IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 20, 2022, accepted January 31, 2022, date of publication February 4, 2022, date of current version February 11, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3149046

FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs

ZEESHAN ZULKIFL[1], FAWAD KHAN[1], (Senior Member, IEEE), SHAHZAIB TAHIR[1], (Senior Member, IEEE), MEHREEN AFZAL[2], WASEEM IQBAL[1], ABDUL REHMAN[1], SAQIB SAEED[3], AND ABDULLAH M. ALMUHAIDEB[4]

[1]Department of Information Security, College of Signals, National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan
[2]Department of Cyber Security, Air University, Islamabad 44000, Pakistan
[3]Saudi Aramco Cybersecurity Chair, Department of Computer Information Systems, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia
[4]Saudi Aramco Cybersecurity Chair, Department of Networks and Communications, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia

Corresponding author: Shahzaib Tahir (shahzaib.tahir@mcs.edu.pk)

This work was supported by the Saudi Aramco Cybersecurity Chair, Imam Abdulrahman Bin Faisal University.

ABSTRACT Internet of Things (IoT) is a system of interconnected devices that have the ability to monitor and transfer data to peers without human intervention. Authentication, Authorization and Audit Logs (AAA) are prime features of Network Security and easily attained in legacy systems, however, remains unachieved in IoT. The IoTs require due security considerations as the conventional security mechanisms are not optimized for such devices due to various aspects such as heterogeneity, resource constrained processing, storage and multiple factors. Additionally, the legacy systems are mostly centralized and thus introduce a single point of failure. In this research, a novel framework, FBASHI is presented that is based on fuzzy logic and blockchain technology to achieve AAA services. The proposed system is developed using Hyperledger that is a blockchain platform providing privacy and fast response capability, therefore, it is best suited for the healthcare IoT environments. This work proposes behavior driven adaptive security mechanism for healthcare IoTs and networks based on blockchain by utilizing fuzzy logic and presents a heuristic approach towards behavior driven adaptive security providing AAA services. FBASHI is implemented to analyze its security and practicality. Furthermore, a comparison is drawn with other blockchain-based solutions.

INDEX TERMS Hyperledger, trust management, authentication, contextual access control, MFA.

I. INTRODUCTION

IoTs have emerged as a revolutionary technology capturing the world at a fast pace. IoT combined with AI, blockchain and 5G are taking the world into era of contextual connectivity enhancing personalized human experience. The IoTs are epicenter of this revolution threatened by diversified attack vectors. Gartner has projected the IoT security expenditures to hit $3.1 billion by 2021 [1]. Being resource constrained, IoTs rely on traditional security mechanisms like passwords that are susceptible to variety of attack vectors. As a result IoTs can be easily compromised due to insecure remote access [2].

Electronic healthcare refers to the monitoring, maintenance and improvement of the health of a patient by the use of digital technologies and telecommunications. The healthcare sector is rapidly adopting the IoT technology and transforming the hospital centric healthcare services to home centric healthcare services. Either way the modern healthcare services are dependent on IoTs and trust is the foundation of security and privacy in healthcare. IoTs have the weakest link when it comes to trust as these devices are interconnected and usually dependent on traditional security mechanisms which usually imply a centralized architecture which is incompatible with IoTs.

Blockchain is an emerging technology which has many intrinsic features including decentralized applications (Dapps), decentralized trust, transparency, immutability and provenance [3]. Due to its property of decentralized trust and immutability, blockchain has the potential of providing foolproof security for IoTs specially in the healthcare environment [41], [42]. The healthcare devices are service

The associate editor coordinating the review of this manuscript and approving it for publication was Giovanni Pau.

critical that record sensitive patient data for smart diagnosis, AI driven disease profiling, vitals management etc. Any malfunctioning within the IoT devices can lead to severe consequences, for instance, a smart ventilator machine's failure can be instantly fatal for an ICU patient. Recently a vulnerability was discovered in GE Aestiva and Aespire anesthesia devices that allowed a hacker to bypass the authentication mechanisms and manipulate the drug levels causing serious health injuries to patients which could be fatal [4]. Similarly, there is a breach of trust when insiders compromise the sensitive healthcare data of patients and sell it in the black market for personal gains. To protect the privacy of the individual's data, HIPAA and GDPR pose heavy fines on the organizations that mishandle or leak the data of the patients without their prior consent [5], [6]. Furthermore, often the IoT device manufacturers do not comply with the security standards while designing such healthcare devices and security is usually an after thought. This leads to the necessity of having adequate security mechanisms in place which are diverse and comply with modern health standards like HIPAA and GDPR.

Access Control and Identity Management has been an Achilles heel for IoTs due to their heterogeneous nature and scalability issues. Ownership and identity relationships in the IoT are closely related to the authentication and authorization of the devices and the individuals respectively. The owner of an IoT device may change over time and may be asked for authentication. Moreover, the data collected by a device needs proper authorization mechanisms in order to ensure privacy and traceability. The conventional authentication mechanisms like passwords are no more effective and most of the devices are compromised due to folk model implementation of security in these devices by manufacturers. No standard security protocol exists for IoTs, hence, a number of proposed authentication and authorization protocols exist [10], [20], [21] [22], [25] [31]. These protocols lack different aspects in terms of security and efficiency for IoTs and subsequently discussed in succeeding section.

In this research, we leverage blockchain technology to tackle highlighted issues in healthcare IoTs through Hyperledger's certificate based identity solution avoiding third party reliance and achieving distributed trust. Furthermore, fuzzy logic handles uncertainty of device behavior through context and trust-based driven logic providing adaptive security mechanism for IoT and other network devices.

A. CONTRIBUTIONS

The following contributions are made to the healthcare industry through this research:

- This work addresses the authentication and trust issues in IoTs for healthcare through a novel approach using blockchain enhancing security.
- This paper utilizes fuzzy logic for adaptive authentication and authorization mechanism providing AAA services without a central server, third party reliance and avoiding password-based security mechanisms.
- The proposed system "FBASHI" is implemented and a comprehensive security and performance analysis is performed. FBASHI is proven to be practical and security-wise effective for IoT-based distributed architectures.

B. ORGANIZATION

Section II discusses the existing authentication protocols in healthcare IoTs including the ones utilizing blockchain by briefly discussing their pros and cons. In Section III preliminaries related to blockchain-hyperledger and fuzzy logic are presented to enhance the understanding of the proposed healthcare security framework. Section IV discusses the proposed framework via a scenario that aids to formalise design goals. Section V discusses the threat model by highlighting the attack vectors and the mitigation strategies that are put in place within the proposed framework. Section VI provides comparative analysis against the state-of-the-art. This section also gives performance-based analysis for practical usecase. Conclusion and future work is drawn towards the end in the Section VII.

II. RELATED RESEARCH

Many IoT-based authentication protocols have been designed but only few exist that are specific to healthcare-based IoTs [7] [8]. Amin *et al.* [10] proposed anonymous password based authentication protocol for wireless medical sensors. The protocol utilizes hash function and session key for mutual authentication verified by BAN logic model. Jiang *et al.* [9] improved password-based authentication work of [10] both protocols rely on password-based authentication which is susceptible to guessing attacks and weak password vulnerability. Ferag *et al.* [11] has carried out a comprehensive survey of around 40 authentication protocols designed for IoT. These protocols mostly cater for a specific attack in IoT domain and does not provide a comprehensive solution. Due to ubiquitous and heterogeneous nature of IoT, access control and identity management are a major concern. Riveria *et al.* [12] used OAuth 2.0 to define an access control model for IoT. The drawback of this model is that it relies on third-party services and centralized architecture. Significant work exists on authentication mechanism and access control but few of the approaches incorporate both [13]–[15]. Identity-based access control models have a central identity server or a trust server to manage the access control [16]–[18]. These servers induce a single point of failure and makes system less resilient to network attacks. DTLS protocol have been used to achieve security in IoTs [19]–[22] but all of these lack MFA, dynamic access control and are resource intensive.

