
FortiRx 2.0: Smart Privacy-Preserved Demand Forecasting of Prescription Drugs in Healthcare-CPS

Presenter: Sukrutha L. T. Vangipuram

Anand Kumar Bapatla¹, S. P. Mohanty², E. Kougianos³
University of North Texas, Denton, TX, USA.^{1,2,3}

Email: ab0841@unt.edu¹, saraju.mohanty@unt.edu², elias.kougianos@unt.edu³

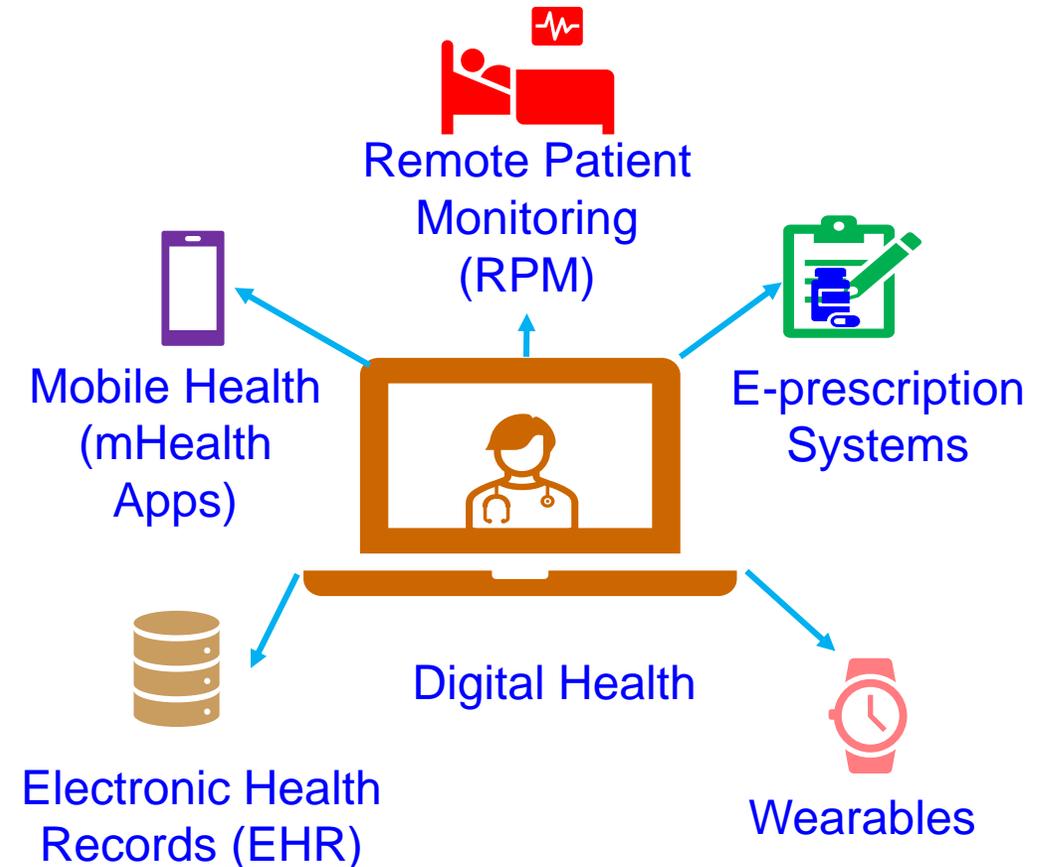
Outline

- Digital Health Technologies and E-Prescription
- Challenges
- Blockchain as a Solution
- Overview of FortiRx
- Novel Contributions
- Architectural Overview
- Implementation Details
- Results and Analysis
- Conclusion

Digital Health Technologies and E-Prescription

What are Digital Health Technologies?

- Digital Health Technologies encompasses a range of digital tools and platforms to improve healthcare services
- Facilitates remote consultation, personalized health tracking, and data-driven interventions
- E-prescription systems are crucial components of Digital Health Technologies and are often integrated into Electronic Health Records



Electronic Health Records (EHR's)

- Electronic Health Record (EHR) is an electronic version of patient medical history maintained by the provider
- Contains demographics, progress notes, problems, medications, and other administrative information

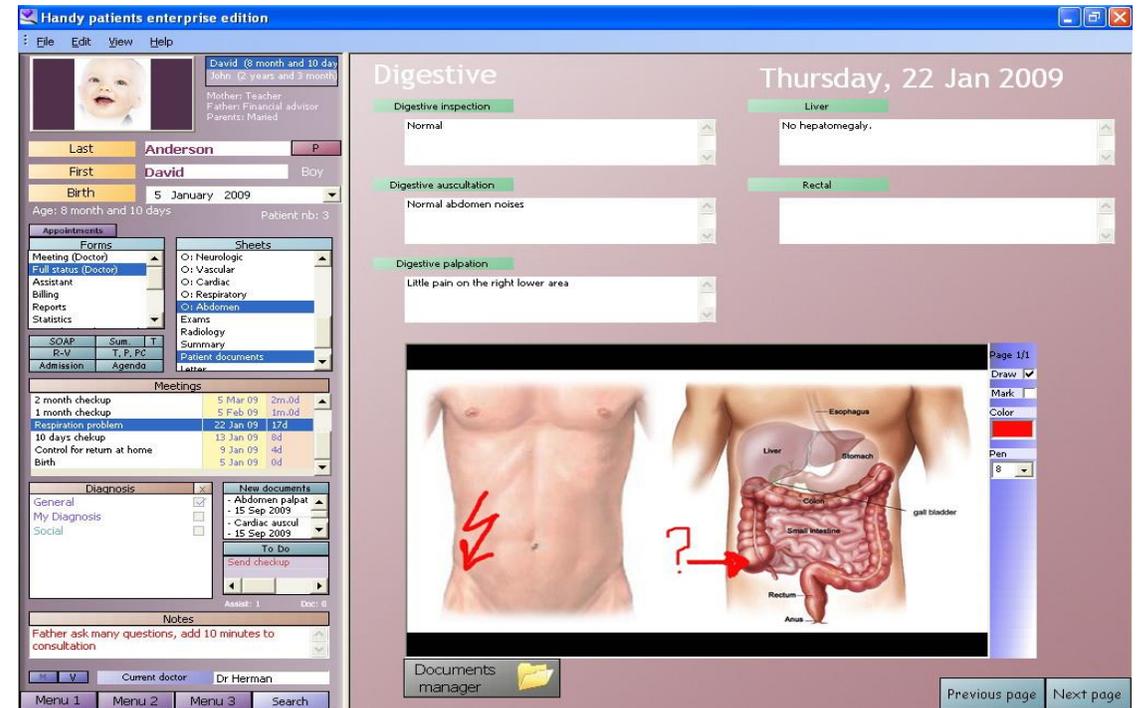
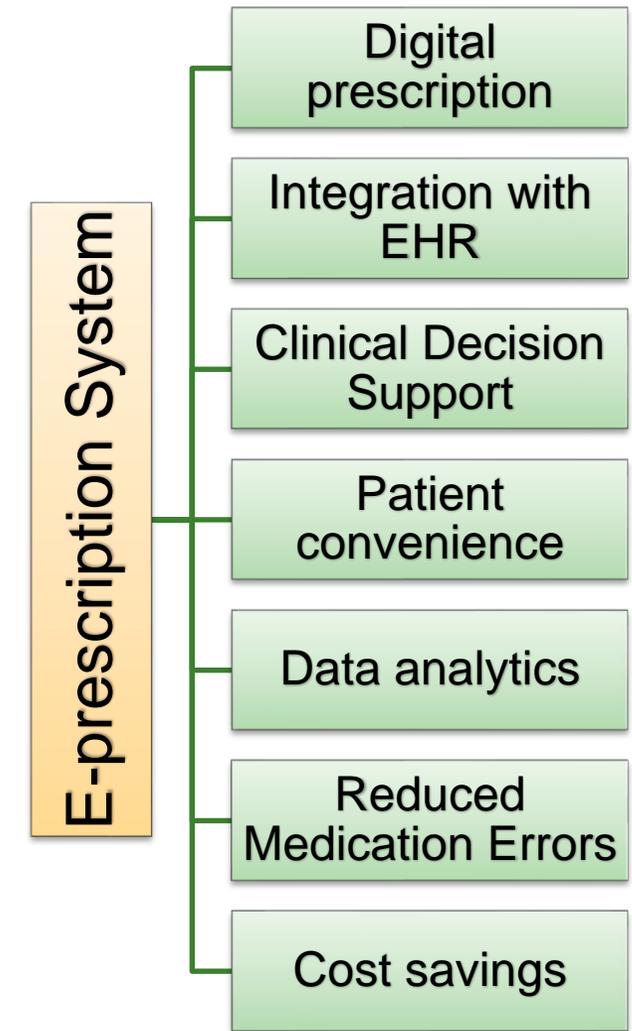


Image Source: DaCarpenter, An electronic medical record example, Handy patients electronic medical record (free open-source version)

