security with using data access control method, in our project all user nodes have public private key pairs, digital certificates and accessing and transmitting data.With this aspects while mentioned project is focusing on only access control and data protection on storage, in our project has multiple security prevention solutions both while collection, transmission , accessing , storing steps multilevel.

The article [10] mentions about cyber threats to personal medical devices and they present solution approaches. They suggested that used to lightweight cryptographic protocols for encryption of patient's data, then record on the cloud-based PHR (Personal Health Record) service. The data can be seen by authorized entities and verification of these entities can be done by using symmetric or asymmetric cryptographic protocols.

In this study, they work with personal medical devices, so devices are used by a specific person. However, in the hospital environment, devices can be assigned, different people. To deal with this situation, we match the patient and the device at the application level by authorized people. In the article, the encryption scheme is designed for medical devices. However, the constraint on the medical devices' memory causes the limited encryption scheme. This is a disadvantage for the system because it is vulnerable to cyber-attacks. Due to these memory limitations, we offer a rule-based approach by building up a smart contract scheme and use collectors, which have higher capacities than IoT devices.

In the paper [11], they suggest a secure and lightweight authentication scheme using elliptic curve cryptography for IoT based e-health applications. They collect data from nodes to a head node, then, sends it to the base station. A head node is an IoT device with a limited capacity to make calculations. In this way, they studied with the small size of the keys.In our approach; we studied with collectors to prevent limited memory issues. Collectors take the hash of the data with the patients' private keys to protect the integrity of the messages and to provide authentication, we also suggest the certification scheme.

Table 1. Comparison of related works against our project for attack types.



Project/Paper	Attacks					
	Eavesdroppin	Collusion	False data inj.	Sinkhole attack	Reply attacks	Others
PrivacyProtector [9], 2018	prevented	weak	prevented	weak	weak	
Cyber Security for Personal Medical Devices IoT [10], 2014	prevented	prevented	weak	weak	weak	
Secure and Lightweight Auth. Scheme for IoT based E-health Applications [11], 2018	weak	weak	prevented	prevented	weak	Man in the middle
IoTChain: [12], 2018	prevented	weak	weak	weak	weak	
Our Proposed Solution	prevented	prevented	prevented	prevented	prevented	spoofing, node capture

An Ethereum Blockchain based approach to provide security to the IoT devices is used at Alphand et al. [12]. They offer a security architecture called IoT Chain to provide access control to the IoT devices and use the OSCAR scheme and the ACE framework to secure authorization while accessing the IoT resources. IoT chain use Blockchain generate access control tokens with Ethereum smart contracts scheme. In our system smart contracts use for rule policy control for transmitting data.

In our study and their studies have similar approachs like: Both smart contracts are used and combined with the Blockchain. In their study, a smart contract is defined by the resource owner. In our study, a smart contract is published by an authorized person (admin of the system). For authentication of the clients or IoT devices, both studies are used third parties (i.e key server, certification authority).

5 Conclusion

In this paper, we have investigated the effects of using the IoT-Blockchain based infrastructure in healthcare system. In 3-layer architecture which consist of IoT devices, Collectors and Application Layers all nodes are certificated. With intended approach, smart contracts were used to apply rule based access to nodes in order to check data contents of devices. For all communication between layers, rules in smart contracts are verified and security and data privacy are thus provided. As in the table 1 and table 2 the proposed solution shows that the rule based smart contract IoT system may be used as a preferable solution to prevent most known attacks to provide secure communication environment and to achieve main security goals. As a result of performed tested in this project analysis shows that IoT - Smart contract rule based schema offers solution for common security problems in IoT sensor networks.

References:

1. EricssonResearch - https://github.com/EricssonResearch/calvin-base/wiki/Security
2. Method for enabling PKI functions in a smart card - https://patents.google.com/patent/US7024226B2/en
3. Advantages of Public Key Technology, Safelayer D - https://www.safelayer.com/en/resources/59-articles/public-key-infrastructure/421-advantages-of-public-key-technology
4. J. Esquiagola, L. Costa, P. Calcina, G. Fedrecheski, M. Zuffo, “Performance Testing of an Internet of Things Platform” , Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security - 2017
5. R. Morabito, “A performance evaluation of container technologies on Internet of Things devices”, IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) – 2016
6. Puppeth - https://github.com/puppeth/go-ethereum
7. Remix IDE Documentation. https://remix.readthedocs.io/en/latest. (accessed 05 29, 2019)
8. Openssl https://www.openssl.org/(accessed 05 25)
9. E. Luo, M. A. Bhuiyan, G. Wang, M. Rahman, J. Wu, and M. Atiquzzaman, Privacy Protector: Privacy-Protected Patient Data Collection in IoT-based Healthcare Systems,IEEE Communication Magazine (COMMAG), 56(2): 163-168, 2018
10. A. Mohan, “Cyber security for personal medical devices Internet of Things,” Proceedings of the IEEE International Conference on Distributed Computing in Sensor Systems, 26-28 May, 2014, pp. 372-374.
11. M. Almulhim, N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications", *Advanced Communication Technology (ICACT) 2018 20th International Conference on*, pp. 481-487, 2018.
12. Olivier Alphand, Michele Amoretti, Timothy Claeys, Simone Dall ’Asta, Andrzej Duda, et al..IoT Chain: Blockchain Security Architecture for the Internet of Things. IEEE Wireless Communications and Networking Conference, Apr 2018, Barcelona, Spain. 2018.