Blockchain has some intrinsic security properties such as distributed trust, transparency, immutabilty, etc, which can be utilized for achieving overall security for different systems [23], [24]. Zyskind *et al.* [25] used blockchain to ensure privacy of user data but only utilized blockchain for storing access control information thus wasted the true potential of blockchain. Similarly, Gauravaram *et al.* [26] utilized blockchain to store access control policies to achieve immutability and distributed property but did not apply identity management and authentication mechanisms. Furthermore, their approach underutilized blockchains computational capability. Ouddah *et al.* [27] utilized true computational potential of blockchain to achieve decentralized access control. They used access tokens for delegating access rights to other peers through transactions. The access control policy was part of a locking script which has to be unlocked by possessor to prove he has the token. The computational capability of locking script is limited than the smart contract thus this model is less efficient. Zhang *et al.* [28] utilized smart contract which is a feature of Ethreum Blockchain for access control in IoTs. Their architecture is designed around gateways and thus gateways are assumed as a trusted entity and not truly verified. Ramachandran [29] also utilized smart contract for access control but they only stored access control policies, time of day, signature of last change and logs etc. Qu *et al.* [30] used Blockchain to verify credibility of an IoT device. The model uses gateway as a trusted entity for connected IoTs. Azaria *et al.* [31] utilized Blockchain to access, store and modify health records. Their model only ensures security of health-related data instead of the underlying system. These approaches [28], [29], [31] are based on Proof of work consensus model which has inherited 51% problem making it vulnerable to cyber attacks. Kim and Lee [32] implemented Zero-knowledge proof on authentication server to protect data of smart meter stored on Blockchain. They used primitive method of username password-based authentication which necessitates the use of authenticating server introducing a single point of failure. Banerjee *et al.* [33] has suggested a blockchain-based solution for compromised firmware detection and self-healing. They stored the Reference Integrity Metrics (RIM) on the blockchain to ensure its integrity. Huh *et al.* [34] proposed a blockchain-based IoT management system which manages the electricity usage of a smart meter by implementing Ethereum smart contract. Different Blockchain solutions [35]–[37] were analyzed based on security, scalability and compatibility; and Hyperledger Fabric was found best suitable for healthcare domain being consortium blockchain ensuring privacy, scalability and compatibility with other systems.

For IoT an efficient mechanism is required for authentication and authorization based on trust as many devices work mutually and if a single device acts maliciously it can compromise the whole network. Fuzzy logic-based systems can quantify trust to handle uncertainty in a better way and can be utilized for malicious behavior detection [38]. Mahalle *et al.* [39] have utilized fuzzy logic for access control in IoT but their approach is centralized in nature and introduces a single point of failure in the system. Furthermore, their approach has scalability issues as all trust logic is centrally located. Walker [40] has generalized the idea of risk-based authentication and emphasized upon its application in IoT domain. Thus, risk-based authentication forms the basis of our concept for adaptive security to achieve trust and access control in healthcare environment.

III. PRELIMINARIES OF PROPOSED SCHEME

The proposed scheme is based on Hyperledger Fabric and Fuzzy logic. This section explains the preliminaries for the understanding of Adaptive Security Framework. Each term is explained briefly below:

A. BLOCKCHAIN ELEMENTS

The entities involved in Blockchain and their associated terminologies are discussed below:

- **Client** Clients are the end users which are not directly involved in blockchain process but the main entities involved in transactions In our case SP (Service Provider) and RE (Requesting Entities) are clients in our case and they interact with blockchain through Anchor peers which in case of SP is a gateway and in case of RE the device itself can also be designated as a peer (Doctor, Nursing Staff, Administrator). The client is also registered to the blockchain network, therefore he has a particular identity and certificate issued by the CA. The clients submit their transactions to blockchain through anchor peer and once a transaction is successful are responded by the same.
- **Anchor Peer** It is an entity which directly interacts with blockchain. It can be RE themselves or a gateway in case of IoTs. It is an SDK client who submits actual transaction-invocation to the endorsers and broadcasts transaction proposals to the ordering service.
- **Peers** Peers are the nodes which are active part of the blockchain network and they perform one or many roles in the blockchain. These are the nodes which are responsible for maintaining the ledger. Following are the types of peers in our blockchain network:
    1) **Endorser** Endorser or endorsing peer is the one which simulates the transaction by running the chaincodes (smart contracts in Hyperledger) related to a particular transaction before it is committed to a block. Every chaincode specifies an endorsement policy which defines all the necessary conditions for a transaction to be termed as valid. Furthermore, the endorsers compare the generated Read Write (RW) sets with existing ones in the ledger and validate individually. Every endorser verifies all the signatures and identities associated with a transaction and each endorser forwards the signed transaction to the anchor peer now called "Endorsed Transaction".
    2) **Committing Peer** It is the peer specified or selected by the Blockchain to commit the transaction to the Blockchain network. The Leading peer as discussed above is usually the committing peer. This peer commits the transaction to the block as

specified by the ordering service and initiates the gossip protocol for ledger update by other peers of channel. This peer can be elected through consensus or may be assigned a specific role.

3) **Ordering Service** Ordering service provides the communication channel to all the participants of blockchain and guarantees deliveries. Ordering service can be implemented in variety of ways using different node fault models. It provides connectivity between clients and peers through channel. Clients broadcast their transaction requests which are broadcast to all peers. The channel supports atomic delivery of all messages.

- **Channel** A channel is a mechanism for managing communication between entities participating in the blockchain network. Channel logically behaves like a LAN where all the data and transactions are private within channel and no data is shared with outside peers. In the healthcare environment data privacy is of utmost importance, therefore, each department has a separate channel and a device or entity can be part of more than one channel. For example, if a doctor has his duty in the medical department but also performs duties in the Emergency ward, in that case he will have two separate datasets for each channel, however his same identity will work across both channels. When a new channel is created, a genesis block is formed which stores the configuration information about the channel policies, members and anchor peers. When a new member is added to an existing channel either the genesis block or a more recent reconfiguration block, is shared with the new member. A leading peer is also elected which is the one which has the responsibility to determine which peer communicates with the ordering service on behalf of the member. If no leader has been designated, than a leader is chosen through consensus. The ordering service orders transactions and delivers them to each leading peer in the form of a block, which then distributes the block to its member peers, across the channel, using the gossip protocol. The propagation of data includes transaction information, ledger state and channel membership, and is restricted to only those peers which have verifiable membership for the channel.
- **Ledger** Ledger provides verifiable history of all successful and unsuccessful transactions occurring over the blockchain. Ordering service is responsible for construction of ledger by maintaining ordered hashchain of blocks of transactions. Hashchain imposes the total order of blocks in a ledger, where each block is an array of totally ordered transactions which formulates an entirely ordered blockchain. All peers have ledgers and optionally orderer can also have a ledger which is called ''Order Ledger''. All other peers have peer ledgers and they can replay the history of transactions to update or reconstruct the ledger state.

B. IDENTITY MANAGEMENT

Identity is an integral part of any IT system; it aids in mapping various actors in an organization to their roles in the system. These actors then verify their identity through authentication mechanisms and are authorized to perform certain actions allowed by the system. Without a centralized identity management, it is a challenge for IT professionals to manage authentication and authorization across wide range of devices. X.509 certificates in Hyperledger Fabric are responsible for provision of detailed identity which is verifiable by the system administrators. In our blockchain-based framework two entities play vital role in identity management that are as follows:

1) CERTIFICATE AUTHORITY (CA)

A Certificate Authority is an entity responsible to dispense certificates to various actors in a network. These certificates bind the public key of the principal with various associated attributes and are digitally signed by the CA. Consequently, if CA is a trusted entity and its public key is known, then one can trust the specific principal as he is having a valid certificate, and owns the included attributes and public key, by validating the CA's signature on the principal's certificate. Three kind of certificates are issued: enrollment certificate, transaction certificate and TLS certificate. CA can be of various types as shown in figure 1 e.g., Root CA, Department CA and local CA. If an entity, for instance, a patient is issued an identity by Root CA his identity will be available in every department. CA role includes:

1) Registration of Identities
2) Issuance of Certificates
3) Certificate Renewal and Revocation

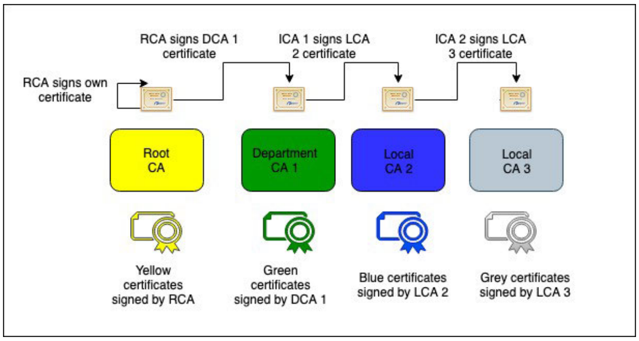

RCA signs DCA 1 certificate
ICA 1 signs LCA 2 certificate
ICA 2 signs LCA 3 certificate
RCA signs own certificate
Root CA
Department CA 1
Local CA 2
Local CA 3
Yellow certificates signed by RCA
Green certificates signed by DCA 1
Blue certificates signed by LCA 2
Grey certificates signed by LCA 3

FIGURE 1. CA hierarchy of FBASHI.