Electronic Prescription

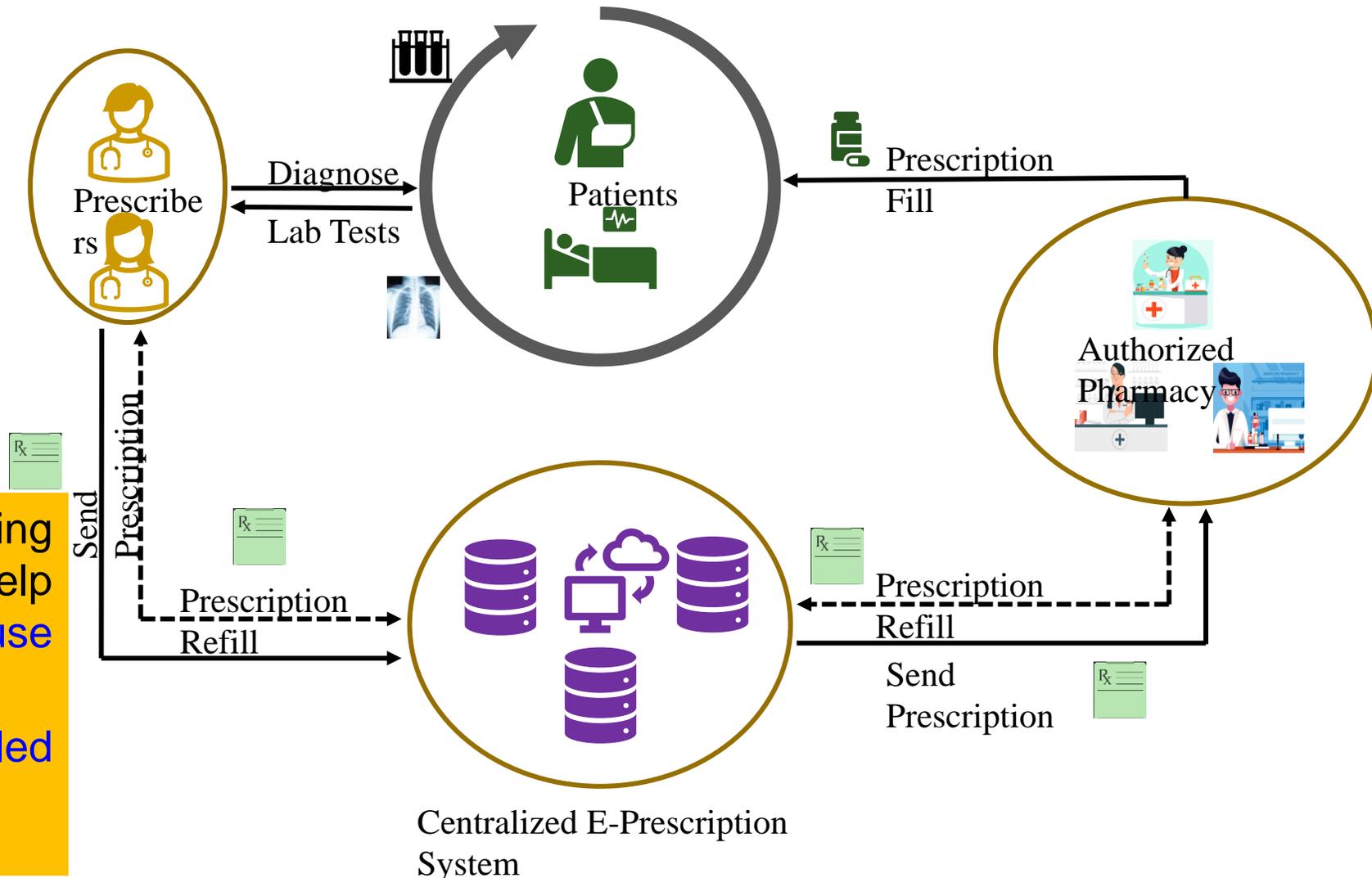
- Revolutionized the way medications are prescribed, processed, and dispensed
- Digital version of prescriptions increase legibility and reduces medication errors
- Clinical Decision Support Tools – Warn potential drug interactions, suggest alternate medication, offer dosage recommendations

- More than 100,000 reports of medication errors (FDA)
- 40% of Americans report being involved in medical errors (Institute for Healthcare Improvement/NORC at the University of Chicago)
- 1 in 5 doses of medication provided during patient visits is administered incorrectly



E-Prescription System and Issues

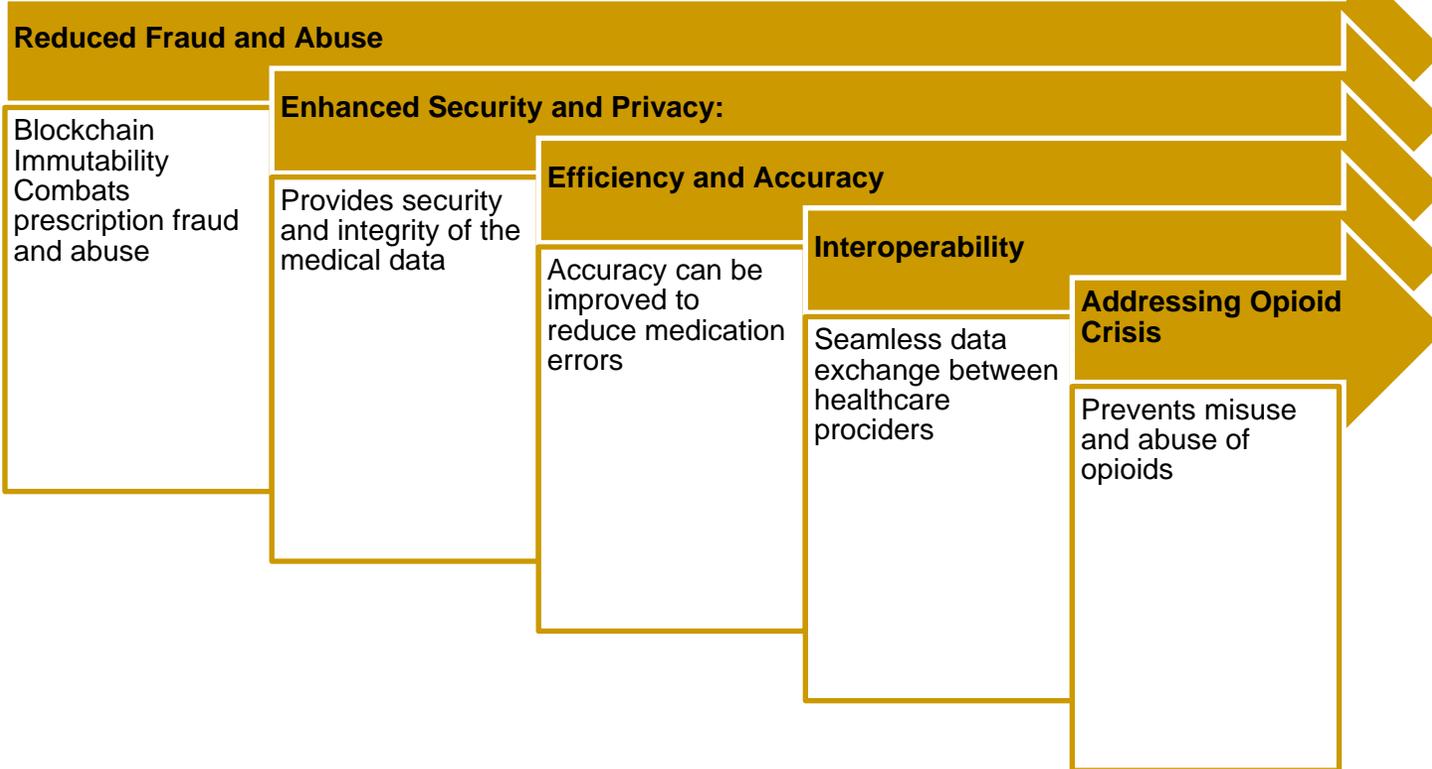
- Single Point of Failure (SPOF)
- Data Security
- Privacy Concerns
- Interoperability Concerns (PDMP)
- System availability Issues



- Prescription Drug Monitoring Programs (PDMP) help mitigate prescription misuse and diversion
- Oversight of controlled substance prescriptions

Motivation

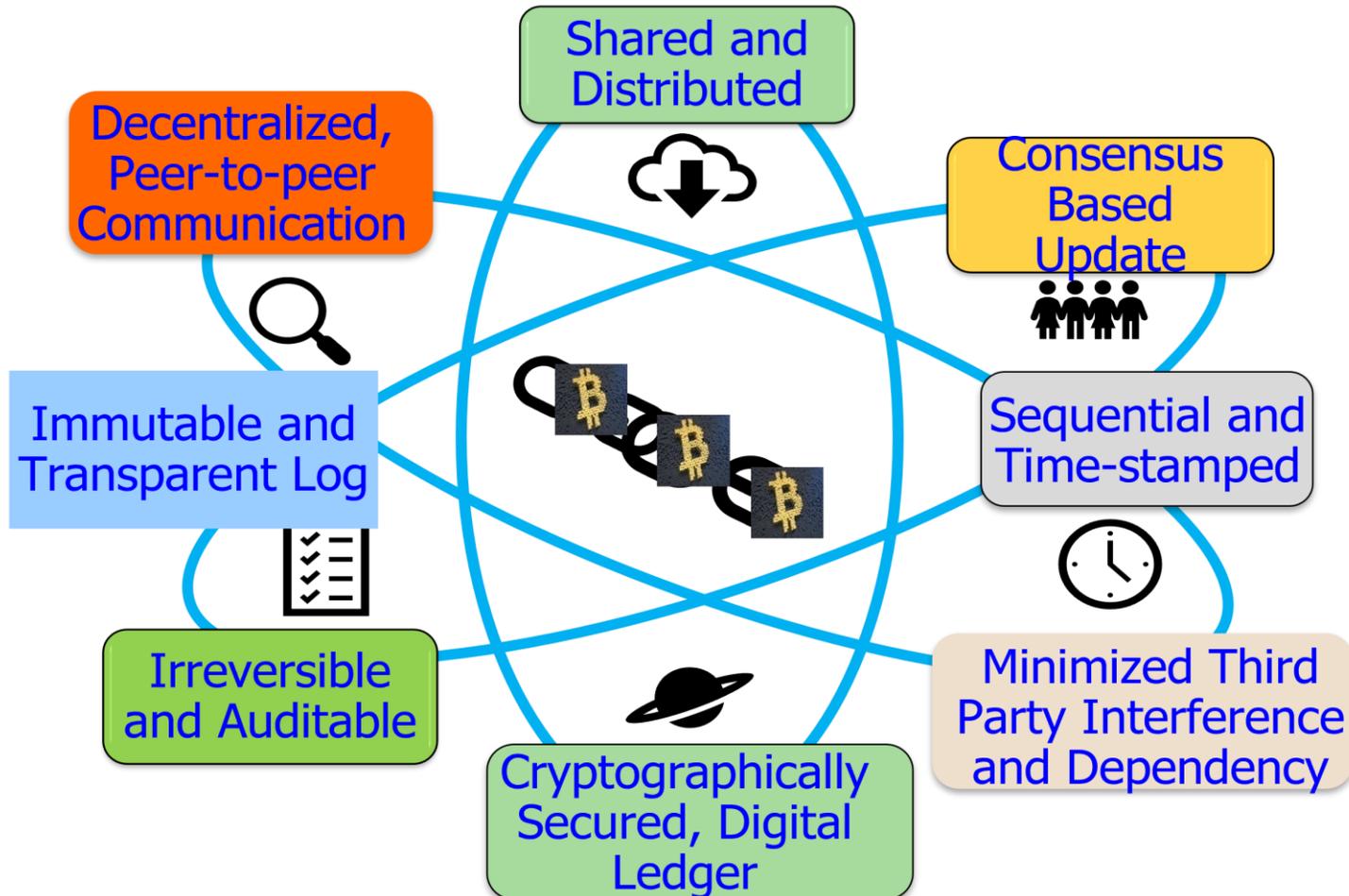
Prescription Drug Type	Annual Abusers	% Among Rx Abusers	% Among Americans
Painkillers	9.7 million	59.5%	3.43%
Opioids Alone	9.3 million	57.1%	3.29%
Sedatives	5.9 million	36.2%	2.08%
Stimulants	4.9 million	30.1%	1.73%
Benzodiazepine Alone	4.8 million	29.4%	1.70%
All Prescription Drugs	16.3 million	100%	5.76%



- 16M – 6% of Americans over the age of 12 abuse prescriptions in a year.
- 2M – 12% of prescription drug abusers are addicted.

