BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications

https://youtu.be/Epvu9B44ZfQ

한성대학교 HANSUNG UNIVERSITY

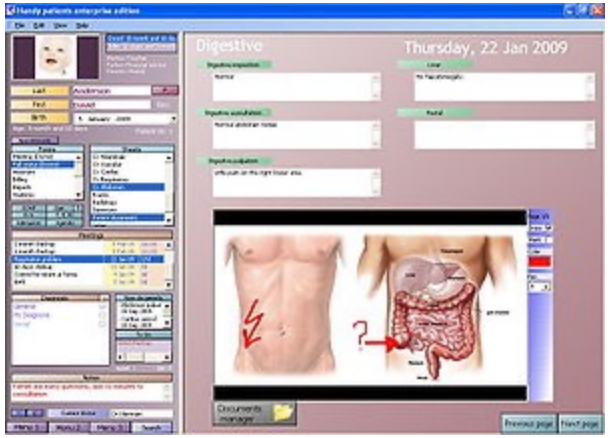
CryptoCraft LAB
https://crypto.modoo.at

개요

- EHR
  - Electronic Health Record (전자의무기록)
  - 디지털 형태로 체계적으로 수집되어 전자적으로 저장된 환자 및 인구의 건강정보

- 본 논문에서는 EHR을 블록체인 기반으로 만듦

- 또한 DaaS(Deep Learning as a Service)를 이용하여 질병을 예측



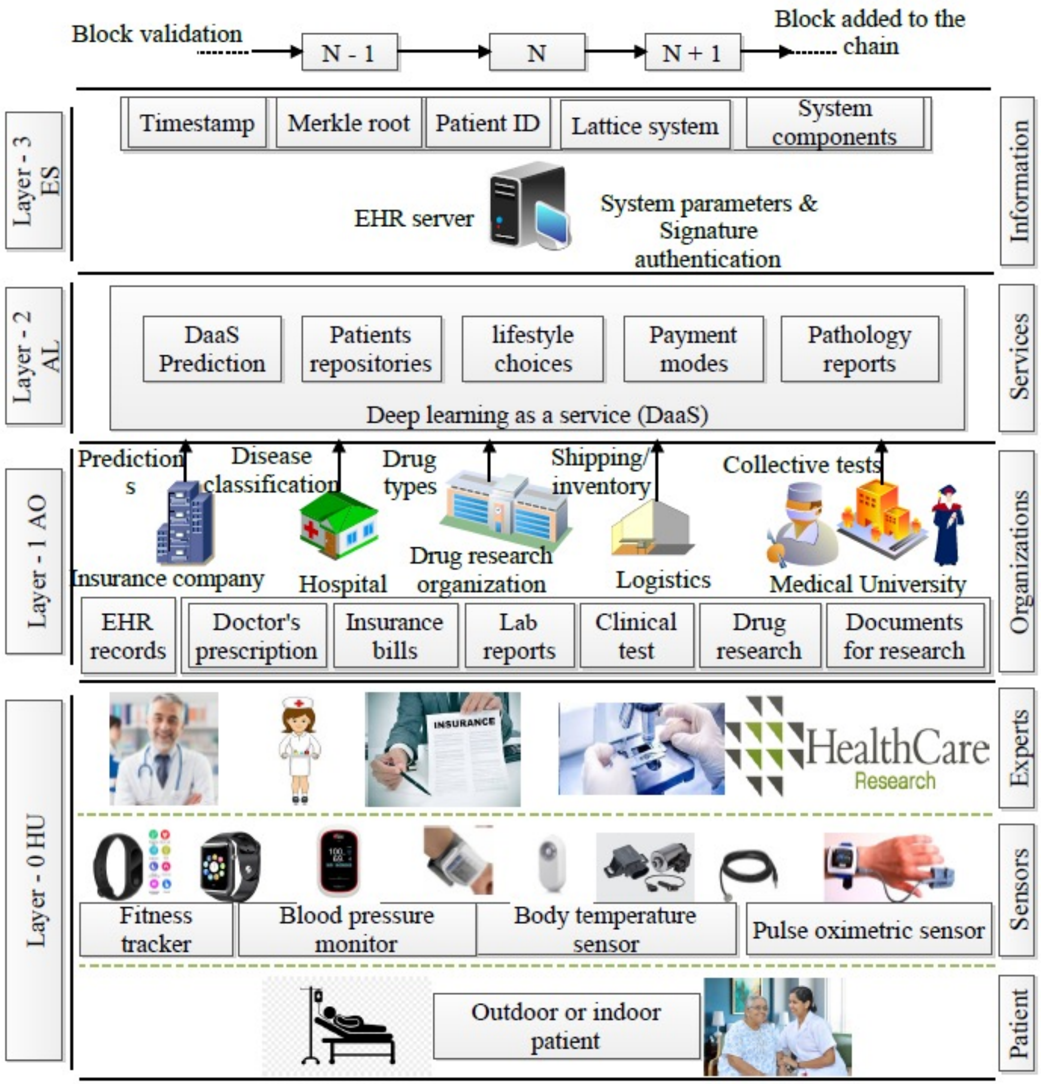
Sample view of an electronic health record