2) MEMBERSHIP SERVICE PROVIDER

Once an Identity is issued it must be verifiable. For this purpose, we require another entity known as MSP (Membership Service Provider). Trust has been further distributed in FABSHI by delegating the responsibility of verification to MSP instead of CA. MSP is also responsible for managing identities once they have been created by the CA. The MSP can also be deployed at any level and depends on the network size and security requirements. A device itself can have an isolated MSP running within which it can verify signatures belonging to other actors of the network. If network is large, several MSPs can be setup. For example, a channel MSP is responsible for verification of all transactions occurring on that channel.

C. AUTHENTICATION FIS

In this research three main Fuzzy Inference Systems (FIS) are used and their designs and logic are discussed in this section for understanding of the architecture. The authentication mechanism is designed to achieve adaptivity through risk assessment based on parameters usually available in the network packets such as HTTP header. The RE will always initiate a transaction request in relation to the context of healthcare. Thus, all transactions must contain patient's ID along with RE and SP ID. We define a Mamdani FIS for our authentication system as shown in figure 2.

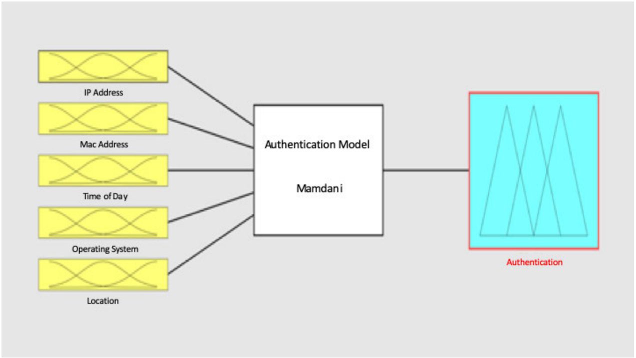
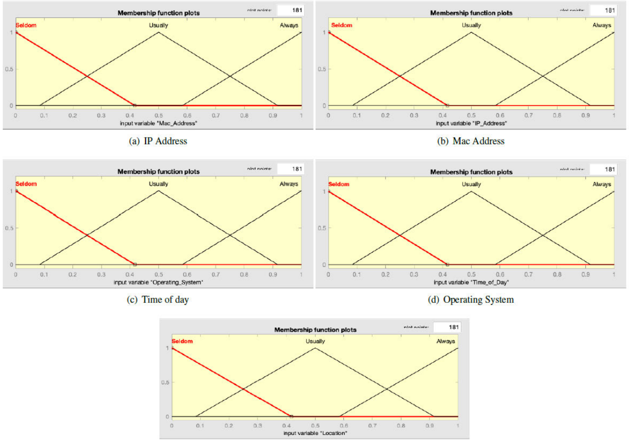


FIGURE 2. Authentication FIS.

The parameters for our framework are IP address, MAC address, time of day, Operating System and location. These parameters will be analyzed in conjunction with history of transactions maintained by blockchain. Each parameter will be analyzed separately and frequency distribution for that particular parameter will be calculated. This frequency distribution is normalized to get the membership functions for each fuzzy set associated with parameter. For example, in figure 3 three fuzzy sets for each parameter seldom, usually and always are shown. The membership function is along the y-axis and set values are along the x-axis.

Mamdani FIS is used to calculate fuzzy output which is type of authentication mechanism. Based on 5 parameters and each having 3 fuzzy sets, 125 rules can be defined for fuzzy system, figure 4 shows 9 rules due to space constraint. In the stated example, the frequency distribution for parameters is 0.206 IP, 0.55 mac address, 0.179 for time of day, 0.133 for Operating System and 0.095 for location. Thus subsequent output of fuzzy system is 0.391 implicating Biometric authentication.

The output contains 3 fuzzy sets of biometric, OTP (One Time Password) and CA and their membership functions are shown in figure 5 according to the given parameters, the MFA is applied and RE is required to authenticate through particular method given by fuzzy output. If the Membership function of device is max for Biometric, than the device will be authenticated through Biometrics. Furthermore, Biometrics and OTP-based authentication also involve an OTP being sent to patient device for endorsement. On successful authentication, a nonce generated by IoT during previous transaction is hashed with Hash of last valid transaction and new hash is treated as direct knowledge K$_d$ for RE.



(a) IP Address
(b) Mac Address
(c) Time of day
(d) Operating System
(e) Location

FIGURE 3. Membership functions of each device parameter is along y-axis and threshold value of each linguistic variable is along the x-axis.

D. TRUST EVALUATION FIS

The purpose of this function is to provide trust feedback based on previous transactions as input to the fuzzy logic of authorization transaction. The trust feedback along with authentication provides sufficient proof for fuzzy logic to apply rules to assign the type of access privileges the RE can have. The RE request is mapped to particular access right permission set accordingly with the trust feedback score. Trust of a device constitutes of three main elements [39]:

1) **Experience:** The transactions experience which is dependent on the previous transactions between RE and SP. The experience ${}_{RE}E_{SP}$ is calculated by eq (1)

$$ {}_{RE}E_{SP} = \begin{cases} 0 & \text{if } n = 0 \\ \dfrac{\sum_{t=1}^{n} E_t}{\sum_{t=1}^{n} |E_t|} & \text{if } n \neq 0 \end{cases} \tag{1} $$

Here, range of ${}_{RE}E_{SP}$ ∈[-1,1]. E_t is +1 for successful transaction and -1 for unsuccessful transaction. The membership functions and fuzzy sets of ${}_{RE}E_{SP}$ are shown in figure 6.

2) **Knowledge:** K$_d$ is calculated in each transaction and if K$_d$ provided by RE is different from the one generated by SP then -1 or else 1 is given as value of K$_d$ and aggregate value of ${}_{RE}K_{SP}$ is given by eq (2)

$$ {}_{RE}K_{SP} = \begin{cases} 0 & \text{if } n = 0 \\ \dfrac{\sum_{t=1}^{n} K_t}{\sum_{t=1}^{n} |K_t|} & \text{if } n \neq 0 \end{cases} \tag{2} $$

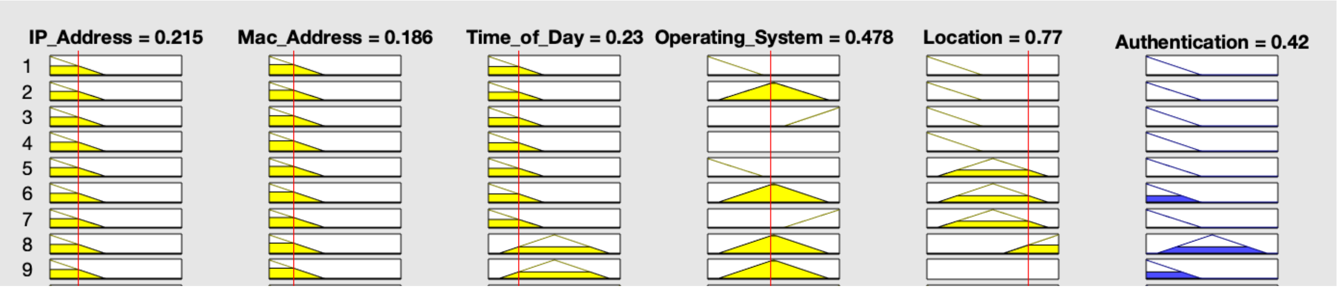


FIGURE 4. FIS rules viewer.