Statistics Source: <https://drugabusestatistics.org/prescription-drug-abuse-statistics/>

Blockchain Technology



Technical Definition: A blockchain is a linked list that is built with hash pointers instead of regular pointers.

Socio-Political–Economic Definition: A blockchain is an open, borderless, decentralized, public, trustless, permissionless, immutable record of transactions.

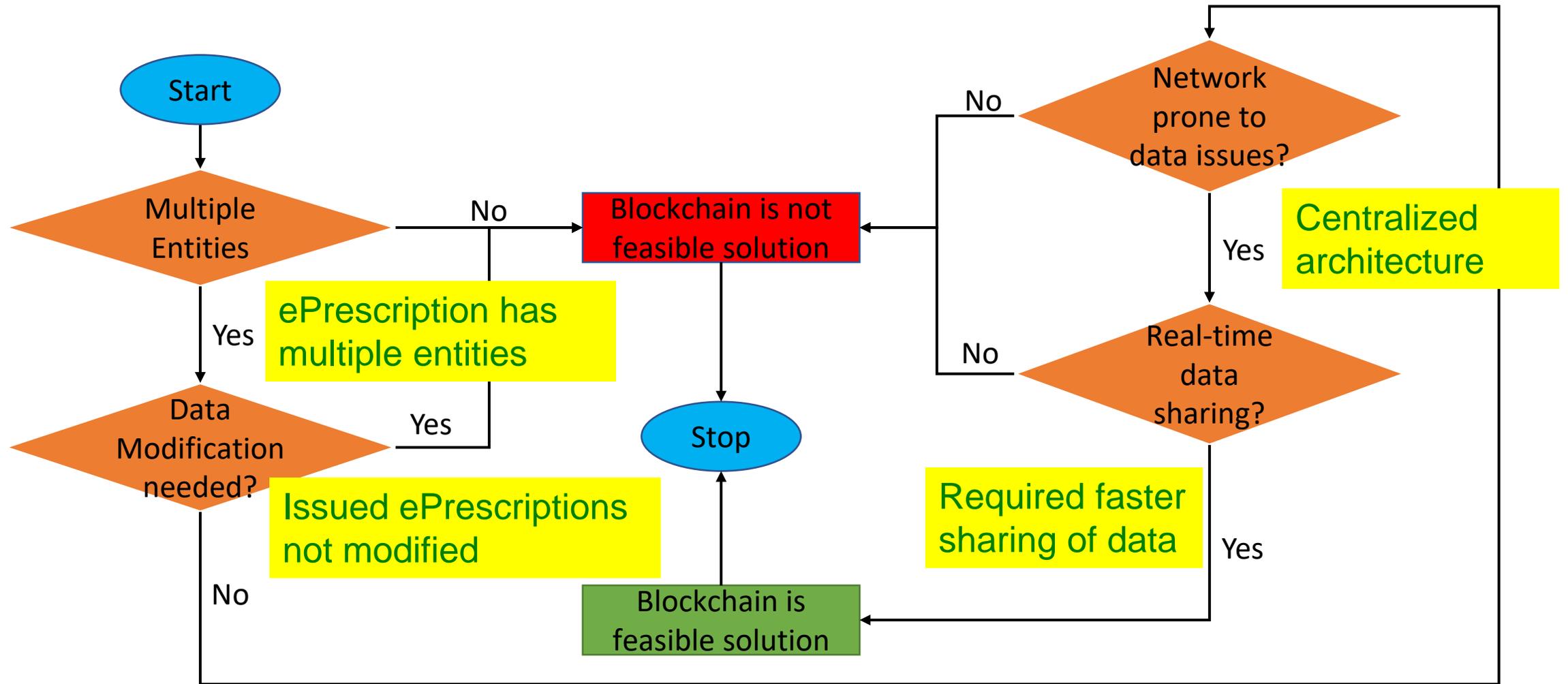
Financial – Accounting Definition: A blockchain is a public, distributed ledger of peer-to-peer transactions.

Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The Blockchain as a Decentralized Security Framework", *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 2, March 2018, pp. 18--21.

Blockchain as a Solution

- **Enhanced Data Security:** Decentralized and immutable ledger reduces the risk of data breaches and maintains data integrity.
- **Patient-Centric Privacy:** Empowers patients to have control over their health data.
- **Interoperability:** Improves interoperability between healthcare providers, pharmacies, PDMP databases, and other participants of the prescription process.
- **High Availability:** Blockchain-based e-prescription systems are more resilient to downtime, ensuring uninterrupted access.
- **Automated Processes:** Smart Contracts can automate various aspects of the e-prescription process.

Evaluating Blockchain for E-prescription

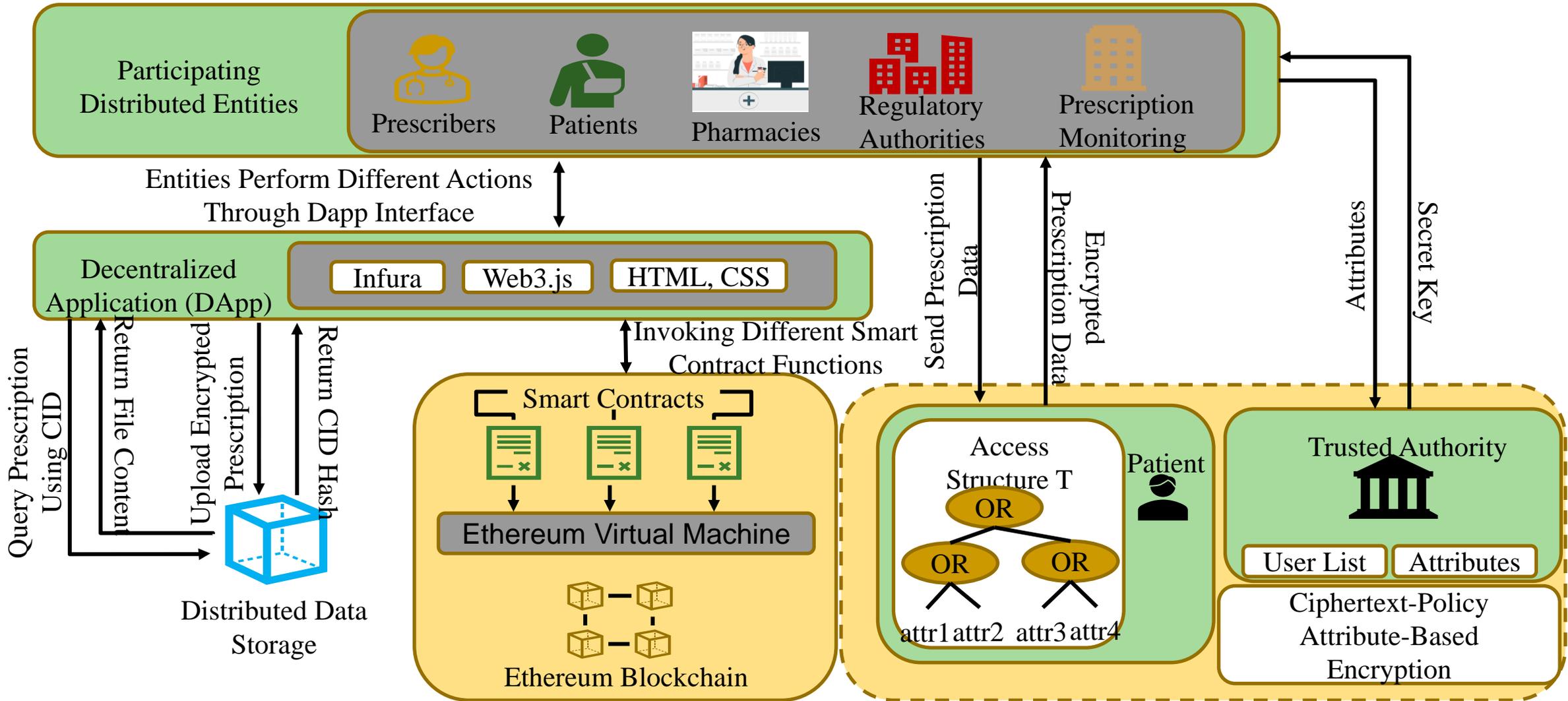


FortiRx: Distributed Ledger based Verifiable and Trustworthy Electronic Prescription Sharing

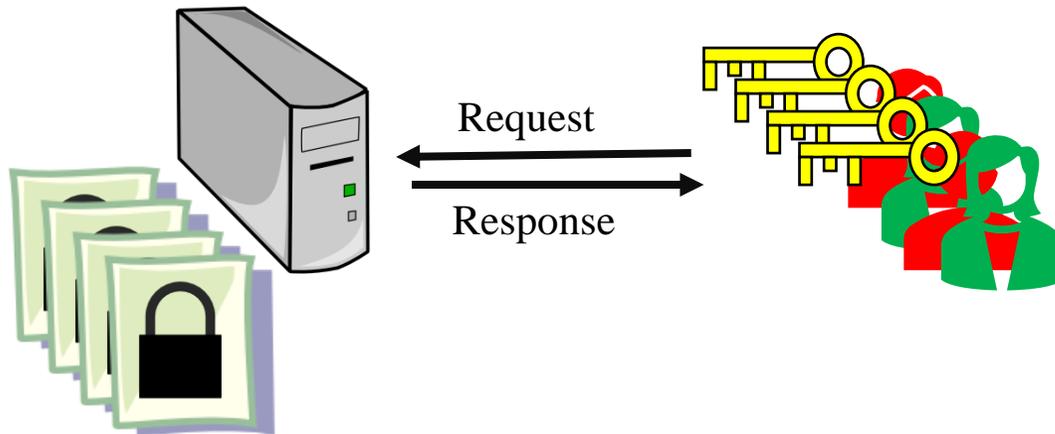
Novel Contributions

- Proposed FortiRx makes use of blockchain combined with the distributed file system (IPFS) to create a **decentralized environment** for all the participating entities.
- Blockchain enhances the **interoperability** of the system.
- Usage of **off-chain distributed file-sharing systems** to store prescription information can help in reducing the amount of on-chain data.
- It is **resistant to Single Point of Failure (SPOF)** and reduces response latency
- It avoids **data tampering** and prescription abuse
- **Cipher text-policy attribute-based encryption (CP-ABE)** provides a robust access control mechanism.