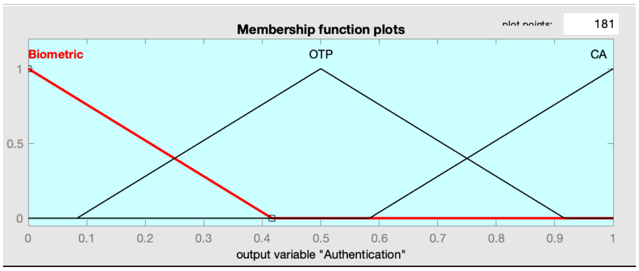


FIGURE 5. Membership function of authentication output.

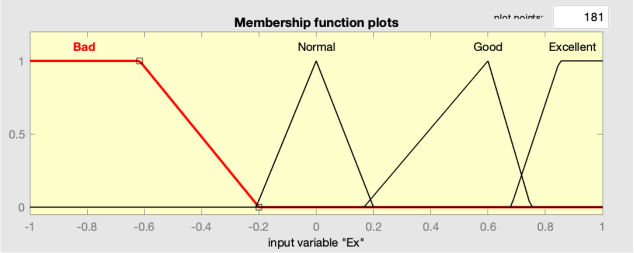


FIGURE 6. Membership functions of ${}_{RE}E_{SP}$.

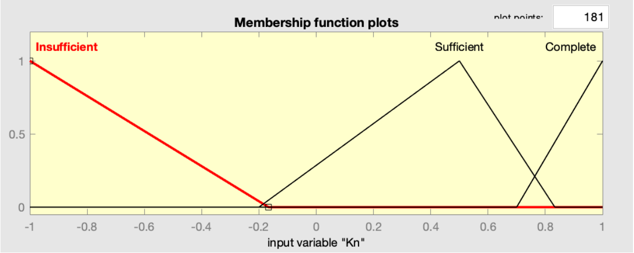


FIGURE 7. Membership functions of ${}_{RE}K_{SP}$.

In eq 2 ${}_{RE}K_{SP}$ ∈[-1,1] and denotes the knowledge of RE with respect to SP. The membership functions and fuzzy sets for ${}_{RE}K_{SP}$ are shown in figure 7.

3) **Reputation:** The last is the Reputation calculated by blockchain based on the experiences of all devices with pretext to RE. In this case the context is RE, thus reputation is given by eq (3)

$$R_{RE} = \frac{\sum_{t=1}^{n} \{E_{sp}\}_t}{\sum_{t=1}^{n} |E_{sp}|_t} \tag{3}$$

In eq 3 R_{RE} ∈[-1,1] and denotes the experience of BAN SP devices with RE. The membership function and fuzzy sets associated with reputation are shown in figure 8. The fuzzy output in terms of trust is calculated based on 27 rules and shown in figure 9.

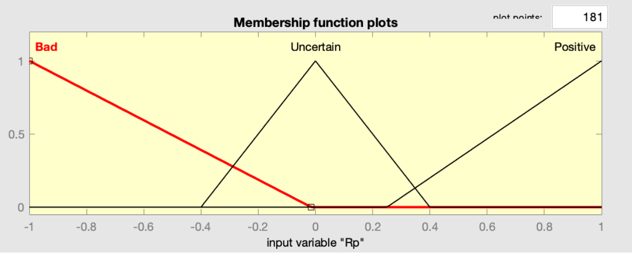


FIGURE 8. Membership functions of R_{RE}.

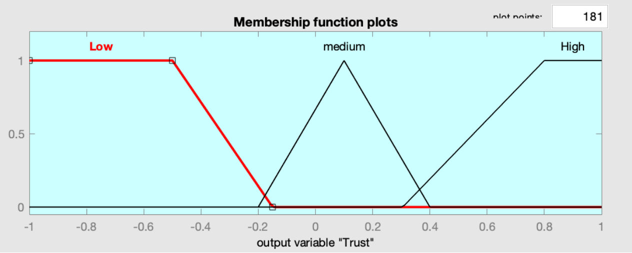


FIGURE 9. Membership functions of Output 'Trust'.

E. ACCESS CONTROL FIS

The last function is Access control function. In this function the Trust and Authentication linguistic values of previous functions is taken as input and Access Control is given as an output as shown in figure 10. The Access Rights are linguistically defined as {ϕ, Read, Read/Write, Read/Write/execute} and their membership functions are shown in figure 11. The authentication input provides a fresh behavior input of RE whereas the Trust function provides a feedback-based input and this way the access control is adjusted according to device behavior. For example, if trust is low and the device had authenticated through biometrics the output is No Access as shown in figure 12. The device access is revoked and it is

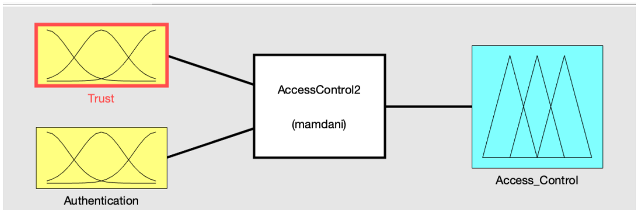


FIGURE 10. Access control FIS.

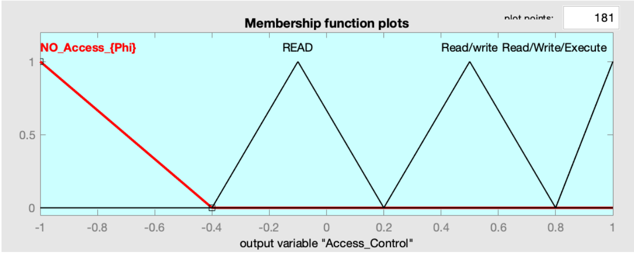


FIGURE 11. Membership functions of output ‘access right’.

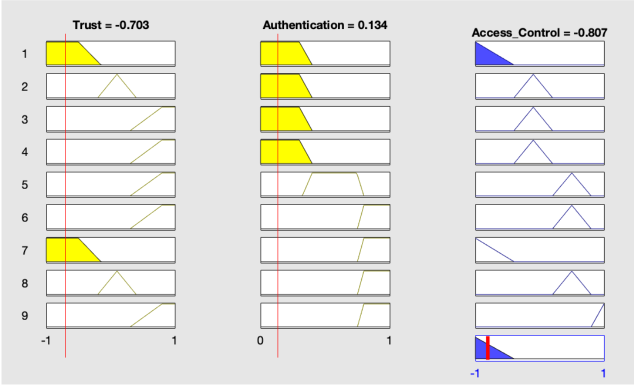


FIGURE 12. Rule viewer - access rights.

asked to re-validate its certificate through admin and admin is notified. If trust is high and authentication is OTP based than access assigned is different. If a device is assigned NO Access, the RE is deemed as malicious, its access is revoked and it has to re-validate its certificate through CA and the transaction parameter of $_{RE}E_{SP}$ is given -1 value accordingly for this transaction. Otherwise the access is granted on basis of least privilege. For example, if output access right is Read/Write whereas the permissions defined for device only contain read access the device will be granted only read access.

IV. FBASHI-ADAPTIVE SECURITY FRAMEWORK

Hospital is the core organization for testing and implementation of our framework. Hyperledger channels are deployed at departmental level and are part of the main chain run at Hospital level. Similarly, hospital can be part of a consortium thus forming part of a bigger blockchain. This way the network is layered in nature and scalable as well. This point onwards, framework will be discussed at departmental level and is equally applicable to every department and scenario in same way. As this architecture has been designed specific to IoT devices, these devices are mostly deployed for a specific service at a departmental level and it is highly unlikely that someone from some other department will seek access request to device data directly. Likewise, it is highly unlikely that a device is moved temporarily from one department to other and if such is the case the device will be re-registered in the new department. Figure 13 shows the basic layout of medical department. IoTs associated with a patient are connected to gateway which is part of Blockchain and acts as Anchor peer for IoT devices. Caregivers form integral part of blockchain network and are randomly assigned roles of blockchain peers according to their privileges defined in certificate.

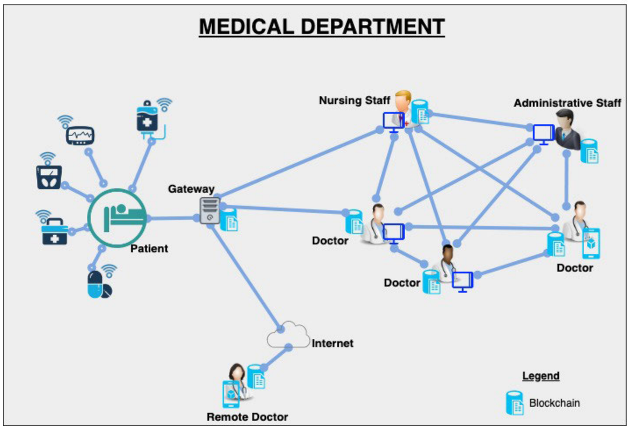


FIGURE 13. Bird eye view of Medical department.

A. TRANSACTION FLOW IN BLOCKCHAIN

To understand the transaction flow in semantic way a toy scenario is considered where a doctor wants to get ECG readings of a patient from an ECG machine which we call SP_{ECG} and the doctor is RE_D (Requesting Entity) in this case. The doctor can be serving in multiple departments in a hospital, for example a heart specialist will have emergency duty in Medical Emergency department, thus in order to carry out the transaction in focus which is in medical department he has to interact with blockchain using the id associated with this department. In healthcare environment patient’s privacy is primary and is catered for by adding patient as context in every transaction. The transaction flow in Hyperledger is shown in figure 14 and each phase of the transaction is discussed below:

1) The RE_D initiates a request access transaction by sending transaction parameters using blockchain protocol of Hyperledger. The clients are connected through anchor peers as already discussed. In this case the RE_D itself is an anchor peer and can initiate transaction. The transaction packet contains following parameters $T_A = \{ID_{RE} \,||\, ID_P||ID_{SP}||\text{Access Type}||\text{Nonce}_{SP}\}$.

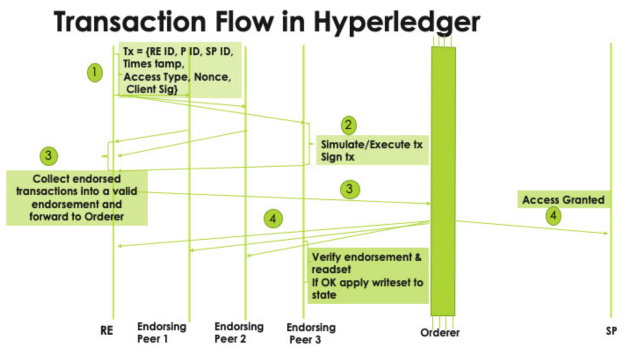

Transaction Flow in Hyperledger
1
Tx = {RE ID, P ID, SP ID, Times tamp, Access Type, Nonce, Client Sig}
2
Simulate/Execute tx Sign tx
3
Collect endorsed transactions into a valid endorsement and forward to Orderer
3
4
Verify endorsement & readset If OK apply writeset to state
Access Granted
4
RE
Endorsing Peer 1
Endorsing Peer 2
Endorsing Peer 3
Orderer
SP

FIGURE 14. Hyperledger transaction flow.

2) The transaction parameters are verified by the Endorsing peers, in each case depending on the group of devices interacting. A set of Endorsing peers are nominated and these can be assigned weights or can use any pluggable consensus algorithm supported by Hyperledger fabric. The Endorsing peers simulate the read, write set of transaction meaning, they simulate the chaincodes and verify the inputs and outputs.
3) After the successful run of chaincode endorsing peers send back endorsed transaction (including their signatures) to Anchor peer.
4) The Anchor peer forwards the endorsed transaction to Orderer who verifies the Endorsed transaction. All the validations of transactions involve a local MSP running within each peer as separate module and it is responsible for verifying all the signatures of every transaction.
5) The Orderer after verifications assigns a block number to the transaction TR and initiates gossip protocol. Once gossip protocol is initiated all the Peers of concerned channel update their ledgers.
6) An Event is generated on completion of this transaction and the RE_D is granted access according to the current access right set of doctor. After successful transaction SP generates a simple transaction to send a Nonce to RE which is also recorded on ledger.

B. TRANSACTION LOGIC

The main driving force of our adaptive security mechanism is the chaincode part of transaction. Here we try to utilize the computational power and rich features of chaincode for maximum benefit of driving security in a distributed fashion. In order to work efficiently the framework requires at least 50 transactions data stored on blockchain. Thus, biometric based verification will be done in initial transactions and predefined access rights will be used. After 50th transaction the framework will be initialized. The transaction logic is based on three functions for understanding purpose however constitute part of same chain code. Figure 15 gives the overview of chaincode logic described later in the algorithms 1,2 and 3. Algorithm 1 describes the process of authentication Fuzzy Inference System (FIS). Algorithm 2 is regarding the trust FIS and algorithm 3 sets out the access control FIS implemented on Hyperledger Fabric.

Algorithm 1 Authentication

```
inferences = { {1, 1, 1, 1}, {1, 1, 1, 2}, {1, 1, 1, 3}, {1, 1, 2, 1}, {1, 1, 2, 2}, {1, 1, 2, 3}, };
function Authentication(crisp_input)
    calculate AuthenticationAccess(crisp_input);
EndFunction
Function calculateAuthenticationAccess(crisp_input)
    output = fuzzyLogicResult(crisp_input, EntityIP, EntityMac, EntityOperatingSystem, EntityLocation,EntityOutputRequest, inferences);
    RETURN output;
EndFunction
```

Algorithm 2 Trust

```
inferences = { {1, 1, 1}, {1, 1, 2}, {1, 1, 3}, {1, 2, 1}, {1, 2, 2}, {1, 2, 3} };
FunctionTrust(crisp_input)
    calculateTrustAccess(crisp_input);
EndFunction
FunctioncalculateTrustAccess(crisp_input)
    output = fuzzyLogicResult(crisp_input, EntityEx, EntityKn, EntityRp,EntityOutputRequest, inferences);
    RETURN output;
EndFunction
```

V. SECURITY ANALYSIS

The framework was designed in MATLAB and tested for different use cases. The parameters were chosen at random to validate concept and analyze outputs of each function. The surface view in figure 16 shows the input/output domain of Ip Address and Mac Address. The frequency distribution of both inputs is directly proportional to Authentication mechanism in use.