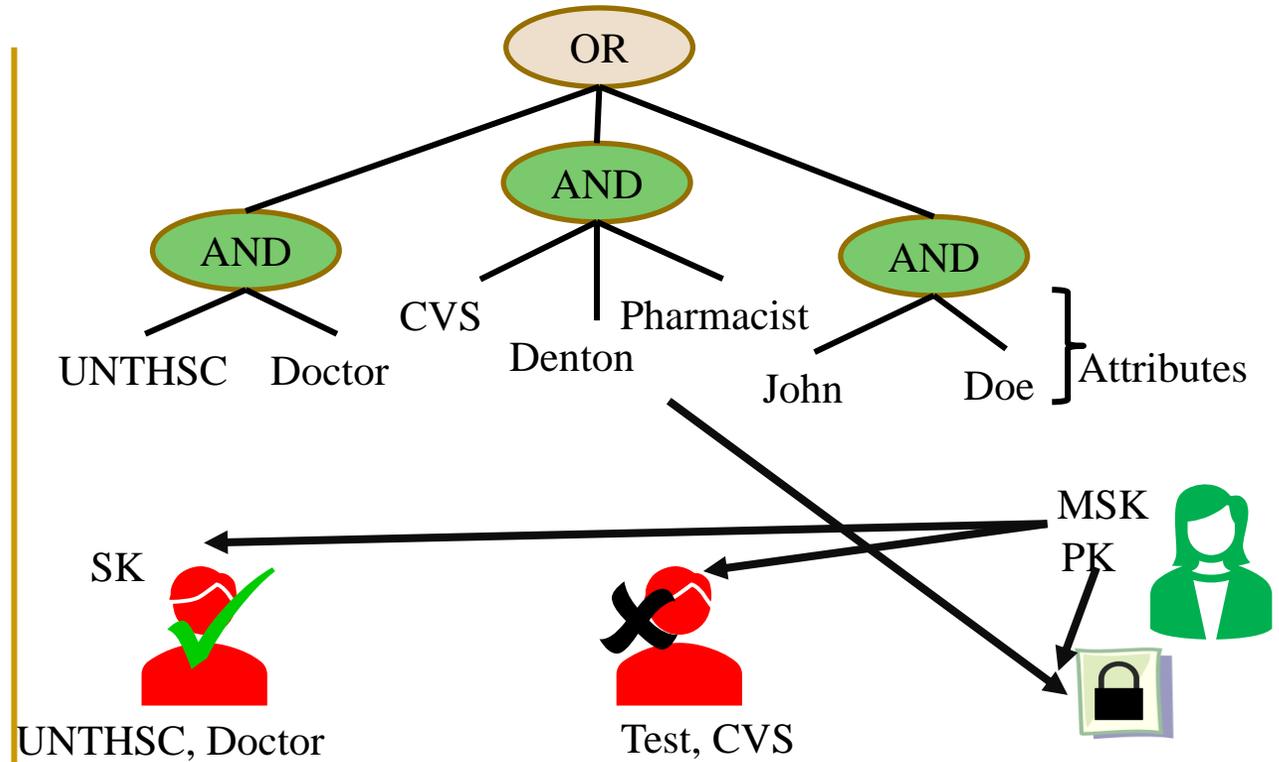
FortiRx Architecture



Asymmetric Encryption vs CP-ABE



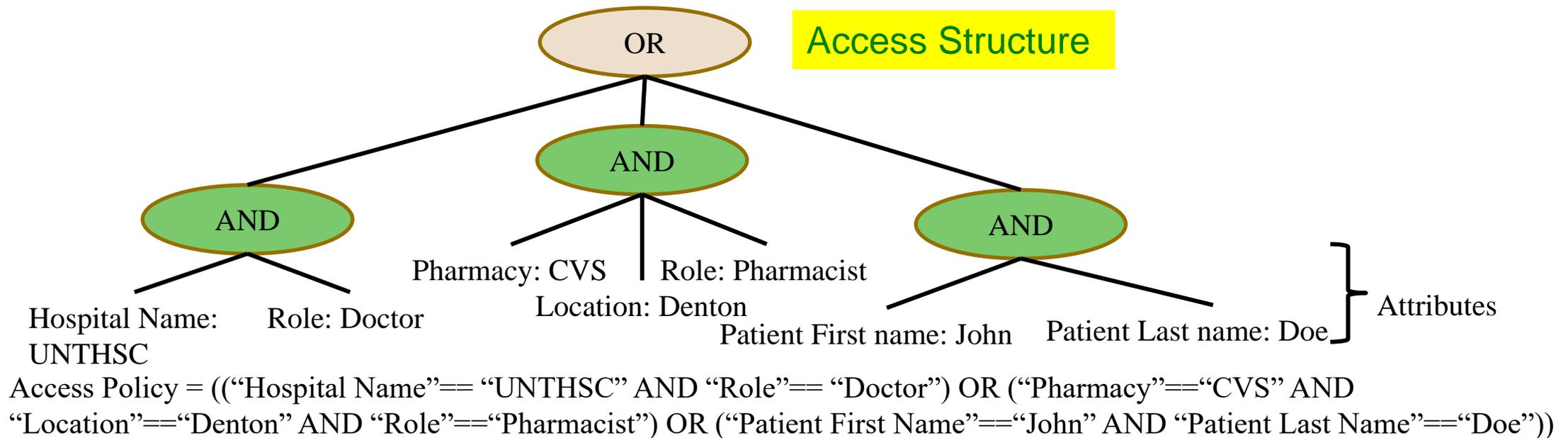
- Secure but not flexible
- New key for every participant
- Fine-grain access control not possible
- Needs efficient key distribution



- User private keys based on “attributes”
- Files can be encrypted under “policy” over those attributes
- Can only decrypt if attributes satisfy policy

Access Control Mechanisms

- For Prescription Access
 - Cipher text-policy attribute-based encryption (CP-ABE) allowing fine-grained control of data access
 - Data-sharing among multiple parties without revealing the content of the data.
 - Access the data based on attributes, such as roles or clearances rather than specific keys.
 - Effectively scales as the number of parties involved in a multi-party access scenario grows

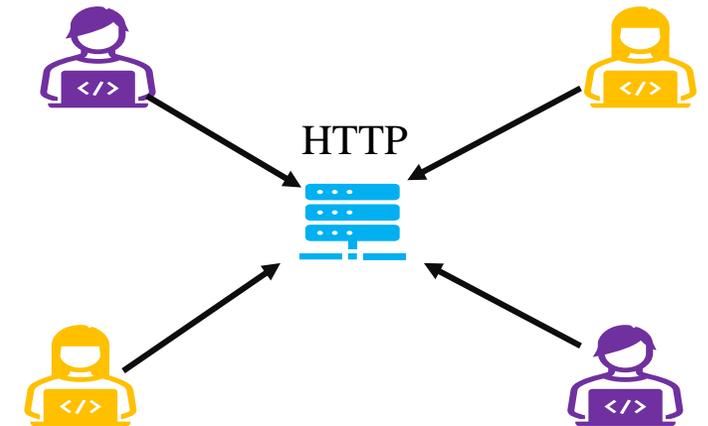
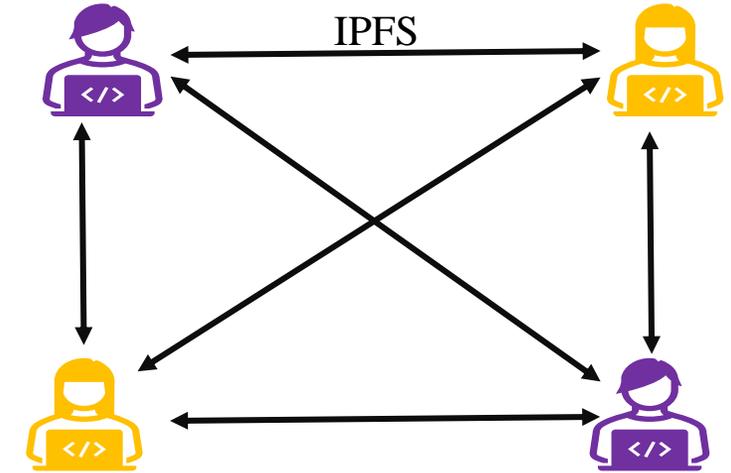


Access Control Mechanisms

- CP-ABE Steps
 - Key Generation – Generates a **master key and a set of attributes**
 - Attribute Assignment – **Attributes assigned** to users or entities
 - Policy Specification – The data owner **specifies an access policy** using a set of attributes
 - Encryption – The data owner **encrypts using the access policy**
 - Decryption – Requesting user **attributes evaluated against policy** and information before decrypting
- For Role Specific Functions
 - **Role-Based Access Control (RBAC)** mechanism automated using smart contracts.
 - **Define, assign, and revoke roles** for specific External Owner Accounts (EOA)
 - **Modifiers** defined and assigned to different smart contract functions
 - Authenticate role-based transactions and **prevent unauthorized access.**

Distributed Data Storage (IPFS)

Aspect	HTTP	IPFS
Adoption and Support	Widespread, universally supported	Growing adoption, expanding support
Protocol Complexity	Simple, well-established	Decentralized, content-addressed
Caching	Supports various caching mechanisms	Distributed content, local caching
Direct Access	Connects to centralized web servers	Peer-to-peer and distributed access
Control	Centralized control by web server	Decentralized, no single control
Data Addressing	URL-based addressing	Content-based addressing (hashes)
Redundancy and Resilience	Limited redundancy	Content distributed across nodes
Data Immutability	Can be updated by the server	Immutable content, cannot be changed
Data Sharing	Limited sharing without a server	Easy sharing with peers and nodes
Offline Access	Requires internet connection	Offline access to previously viewed
Data Retrieval Efficiency	Traditional DNS-based lookup	Efficient DHT-based content routing



Prescription Upload Steps in FortiRx

- Generate a **digital prescription** and create a file.
- For each prescription file, **open and read the contents**.
- Encrypt the prescription content **using a public key and the patient's access policy**, creating a ciphertext.
- For each encrypted prescription file and **upload to IPFS**.
- Retrieve the **Content ID (CID)** from the IPFS response.
- Create a new transaction in the prescription smart contract to **create the prescription** for the patient.
- If the caller of this transaction is the prescriber:
 - Create a new prescription and **associate it with the patient's address**.
 - Emit an event with prescription data, **generating a log**.
 - Return the **transaction hash (Txhash)**.
- If the caller is not the prescriber, **reject the transaction**.