The MATLAB tested logic was then applied to Hyperledger fabric for function validity. The architecture is validated and as the number of transactions increases the Fuzzy Output gives more precise results. The system was found scalable as every device communicates on channel basis and transaction throughput is 10000 transactions per sec for Hyperledger Fabric. The threat model is presented:

1) **Attackers** Attackers whether insider or outsider mostly interact with system as a user. In healthcare monitoring systems the attacker can be an insider compromising EHR and selling them on black market or it can be an outsider with ill intentions to malign hospital reputation by disturbing the working mechanisms of medicals devices. As recently, a vulnerability was found in authentication of Anesthesia devices of GE Aestiva and Aespire [4]. This vulnerability allows a remote attacker to modify device parameters like changing gas density,

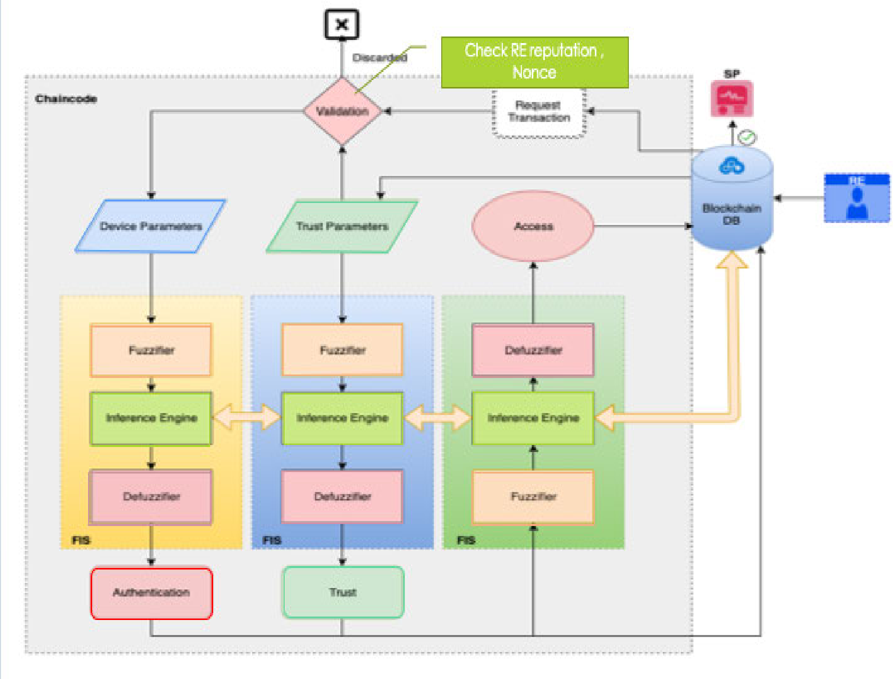


FIGURE 15. Chaincode logic.

Algorithm 3 Access Logic

```
Function takeMaxOfArray(arr)
    max ← a[0];
    For $j \leftarrow 1$ to $arr.length$
        If $arr[j] > max$
            $max \leftarrow arr[j]$;
        Else
            $max \leftarrow max$;
        EndIf
    EndFor
EndFunction
FunctioncalculateTrustAccess(crisp_input)
    output ← fuzzyLogicResult(crisp_inputEntityEx, EntityKn, EntityRp,EntityOutputRequest, inferences);
    RETURN output;
EndFunction
FunctiontakeMaxOfArraySetset
    For $i \leftarrow set.length - 1$ to 0
        $output[i] \leftarrow takeMaxOfArray(set[i])$;
    EndFor
EndFunction
```

silencing alarms and warnings and even changing the time settings of machine. Thus, in our threat model both insider and outsider attackers are considered.

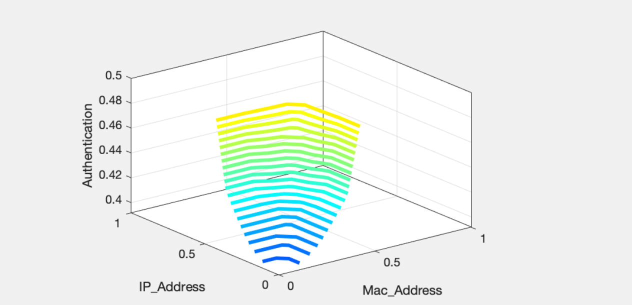


FIGURE 16. Surface view- authentication with two input variables.

2) **Assets** Hospitals provide healthcare services which are life critical and thus any system or device dealing with any sort of healthcare data is treated as an asset. The data is collected from sensors, synthesized by special servers into intelligent information which can be translated to the patient's health records for analysis and treatment by Caregivers. This data is then stored may be on hospital database or integrated with cloud services for interoperability between various medical organizations, government and services like insurance. The following assets evolve through the proposed hospital monitoring system:

   a) Medical IoTs
   b) Caregivers
   c) Patients Health records
   d) Gateways, database servers involved in computations

3) **Threats** Healthcare faces more imminent threats because of high value of patient information in black market and large volume of sensitive data easily available as least importance is given to cyber security in healthcare. Protection against cyber threats in compliance with HIPAA can be challenging and any oversights could easily cost a breach or regulatory fine. Following are the threats identified in healthcare environment which are required to be mitigated by our suggested solution:
   1) Unauthorized access to medical sensors and devices.
   2) Tempering of recorded patient data.
   3) Corruption of data by collusions of peers.
   4) Leakage of information between various tiers (hospital, cloud services and other organizations).
   5) Accidental or deliberate loss of data by caregivers.
   6) Unauthorized access to medical data by users in contrast to assigned roles and responsibilities.
   7) Manipulation of activities and audit logs.
4) **Mitigation Strategies** Table 1 enumerates the mitigation strategies against most common threats achieved through our framework to achieve security objectives for IoTs in healthcare.

VI. COMPARATIVE ANALYSIS

The main objective of our framework is to achieve adaptive security based on user behavior without depending on traditional security mechanisms like passwords and tokens. Moreover, centralized architecture presents single point of failure and thus vulnerable to many attacks like DOS attacks, ransomware attacks etc. Most of the research work in this domain relies on central architecture and very few have utilized the true potential of blockchain technology. Furthermore, most of the work relies on a single authentication mechanism which may be subverted by the adversaries thus our system adapts by applying second factor authentication based on users' attributes and behavior. Table 2 shows comparative analysis of our framework with existing solutions.

A. USABILITY AND COMPARISONS WITH OTHER BLOCKCHAINS

The permissionless or public blockchains face various challenges regarding performance parameters. The public blockchains like Bitcoin and Ethereum are mostly based on PoW consensus which is resource intensive involving high latency in order to achieve security. Some of the public blockchains like Litecoin have reduced block formation time of 2.5 minutes as compared to 10 minutes of Bitcoin. Consequently, Litecoin uses a smaller number of hashes to verify the block as compared to Bitcoin. This problem is absent in Hyperledger because the consensus is achieved through PBFT (Practical Byzantine Fault Tolerance) depending on predefined endorsers and trust is anchored by the governing body. Thus, virtually there is no deliberate latency for achieving security and the block is formed as soon being verified by the endorsers. The security and performance can be achieved in a similar manner as in traditional networks by limiting the channel users to the concerned parties as the concept of VLANs in traditional networks. This enables privacy and scalability at the same time by segregating different parts of networks from each other. Therefore, FBASHI was implemented on Hyperledger blockchain to ascertain the practical feasibility in comparison to existing state of the art and other blockchain based solutions. The performance is evaluated and compared to other blockchains below:

1) LATENCY

Transaction latency is the time transaction takes starting from the point it is submitted to the network to the point it is committed by all peers to the ledger. Hence the performance and throughput somehow rely on this parameter. Latency is the pivot point for the performance of Hyperledger Fabric. As the blocksize increases the latency reduces because Orderer has fewer transactions in backlog when the transaction rate is high. But as shown in figure 17 the smaller blocksize is suitable for lower transaction rates but as in our case the higher blocksize is much suitable to achieve high tps. Thus, blocksize is a major tweaking parameter while configuring Hyperledger Fabric as per the application's demand.

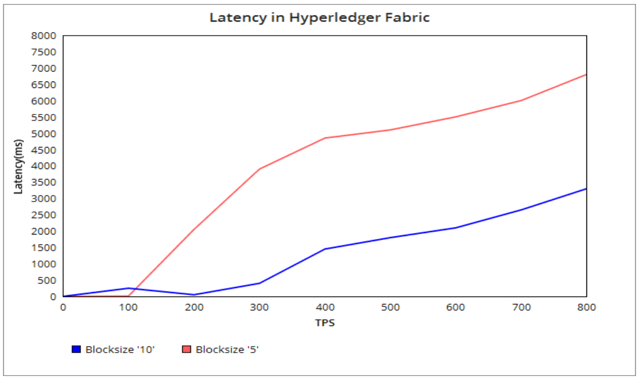


FIGURE 17. Transaction latency with varying blocksize of hyperledger fabric.