Algorithm 1 Proposed Prescription Upload Algorithm for FortiRx.

Input: Digital Prescription Data, public parameters (params,g1,g2,e) generated during CP-ABE setup, Access policy p defined by the patient

Output: Content ID for IPFS file, Transaction hash of prescription creation in blockchain

```
1: A digital prescription is generated, and a file is created
2: For each prescription file f do
3:     Open file in read mode
4:     FileItem  $\leftarrow$  open(filePath,'r')
5:     Read prescription content from the file
6:     prescription content (Pcontent)  $\leftarrow$  fileItem.read()
7:     Encryption is done using the public key (pk) and policy  $p$  to generate ciphertext of the prescription content
8:     Cipher text CT  $\leftarrow$  cpabe.encrypt(pk, Pcontent , $p$ )
9:     A new file is created and generated cipher text is written to that file
10: end for
11: For each encrypted prescription file f do
12:     Send upload request to IPFS
13:     Response (res)  $\leftarrow$  requests.post(Infura endpoint, authentication parameters, file f)
14:     Content ID from response is retrieved
15:     Content ID (CID)  $\leftarrow$  res.text['Hash']
16: end for
17: Prescriber creates a new createPrescription transaction in prescription smart contract
18: Transaction (Tx)  $\leftarrow$  prescription.createPrescription(patient address (Paddr),CID)
19: if caller == Prescriber then
20:     A new prescription is created and added to patient's address
21:     Emit an event (ev) with prescription data and a log is generated
22:     Return transaction hash (Tx hash)
23: else
24:     Reject Tx
25: end if
```

Prescription Retrieval Steps in FortiRx

- For each view request, Retrieve the prescription based on PID from the blockchain using the smart contract.
- Get the IPFS Hash (CID) of the prescription from the retrieved data.
- Request the prescription content from IPFS using CID.
- Receive the ciphertext (CT) from IPFS.
- Obtain a secret key for a specific set of attributes (attr list) from a trusted authority.
- Decrypt the ciphertext (CT) using the secret key to reveal the prescription content.
- Display the decrypted prescription content if the access policy (ρ) evaluates positively for the attribute list (attr list)
- If the access policy doesn't match the attribute list, decryption is not allowed.

Algorithm 2 Proposed Prescription Retrieval Algorithm for FortiRx.

Input: Prescription ID (PID) generated while creating new prescription in blockchain, attribute list of requesting entity (attr list)

Output: Decrypted prescription content (Pcontent)

```
1: For each view request (req) do
2:     Send a function call to prescription smart contract to retrieve Prescription
       based on PID
3:     Retrieved prescription Pret  $\leftarrow$  prescription.viewPrescription(PID)
4:     Get IPFS Hash (CID) from the function response
5:     CID  $\leftarrow$  Pret['IPFSHash']
6:     Send a request to IPFS to retrieve prescription content (Pcontent)
7:     Response (res)  $\leftarrow$  requests.post(Infura end point, CID, authentication
       parameters)
8:     Retrieved cipher text (CT)  $\leftarrow$  res.text
9:     Secret key for a set of attributes attr list is requested from trusted
       authority
10:    Secret key (Sk)  $\leftarrow$  cpabe.keygen(public key (pk), attr list)
11:    Decrypt cipher text using the secret key to get prescription content
12:    if  $\rho$ .evaluate(attr list) then
13:        Pcontent  $\leftarrow$  cpabe.decrypt(Sk, CT)
14:    else
15:        Cannot decrypt prescription content
16:    end if
17: end for
```

Prescription Retrieval Steps in FortiRx

- Pharmacy or physician sends different **status updates**.
- Depending on the type of update, the smart contract is called with the PID as a parameter.
- If the prescription is filled:
 - The smart contract **marks the prescription as filled**.
- If the prescription needs re-filling:
 - The smart contract **requests a refill**.
- Otherwise:
 - The smart contract **issues a refill**.

Algorithm 3 Status Updates for Prescription on Blockchain.

Input: Prescription ID (PID) generated while creating a new prescription in blockchain

Output: The Status of the prescription will be updated

```
1: Different status flag updates will be sent either by the pharmacy or physician
2: Based on the type of status update, different functions of the smart contract
   will be invoked with (PID) as parameter
3: if the Prescription is filled then
4:     prescription.updatePrescriptionStatus(PID)
5:     Smart contract check the pharmacy Ethereum address for
       access and updates isFilled flag of prescription
6: else if Prescription needs re-filling, then
7:     prescription.requestRefill(PID)
8:     Smart contract checks the pharmacy Ethereum address for
       access and updates the requestRefill flag of prescription
9: else
10:    prescription.issueRefill(PID)
11:    Smart contract checks the physician's Ethereum address for
       access and updates the isFilled and requestRefill flags of
       prescription
12: end if
```

Used Sample Prescription Data

John Doe's Bags of Medications

(Note: you would only know what these are if you accessed an electronic pill identifier site like Drugs.com)

Morning Ziplock:

- Allopurinol 2 50 mg tablets: learn he takes 1 or 2 a day depending on whether he has gout
- Aspirin ½ tablet: doctor told him to take ½ tablet
- Clopidogrel 75 mg tablet
- Colchicine 0.6 mg tablet
- Glyburide 1.25 mg tablet
- Toprol XL 50 mg tablet
- Amiloride 5 mg tablet
- Enalapril 20 mg tablet
- Tylenol Arthritis 2 650 mg tablets

Afternoon Ziplock:

- Tylenol Arthritis 2 650 mg tablets

PM Ziplock:

- Colchicine 0.6 mg tablet
- Glyburide 1.25 mg tablet
- Simvastatin 80 mg tablet
- Warfarin 5 mg tablet
- Amiloride 5 mg tablet
- Enalapril 20 mg tablet
- Tylenol Arthritis 2 650 mg tablets

Also has:

- Nitroglycerin bottle of 0.4 mg tablets – takes 1 QD or QOD
- Albuterol inhaler: prn. Does not use often.

Used Sample Prescription Text
File Size: 913 bytes

Source: https://www.hospitalmedicine.org/globalassets/clinical-topics/medication-reconciliation/1_john-doe-case-prework-for-pharmacist-trx-1.pdf

Encrypting and Uploading Prescription to IPFS

```
Encrypted Data
['c1': ['C_tilde': [32156964776025433085096874272998427334474690479036758738867865391736110265035806644773102421649340468956817050900697756452955137114836886501609304445748, 837566400379269078798303153
19691246205565349842994900409338517553806195602057778685102134271693894843639320183727569793818305191624227910299357750124601], 'C': [35452860066177970745295353727985347783341377828447315317630053998745
07628734915994424113705903400007883082931881184216803491065802701878551738836198921870, 8357053971270548801898742801451558038099081469002626868467580741935564068249681349737230985853273920132115071118597
64557659959088159491163104986261305214], 'Cy': {'ONE': [4217179885320506263312146963615183191512100553202611568455650253400934844995153706997045163476799688287756796260512866682609534992049935635875
63283619, 521411298979699148156064926499203539413429517230529788341220697770026386366158867940853699866716963139130467454735515028414526899174370938814309913794843], 'THREE': [4217179885320506263312146
96361518319151210055320261156845565025340093484499515370699704516347679968828775679626051286668260953499204993563587563283619, 5214112989796991481560649264992035394134295172305297883412206977700263863
66158867940853699866717696313913046745473551502841526899147370938814309913794843], 'TWO': [7762487388522305284239768943199371974824965547049285766171004475226355148997034444542313563612682920869926404282215546936496015506735462602279385429747926, 811814252755172149204979014182244586580469082343534043013471943922402107540724704693686375820755678411209976200944280682568090336860288528588108636765908], 'F
OUR': [7762487388522305284239768943199371974824965547049285766171004475226355148997034444542313563612682920869926404282215546936496015506735462602279385429747926, 8118142527551721492049790141822445865804
69082343534043013471943922402107540724704693686375820755678411209976200944280682568090336860288528588108636765908], 'Cyp': {'ONE': [3462661131960550795121839248675829474122878610292834400114018667171825
605253080081037893556941071298311923283299152606716901449101714563002436022383875549, 384423083439924605676512364496339064880684431192825901672750096995758419131423052516109930287272043813550761683608946
0582888374449758314100827252215751090], 'THREE': [757785805731901553911227913961455252556578719604877357264777204903429178043496961384526104595465638589602661347458825158195035073807780654629261877305840
3, 10801058640177912383430790832492492313938988247724311998991797113424481055087320699428305724449140293543089443701536449039254610444906603481227280721629], 'TWO': [83447765333904796760820617110950164
223451087912755754086583352868823538015924755773886449395718065820142364107517989624398404789041439504609573675701538, 860723671256165508057329895536776690030594915101525662237854327801280133721463318
4234746936356553254032732562497913359353608713961993343064197039244719], 'FOUR': [8064280825192130672032932068400289718329034108824984457467435311752920179567656372544882832421463582743642008109993448545
751611723264241486021136894681073, 3561827273631685939592151147010324151126824743991426854170279092465456120594687755108122993849588458094019627359816582456598437223146568156560112031271351]], 'policy':
['(ONE or THREE) and (TWO or FOUR)'], 'attributes': ['ONE', 'THREE', 'TWO', 'FOUR'], 'c2': {'alg': 'HMAC_SHA2', 'msg': {'"ALG": 0, "MODE": 2, "IV": "3xchsyuYidxRTKE/wdWcXg=", "CipherText": "1dKUFv1/IAQ
G0lqe16ZNVxbJP+25Fuy3YfZcFjBBys2GdnvSQV6s3M4ofIVGIBI9790UNRRzYsRL6FoAlIIVs3XdmZuJGjv5TmXhVgZB/Ux789XfTPkz60K7eUl4q8Fv0r2Chsi1EaTXIfID0tEmMAjY1zj1lS8yUvXm3G/zsYDqoaevtaWqtu7YbZ5p060be1qIA0YC1DHL
F4vTIoPqXm6NqzSYNNWw4R6+Ui+5DA0kicLvlJllYsZiVsoo+nC1LSIAITvgyt40CMKkyomFkVxrECAP90832f0c7bqTtpvBN0RQbdAyHGoV6esfLaeX1LqLDcn/vWtqg7+ls+Sto8M0oo0tlvG2qjsot0nll7VbvtkmrnxwllVsq2xtenx8P6RE55d0QCXFRH
7UMGEPHSt0EVrAXFmWlWlFqctOM9tu4J1zc/CI72P5BRwornme803Kf10hu3F810vB0etuo60r3zAdCn4tyY2jy/SeL0dLnQarJtCUB2CE-Vz+RRQYPM+PltoYUvPuhfGpBeW0gKuvh010yVqrMGVjOKLmFyNL4RF+K9UNfINT84msD/UU0g8EKU0W7N6mP4ki9s/r
ZERGdHLkTsnzcw0qe+LTXue4AjgdAIYglDx4dVK+TCch/qAychMddj+wIB0exeh89Xg1cnlqAVA5VJpJnPBfFlmP5qwZ5tg+8DtXhLuvjqldFmaEVlqcW82yUuV0Cccbtu+iu16D7m3K65kovJALZ+i89Hsf0chUuxWabP3ysyiA8y8SZ7S8M0P51/ubQ4k0jMEHG
vI4m2a6tk3ALuTBcrZZF/hemt2/mSn/wfbsQC4A+Hb9P57fn/GY+P8hdPjFO0+HeYxyN4xrY5EJACV0cnvbnhYQRJaEFLEX5BULNSS65Z0MAqha+gzdCmXqJUuYxYjwzTAKHfrevAwLb157VVOXLDK4FYWJRHROTWA3gaCnMhBTPyFUUV2upIITCskn73bX1y11a8CwJ
sv4lsgHASqjehFeb8F0zf1mzc3JXiqzCcZLHvd4hbgVee1HsCRz0QvQnJabGSHWj/57FqX+cZSDE3Fus/cMPrEGGjJMSN7HmvyV6icjATQw4d+OzzM73GNMVMcInttFPAIG858wXmNz2YNN1ZVusjvm/rFfAvDnHfToFCY10GFWSUGFAVzyTwPKZyXMGWmgZr
UaaLNxz0g="}], 'digest': '20776da162fb1e825c56dad07f1c1c33bc776ad7a6c0c7da14468441e4f95'}}

Content ID
<Response [200]>
Prescription.txt: Qme7S5q8LmE875Ke79yQWfY9wQ4YnTEHMur511PrZFF
Folder CID: QmWP13wr64ft1nT7PUPm3wxBr0s5x1Lv1jzWg1zFNXtJFRh

Decrypted Data
[2055518218368535312257156353032542535393806874053072486268224518005117455169046211829527488705937844597456797852989786590374842683211657473035663777879271, 3720114716169197903951888851439982024564117839
553509220866437609836832652740866847294379841501181255853864519743502467547014029491057158033532387391522880]
b'John Doe\x20\x99s Bags of Medications\n(Note: you would only know what these are if you accessed an electronic pill identifier site like\nDrugs.com)\nMorning Ziplock:\n\x20\x80\x2a Allopurinol 2 50
mg tablets: learn he takes 1 or 2 a day depending on whether he has gout\n\x20\x80\x2a Aspirin \xc2\xbd tablet: doctor told him to take \xc2\xbd tablet\n\x20\x80\x2a Clopidogrel 75 mg tablet\n\x20\x80\x2a
a2 Colchicine 0.6 mg tablet\n\x20\x80\x2a Glyburide 1.25 mg tablet\n\x20\x80\x2a Toprol XL 50 mg tablet\n\x20\x80\x2a Amiloride 5 mg tablet\n\x20\x80\x2a Enalapril 20 mg tablet\n\x20\x80\x2a Tylenol Arthritis
2 650 mg tablets\nAfternoon Ziplock:\n\x20\x80\x2a Tylenol Arthritis 2 650 mg tablets\nPM Ziplock:\n\x20\x80\x2a Colchicine 0.6 mg tablet\n\x20\x80\x2a Glyburide 1.25 mg tabl
tatin 80 mg tablet\n\x20\x80\x2a Warfarin 5 mg tablet\n\x20\x80\x2a Amiloride 5 mg tablet\n\x20\x80\x2a Enalapril 20 mg tablet\n\x20\x80\x2a Tylenol Arthritis 2 650 mg tablets\nALS
troglycerin bottle of 0.4 mg tablets \x20\x80\x93 takes 1 QD or QOD\n\x20\x80\x2a Albuterol inhaler: prn. Does not use often.\n'
osboxes@osboxes:~/desktop/FortiRX$
```

Encrypted Prescription

Content ID from IPFS

Retrieved Prescription Information

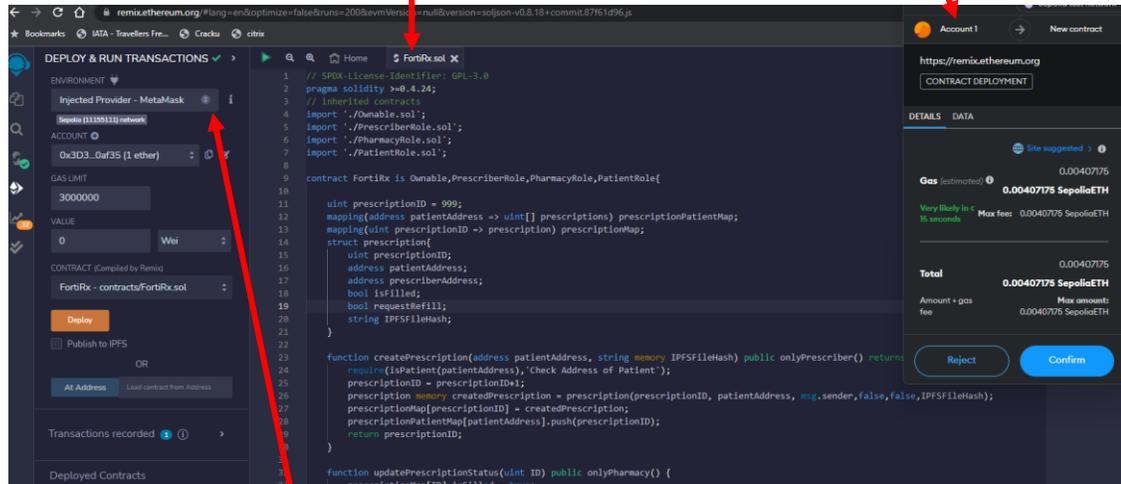


Smart Contract Deployment

Deployment in Sepolia

Smart Contract

Wallet Transaction



Remix Environment
Network Configuration

Ethereum Addresses with Roles

Feature	Value
Physician Account Address	0x3d352313f4f5561d0ffbda205b52a3c3b70af35
Pharmacy Account Address	0x3D352313F4f5561D0fFBda205B52A3c3b70af35
Patient Account Address	0x2a9884dfa7E6890FE8AA99FE2486c613C32b697a
Contract Deployment Hash	0x798d1f5ff49f9df09b9856db2646cebc2029d5cd2a45c5ef0c1b9acb9f217c6f
Prescription Content ID	Qme7Sq8gLmE875kE79QyWWFy9wqQ4yHnTEHMr511PrZfF
Prescription Creation Hash	0xda5bd0ce943325696e91bfe140bd8cdd60eafdc6f2a41b07221e499bfe7f1f7

FortiRx 2.0: Smart Privacy-Preserved Demand Forecasting of Prescription Drugs in Healthcare-CPS

Motivation

- Small changes in the demand at the consumer level can progressively increase the fluctuation the upstream of supply chain
- Patient needs are ever-changing: e.g., serious illness, public health crisis (COVID-19)
- Demand forecasting errors at lower levels of PSC can lead to supply chain disruptions. (Witnessed: COVID-19)