2) THROUGHPUT

Transaction throughput is the amount of time a valid transaction takes to get committed to the blockchain. Many researchers and blockchain benchmarking sites use throughput as the main performance parameter for Blockchain which is not true. The throughput of public blockchains are inadequate and one of root cause behind lack of its adaption in modern banking systems where required throughput is somewhat around 2000 tps. Whereas in AAA services required throughput is greater. FBASHI performs better being based on Hyperledger Fabric having better consensus algorithms and segregation of power between different nodes based upon organizational parameters. Consensus in Hyperledger Fabric is directly linked to endorsers, thus impacting the throughput. As we increase the number of endorsing peers it takes more time for a transaction to get committed to the blockchain

TABLE 1. Mitigation strategies.

Threat	Strategy	Description
Spoofing	X.509 Certificates (Provided by Hyperledger Fabric)	All entities can interact with blockchain only through certificates issued by CA and reliance on local CA hierarchy eliminates third party breaches
Tampering	Blockchain's cryptographic means SHA256, ECDSA)	Blockchain provides immutability through use of hashing and signatures
Repudiation	Digital Signatures	All transactions include signatures thus no entity can deny its actions
Replay Attacks	Read/ write sets, version number	Endorsers use read write sets to validate transactions, invalid key value pairs and version numbers simply deem a transaction invalid
Remote Access	MFA	The Adaptive MFA ensures the device behavior is consistent with usage and only granted access after behavior analysis
Privilege Escalation	Identity Management and Access Control	The X.509 based issued identities define roles and Adaptive access control mechanism works on least privilege mechanism.
Ransomware/ Malware	Adaptive Security	Behavioral analysis helps in better authentication and access control mechanism to deny access to malicious entities.

TABLE 2. Comparison of proposed framework with existing solutions.

Paper	Decentralized	Authentication	Access Control	Trust Management	MFA	Adaptivity
[13][14][19][20][21]	55	51	55	55	55	55
[15][17][18]	55	51	51	55	55	55
[25][28][30]	51	55	51	51	55	55
[26][27][29][31]	51	55	51	55	55	55
[32]	51	51	55	55	55	55
[34]	51	55	55	55	55	55
FBASHI	51	51	51	51	51	51

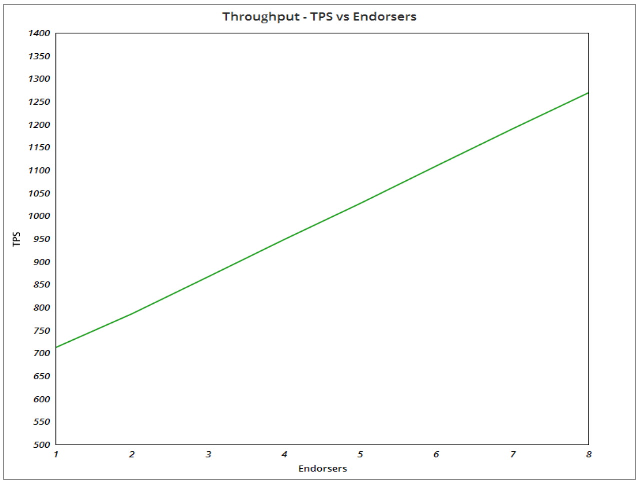


FIGURE 18. Impact of endorsers on transaction rate of hyperledger fabric.

after due endorsement of each endorser. The performance can further degrade if we use endorsers from multiple medical departments. This is the reason behind configuring a separate channel on departmental basis and load balancing endorsement to achieve max performance for proposed architecture. Figure 18 clearly shows as we increase the number of endorsers the throughput in terms of tps will increase but this is only valid when their is load blanacing between endorsers and they are not from multiple organizations. We achieve this linearity by limiting the endorsers to departmental level thus reducing the lag. This can get worse if all endorsers are included for same task resulting in saturation, consuming all the available CPU resources allocated to the container. Thus, these parameters must be tweaked accordingly as per requirements of the application.

VII. CONCLUSION AND FUTURE WORK

Over a period of time the device behavior must remain consistent and a user using a system in a hospital is most likely to use same machine with same IP, location and device. Thus, this behavior must fall within a specific range. This research normalizes device behavior through FIS using Hyperledger Fabric to achieve distributed trust, fuzziness and removing single point of failure from AAA services. Patient endorsement through OTP improves security and privacy sufficing HIPAA and GDPR compliance as patient must be in full control of his data. Our framework successfully detects malicious behavior and thwarts various types of threats against IoT in healthcare. In future, we intend to explore AI capability of blockchain by including more parameters and expanding this framework to other parts of network for foolproof security.

DECLARATIONS

CONFLICT OF INTERESTS

There are no conflicts of interest for all authors.

REFERENCES

[1] F. Paul. (Mar. 28, 2018). *Network World*. Accessed: Dec. 25, 2021. [Online]. Available: https://www.networkworld.com/article/3267065/people-are-really-worried-about-iot-data-privacy-and-securityand-they-should-be.html#nww-fsb

[2] F. Paul. (Jan. 14, 2019). *Network World*. Accessed: Dec. 29, 2021. [Online]. Available: https://www.networkworld.com/article/3332032/top-10-iot-vulnerabilities.html

[3] F. Dai, Y. Shi, N. Meng, L. Wei, and Z. Ye, "From bitcoin to cybersecurity: A comparative study of blockchain application and security issues," in *Proc. 4th Int. Conf. Syst. Informat. (ICSAI)*, Nov. 2017, pp. 975–979.

[4] Journal, HIPAA. (Jul. 10, 2019). *HIPAA JOURNAL*. Accessed: Aug. 1, 2021. [Online]. Available: https://www.hipaajournal.com/vulnerability-identified-in-ge-aestiva-and-aespire-anesthesia-machines/

[5] HIPAA. (2018). *HIPAA Guide*. Accessed: Aug. 1, 2021. [Online]. Available: https://www.hipaaguide.net/hipaa-for-dummies/

[6] HIPAA. (2018). *HIPAA Guide*. Accessed: Aug. 1, 2021. [Online]. Available: https://www.hipaaguide.net/gdpr-for-dummies/

[7] J.-L. Hou and K.-H. Yeh, "Novel authentication schemes for IoT based Healthcare systems," *Int. J. Distrib. Sensor Netw.*, vol. 2015, pp. 1–9, Nov. 2015.

[8] G. Manogaran, R. Varatharajan, D. Lopez, P. M. Kumar, R. Sundarasekar, and C. Thota, "A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system," *Future Gener. Comput. Syst.*, vol. 82, pp. 375–387, May 2018.

[9] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and A. C. Shehzad, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Comput. Elect. Eng.*, vol. 63, pp. 182–195, Oct. 2017.

[10] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Gener. Comput. Syst.*, vol. 80, pp. 483–495, Mar. 2018.

[11] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for Internet of Things: A comprehensive survey," *Secur. Commun. Netw.*, vol. 2017, pp. 1–41, Nov. 2017.

[12] D. Rivera, L. Cruz-Piris, G. Lopez-Civera, E. de la Hoz, and I. Marsa-Maestre, "Applying an unified access control for IoT-based intelligent agent systems," in *Proc. IEEE 8th Int. Conf. Service-Oriented Comput. Appl. (SOCA)*, Oct. 2015.

[13] H. Ning, H. Liu, and L. T. Yang, "Aggregated-proof based hierarchical authentication scheme for the Internet of Things," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 3, pp. 657–667, Mar. 2015.

[14] A. Singh and K. Chatterjee, "A secure multi-tier authentication scheme in cloud computing environment," in *Proc. Int. Conf. Circuits, Power Comput. Technol. (ICCPCT)*, Mar. 2015, pp. 1–7.

[15] C. Hu, J. Zhang, and Q. Wen, "An identity-based personal location system with protected privacy in IoT," in *Proc. 4th IEEE Int. Conf. Broadband Netw. Multimedia Technol.*, Oct. 2011, pp. 192–195.

[16] J. H. Yang and P. Y. Lin, "An ID-based user authentication scheme for cloud computing," in *Proc. 10th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Aug. 2014, pp. 98–101.

[17] C. Lai, H. Li, X. Liang, R. Lu, K. Zhang, and X. Shen, "CPAL: A conditional privacy-preserving authentication with access linkability for roaming service," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 46–57, Feb. 2014.