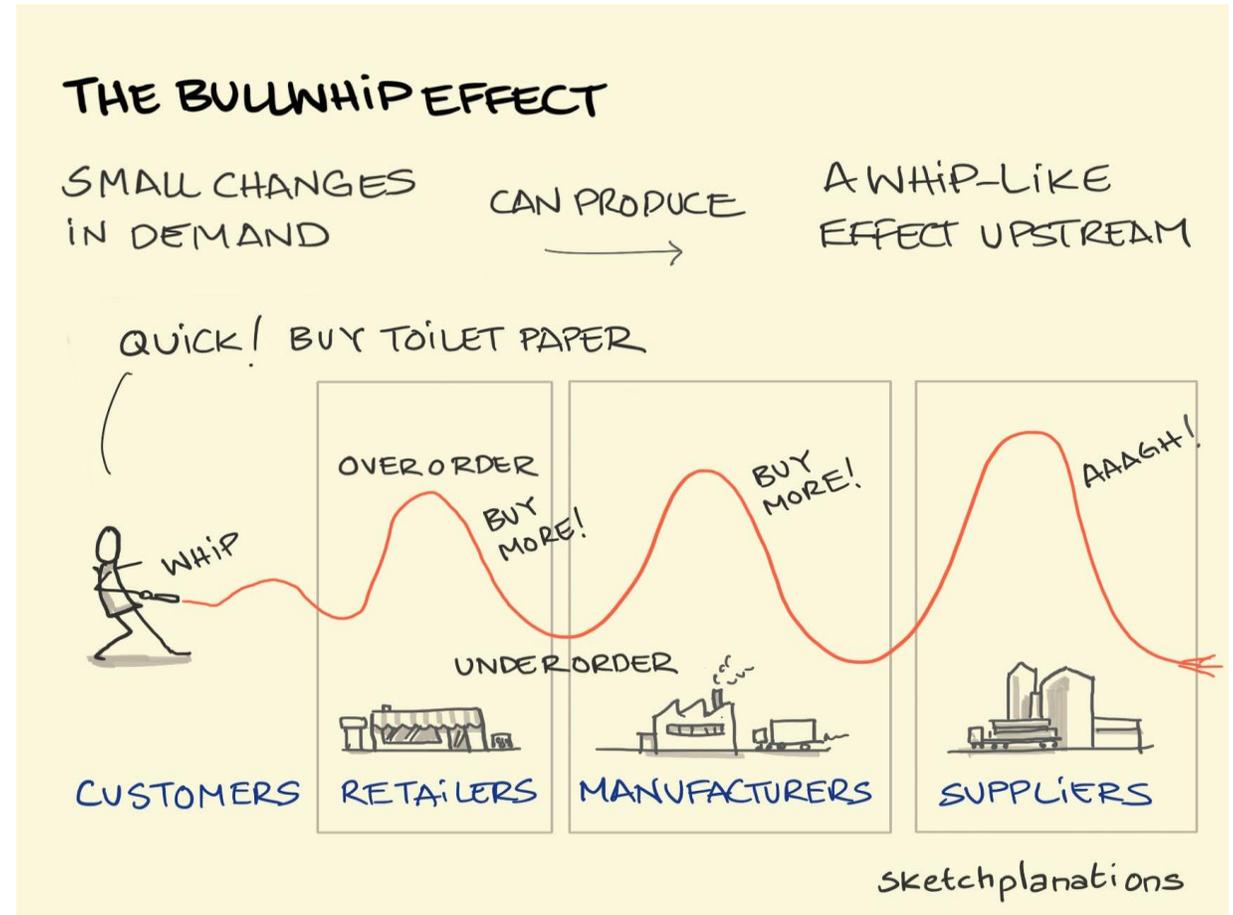


Image Source: <https://sketchplanations.com/the-overview-effect>

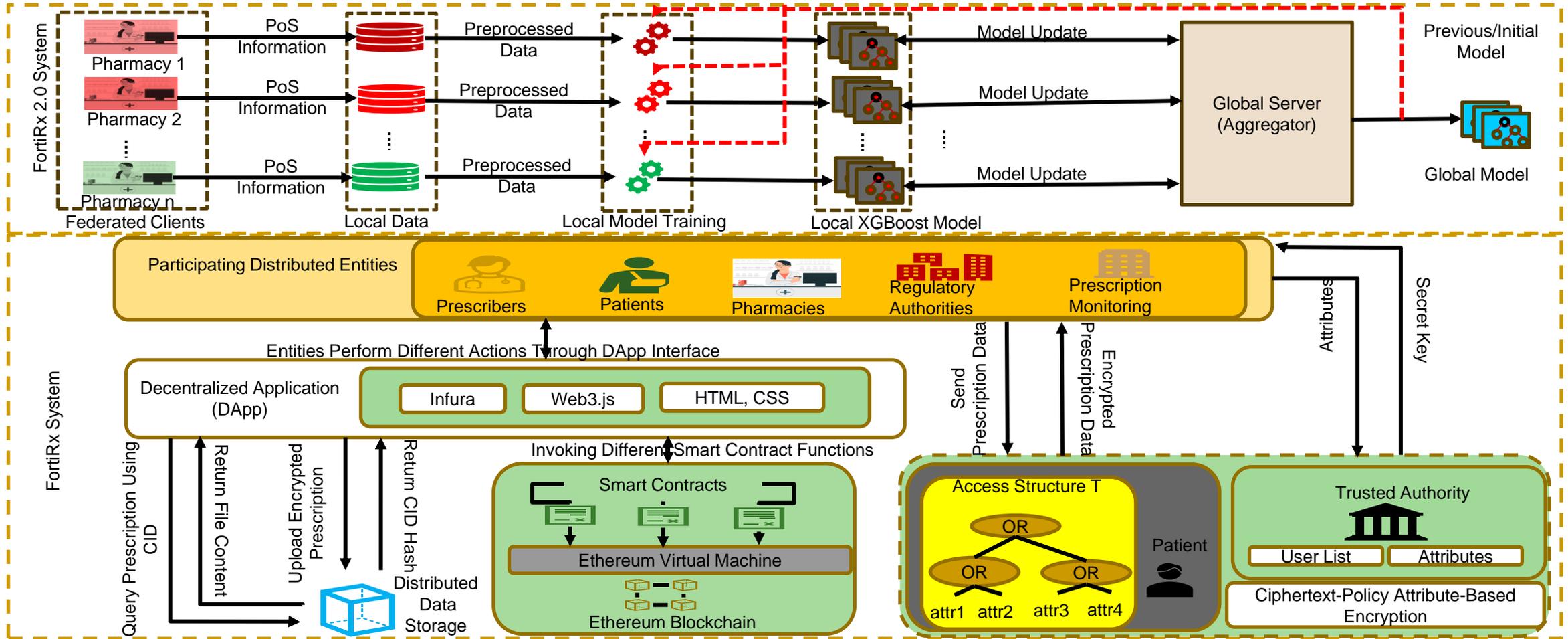
Demand Forecasting Model – PSC Problems



Novel Contributions

- Utilizing **real-time prescription information** can help in creating **accurate DFM** that reduces overstocking and understocking issues in the supply chain.
- Blockchain-leveraged decentralized architecture can help in **real-time sales data** available.
- **Federated learning** approach and **CP-ABE** access control mechanism ensures the **privacy of the patients** and doesn't reveal the patient prescription information to unintended parties.
- Blockchain-based approach helps in creating a **cost-effective** and **adaptable** E-Prescription system.
- The Trust model through consensus protocols ensures **no outliers** and helps in the **accuracy of the DFM**.

FortiRx 2.0 Architecture



Federated XGBoost Steps

- Data is partitioned into **local datasets** and resides at each **local pharmacy**.

$$\text{Dataset } D = \bigcup_{i=1}^n D_{ci}$$

- Each **federated client (Pharmacy)** loads the local dataset and **trains the local XGBoost model** using initialized parameters.

$$M_{ci} = XGBoostTrain(D_{ci}, \theta_{ci})$$

- A **starting point global model** M_{global} is initialized at the server using **global hyperparameters** Θ_{global} as follows:

$$M_{global} = XGBoostInitialize(\theta_{global})$$

Federated XGBoost Steps

- The **number of iterations** of federated training is determined by a **pre-determined value T**.
- At each iteration client c_i **generates a model update** which are gradients ∇_{c_i} and/or Hessians H_{c_i} .

$$\nabla_{c_i}, H_{c_i} = \text{CalculateGradientHessians}(D_{c_i}, M_{c_i})$$

- These computed gradients and/or Hessians will be **packaged as model update** Ψ_{c_i} .

$$\Psi_{c_i} = \text{PackageModelUpdate}(\nabla_{c_i}, H_{c_i})$$

- Updates sent back from the client C_i to the centralized server and **aggregated**.

$$\Psi_{\text{aggregate}} = \text{AggregateModelUpdates}(\Psi_{c_1}, \Psi_{c_2}, \Psi_{c_3}, \dots, \Psi_{c_n})$$

- The aggregated model is sent back to the client C_i and retrained by integrating the aggregated model.

Dataset and Exploratory Analysis

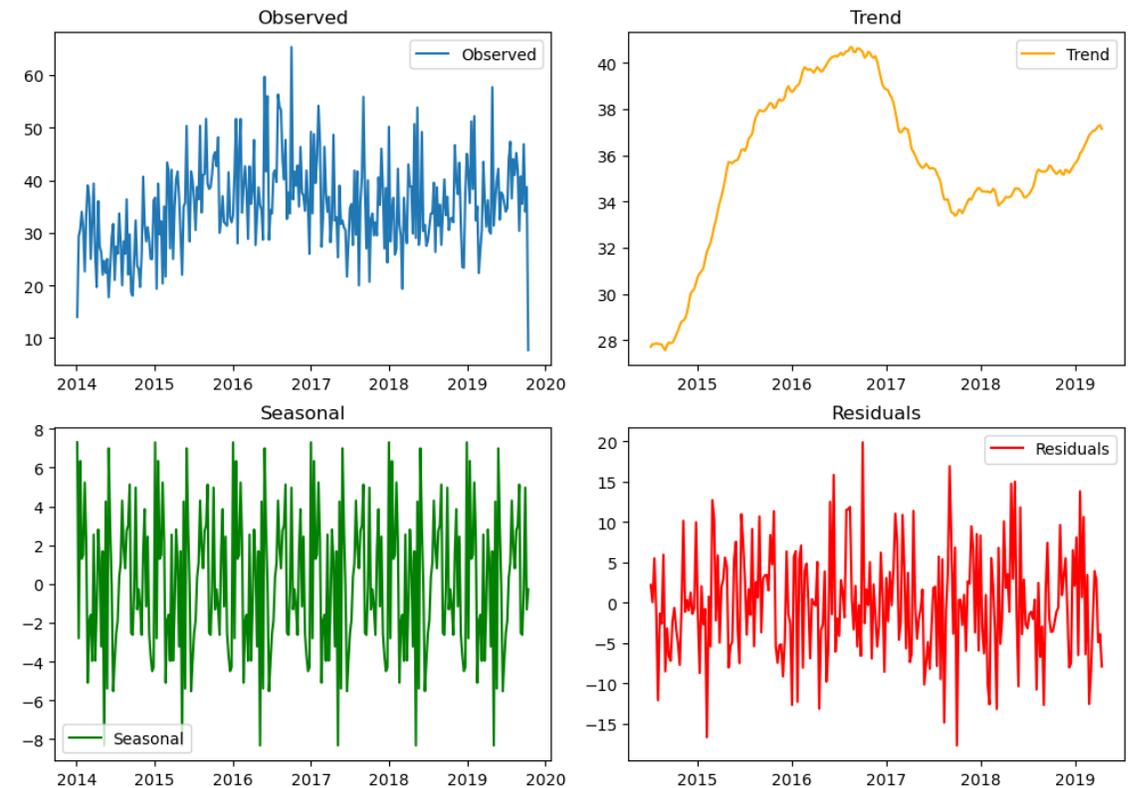
- Public Pharma Sales dataset from [Kaggle](#) is used for simulation and analysis of the proposed FortiRx 2.0.
- Covers sales data collected over [6 years from 2014-2019](#) for a selected type of drugs and [classified into 8 groups](#) based on [Anatomical Therapeutic Chemical \(ATC\) Classification](#).
- Categories: M01AB, M01AE, N02BA, N02BE, N05C, N05B, R03, and R06.

Dataset Name	Frequency	No.of Recordings
Saleshourly.csv	Hourly	656928
Salesdaily.csv	Daily	27390
Salesweekly.csv	Weekly	2726
Salesmonthly.csv	Monthly	638

Dataset and Exploratory Analysis

- Seasonal decomposition – helps in breaking down the time-series data into fundamental components
- Fundamental components: Trend, Seasonality, Residual

Seasonal Decomposition - Drug Category: M01AB



Implementation

- Programming Language: Python
- Desktop: Intel i7-11700F @ 2.5 GHz
- Operating Systems: Windows
- RAM: 16GB
- GPU: GeForce RTX 3060 12GB
- Federated Framework: Flower
- Federated Clients: 5
- Train/Test Split: 80%-20%

Configuration Parameters

Parameter	Value
Train Split	80%
Test Split	20%
Number of Communication Rounds	15
Local Training Iterations	100
Model Update Aggregation	FedAvg
Batch Size of Client	64
Fraction of clients selected for evaluation	1.0
Minimum number of clients need to be connected	1

Evaluation Metrics

- Centralized evaluation is performed with two metrics Loss and Mean Squared Error (MSE).
- Compared with Naïve Forecasting as a baseline for forecasting performance of implemented FortiRx 2.0.

- Naïve Model:

$$\text{Forecast}_{t+1} = \text{Actual}_t$$

- Seasonal Naïve Forecast:

$$\text{Forecast}_{t+1} = \text{Actual}_{t+1-k}$$

Where k is the length of seasonal cycle

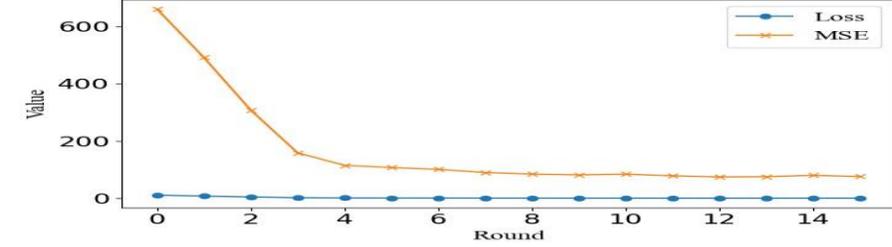
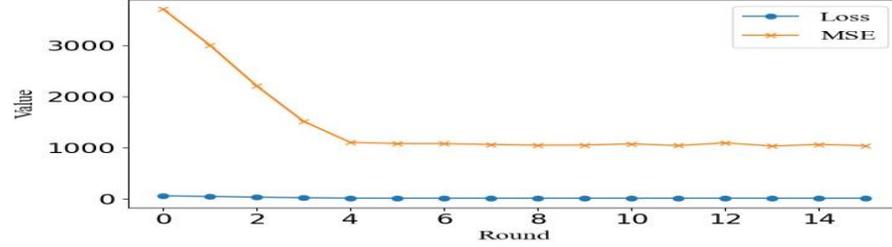
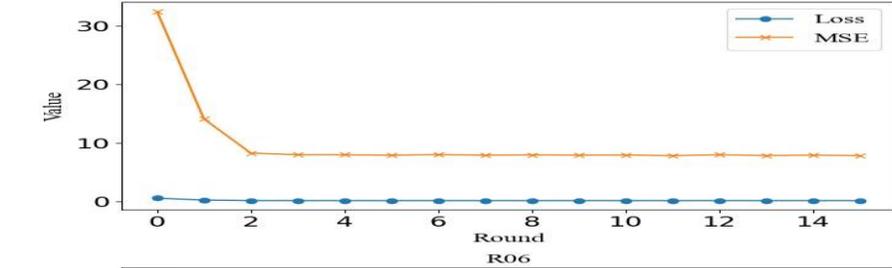
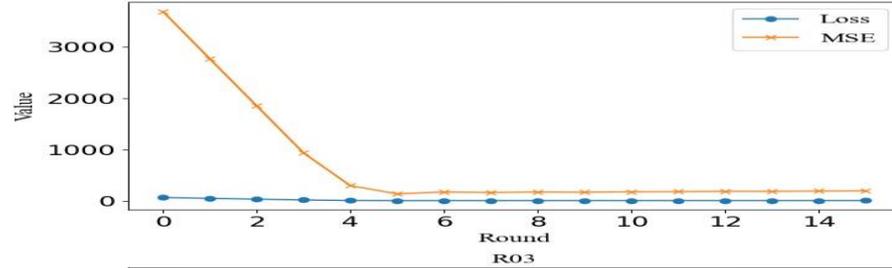
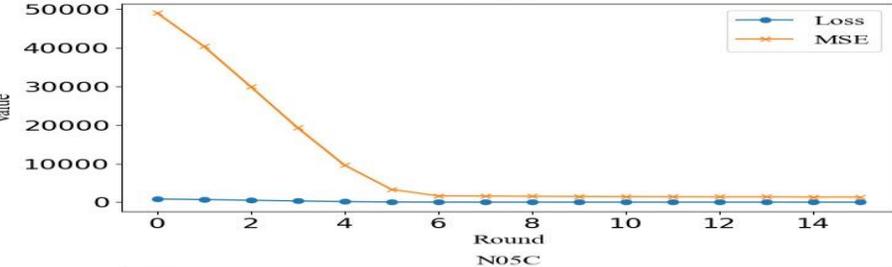
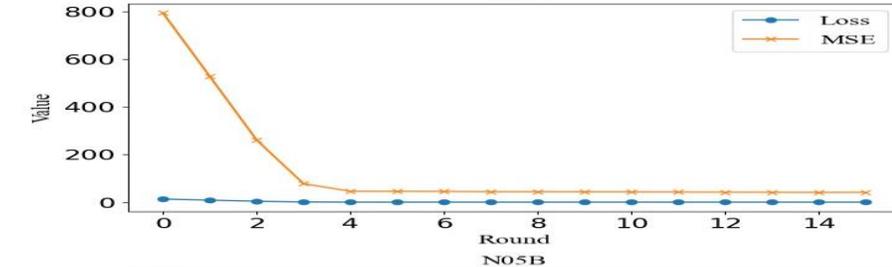
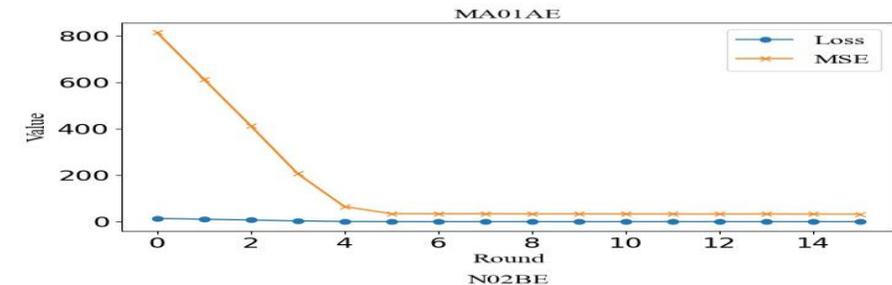
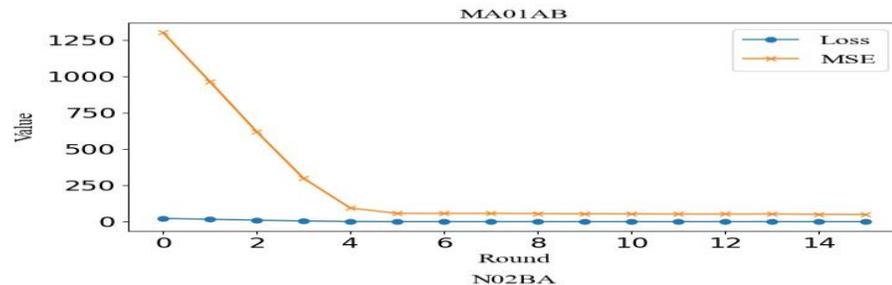
- Loss Function measures the difference between the predicted values from the actual values. Let the Loss L with predicted values \hat{y} and actual value y can be computed as follows:

$$L_i(\hat{y}, y) = (\hat{y}_i - yi)^2$$

- Mean Square Error (MSE) is another metric. Given n data points with predicted value \hat{y} and true value as y.

$$MSE = \frac{1}{n} \sum_{1}^n (\hat{y}_i - yi)^2$$

Evaluation Metrics of Implemented Model



Comparative Analysis with Baseline

Method	Metric	M01AB	M01AE	N02BA	N02BE	N05B	N05C	R03	R06
Naive	Loss	415.83	375.466	267.55	2042.151	629.4	162	1168.25	329.2
Naive	MSE	116.014	93.875	44.741	2753.643	255.485	14.92	948.56	82.228
Seasonal Naïve	Loss	449.31	511.552	301.25	3530.317	699.8	166	1218.167	596.57
Seasonal Naïve	MSE	137.699	197.862	58.105	8829.751	294.693	17.76	1068.78	250.794
Federated XGBoost	Loss	0.86	0.542	0.695	22.76	2.718	0.133	17.702	1.304
Federated XGBoost	MSE	50.073	52.774	41.403	1346.836	161.162	7.845	1044.049	76.623

Conclusions

- A Real-time reliable blockchain-based prescription information sharing system is proposed.
- Efficient usage of this real-time data to build accurate DFM is proposed in FortiRx 2.0.
- The Proposed Federated approach ensures security and privacy of patient information.
- Proposed methods are implemented and analyzed with different metrics Loss and MSE.
- Comparing with baseline models proves the effectiveness of the proposed FortiRx 2.0.

Future Work

- More advanced models like LSTM will be explored to improve the performance of the proposed system.
- Multivariate time series analysis with more exploratory attributes such as location, price of drug, weather conditions, etc. will be designed.

Thank You !!