[18] M. Ali, M. ElTabakh, and C. Nita-Rotaru, "FT-RC4: A robust security mechanism for data stream systems," Purdue Univ., West Lafayette, IN, USA, Tech. Rep. 05-024, 2005.

[19] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2710–2723, Nov. 2013.

[20] S. R. Moosavi, T. N. Gia, E. Nigussie, A. M. Rahmani, S. Virtanen, H. Tenhunen, and J. Isoaho, "End-to-end security scheme for mobility enabled healthcare Internet of Things," *Future Gener. Comput. Syst.*, vol. 64, pp. 108–124, Nov. 2016.

[21] S. R. Moosavi, E. Nigussie, S. Virtanen, and J. Isoaho, "Cryptographic key generation using ECG signal," in *Proc. 14th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2017, pp. 1024–1031.

[22] P. M. Kumar and U. D. Gandhi, "Enhanced DTLS with CoAP-based authentication scheme for the Internet of Things in healthcare application," *J. Supercomput.*, vol. 76, no. 6, pp. 3963–3983, Jun. 2020.

[23] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[24] K. Zile and R. Strazdiia, "Blockchain use cases and their feasibility," *Appl. Comput. Syst.*, vol. 23, no. 1, pp. 12–20, May 2018.

[25] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, May 2015, pp. 180–184.

[26] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.

[27] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "FairAccess: A new blockchain-based access control framework for the Internet of Things," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5943–5964, 2017.

[28] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1594–1605, Apr. 2019.

[29] A. Ramachandran and D. M. Kantarcioglu, "Using blockchain and smart contracts for secure data provenance management," 2017, *arXiv:1709.10000*.

[30] C. Qu, M. Tao, J. Zhang, X. Hong, and R. Yuan, "Blockchain based credibility verification method for IoT entities," *Secur. Commun. Netw.*, vol. 2018, pp. 1–11, Jun. 2018.

[31] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.

[32] C. H. Lee and K.-H. Kim, "Implementation of IoT system using block chain with authentication and data protection," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2018, pp. 936–940.

[33] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for Internet of Things security: A position paper," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 149–160, Aug. 2018.

[34] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2017, pp. 464–467.

[35] V. Shermin and K. Valentin. (2017). *Blockchain A Beginners Guide*. [Online]. Available: https://blockchainhub.net/

[36] Z. Hintzman, "Comparing blockchain implementations," in *Proc. SCTE-ISBE and NCTA*, 2017, pp. 1–29.

[37] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, 2017, pp. 1–6.

[38] J. Lei, G. Cui, and G. Xing, "Trust calculation and delivery control in trust-based access control," *Wuhan Univ. J. Natural Sci.*, vol. 13, no. 6, pp. 765–768, Dec. 2008.

[39] P. N. Mahalle, P. A. Thakre, N. R. Prasad, and R. Prasad, "A fuzzy approach to trust based access control in Internet of Things," in *Proc. Wireless VITAE*, Jun. 2013, pp. 1–5.

[40] A. Walker. (Jan. 18, 2018). *Risk-Based Authentication: The Future of Workplace Security*. G2. Accessed: Dec. 31, 2021. [Online]. Available: https://learn.g2.com/trends/risk-based-authentication

[41] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham, and M. Omar, "The role of blockchain technology in telehealth and telemedicine," *Int. J. Med. Informat.*, vol. 148, Apr. 2021, Art. no. 104399.

[42] I. Abu-Elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-Alrazaq, "The benefits and threats of blockchain technology in healthcare: A scoping review," *Int. J. Med. Informat.*, vol. 142, Oct. 2020, Art. no. 104246.

ZEESHAN ZULKIFL received the B.E. degree in telecommunication engineering from NUST, Pakistan, in 2014, and the M.S. degree in information security from NUST. He is currently a part of teaching faculty with NUST. His research interests include blockchain, the IoT security, cyber forensics, and data security and privacy.

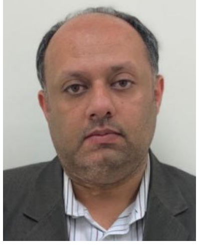
FAWAD KHAN (Senior Member, IEEE) received the B.S. degree in electrical engineering from UET Peshawar, in 2010, the M.S. degree in electrical engineering from CECOS University, in 2014, and the Ph.D. degree from the School of Cyber Engineering, Xidian University, in 2018. Currently, he is working with the National University of Science and Technology, Pakistan. His research interests include cryptography, information security, blockchain, and access control.

SHAHZAIB TAHIR (Senior Member, IEEE) received the B.E. degree in software engineering from Bahria University, Islamabad, Pakistan, in 2013, the M.S. degree in information security from NUST, Islamabad, in 2015, and the Ph.D. degree in information engineering from the City, University of London, U.K., in 2019. He was a Research Fellow with the City, University of London. He is currently an Assistant Professor with the Department of Information Security, NUST, and also the Chief Technical Officer of CityDefend Ltd., U.K. He is an alumni of InnovateUK and CyberASAP and also the Co-PI of the Information Security and Privacy Laboratory, NUST. His research interests include applied cryptography and cloud security. He has been a TPC member of many international IEEE conferences. He is a Reviewer of IEEE Transactions on Dependable and Secure Computing, *IEEE Communications Magazine*, *Computers and Security* (Elsevier), IEEE Journal of Biomedical and Health Informatics, IEEE Access, IEEE ICC, *FGCS* (Elsevier), *Cluster Computing* (Springer), *Sadhna* (Springer), and *Science China Information Sciences* (Springer).

MEHREEN AFZAL graduated in mathematics and the Ph.D. degree in information security from NUST, Pakistan, in 2010. She is currently an Associate Professor at Air University, Islamabad, Pakistan. Her contributions include research articles on cryptanalysis and design of cryptographic algorithms/protocols. Her research interests include information security and cryptology.

WASEEM IQBAL received the bachelor's degree in computer sciences from the Department of Computer Science, University of Peshawar, in 2008, and the master's degree in information security from MCS–NUST, in 2012, where he is currently pursuing the Ph.D. degree. He is currently an Assistant Professor with the Department of Information Security, NUST. He is also an Academician, a Researcher, a Security Professional, and an Industry Consultant. His professional services include, but not limited to, an industry consultation, a workshops organizer/resource person, a technical program committee member, a conference chief organizer, an invited speaker, and a reviewer for several international conferences. He has authored over 35 scientific research articles in prestigious international journals (ISI-Indexed) and conferences.

ABDUL REHMAN received the B.S. degree in software engineering from Foundation University Islamabad, Pakistan. He is currently pursuing the M.S. degree in information security with NUST, Islamabad. He is currently serving as a Research Associate with the National Cyber Security Auditing and Evaluation Laboratory (NCSAEL). His interests include cyber forensics, data security, and privacy.



SAQIB SAEED received the B.Sc. degree (Hons.) in computer science from International Islamic University, Islamabad, Pakistan, in 2001, the M.Sc. degree in software technology from the Stuttgart Technology University of Applied Sciences, Germany, in 2003, and the Ph.D. degree in information systems from the University of Siegen, Germany, in 2012. He is currently an Associate Professor with the Department of Computer Information Systems, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia. He is also a Certified Software Quality Engineer from the American Society of Quality. His research interests include human-centered computing, data visualization and analytics, software engineering, information systems management, and digital business transformation. He is a member of the advisory boards of several international journals. He is an Associate Editor of IEEE Access and *International Journal of Public Administration in the Digital Age*.

ABDULLAH M. ALMUHAIDEB received the B.S. degree (Hons.) in computer information system from King Faisal University, Saudi Arabia, in 2003, and the M.S. (Hons.) and Ph.D. degrees in network security from Monash University, Melbourne, Australia, in 2007 and 2013, respectively. He is currently an Associate Professor in information security, a Supervisor of the Saudi Aramco Cybersecurity Chair, and the Dean of the College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Saudi Arabia. He has published two patents and more than 40 scientific articles in journals and premier ACM/IEEE/Springer conferences. His research interests include mobile security, authentication and identification, and ubiquitous wireless access.