Motivation

- healthcare 4.0 어플리케이션 개발을 위한 프레임워크 (BinDaaS) 제안

- 해당 프레임워크는 블록체인 백엔드 + 딥러닝 기술로 이루어짐

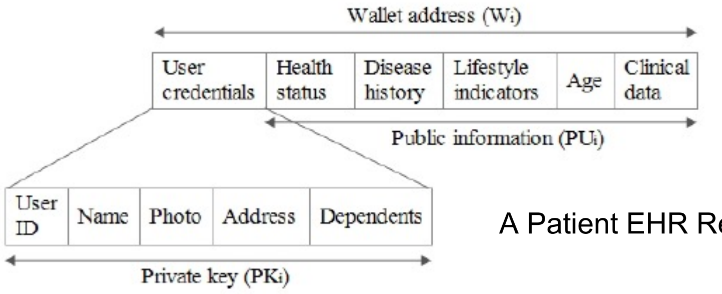
System Architecture of BinDaaS



CASE-I
HU를 통해 수집된 데이터는 AO 레이어를 통해 인증 받아야 함
ex) 의사는 병원에 의해 인증을 받아야 함

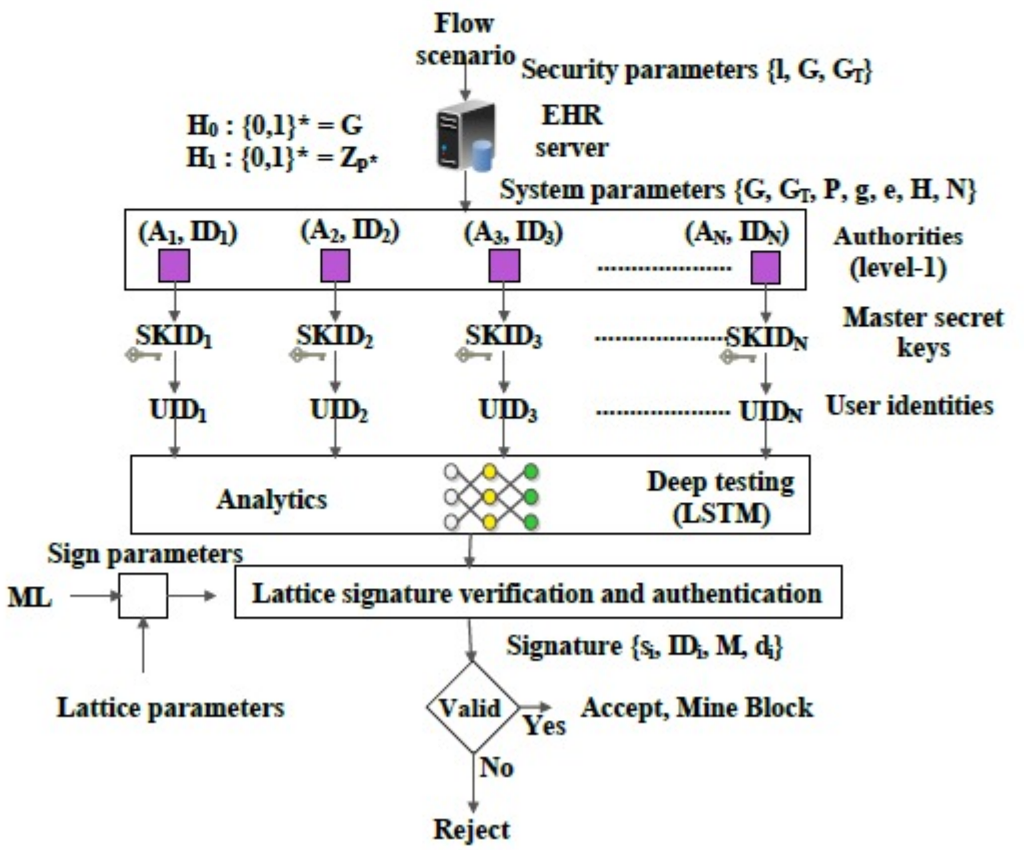
CASE-II
AO 레이어는 ES 서버에 의해 인증을 받아야 함

CASE-III
ES 서버의 파라미터들이 충족되면, ES에 의해 ES_Notary에서 공증 작업을 수행한 뒤 새로운 블록을 생성하여 네트워크의 모든 유저에 전파



A Patient EHR Record Structure

Proposed HCAAM scheme using lattices in BinDaaS



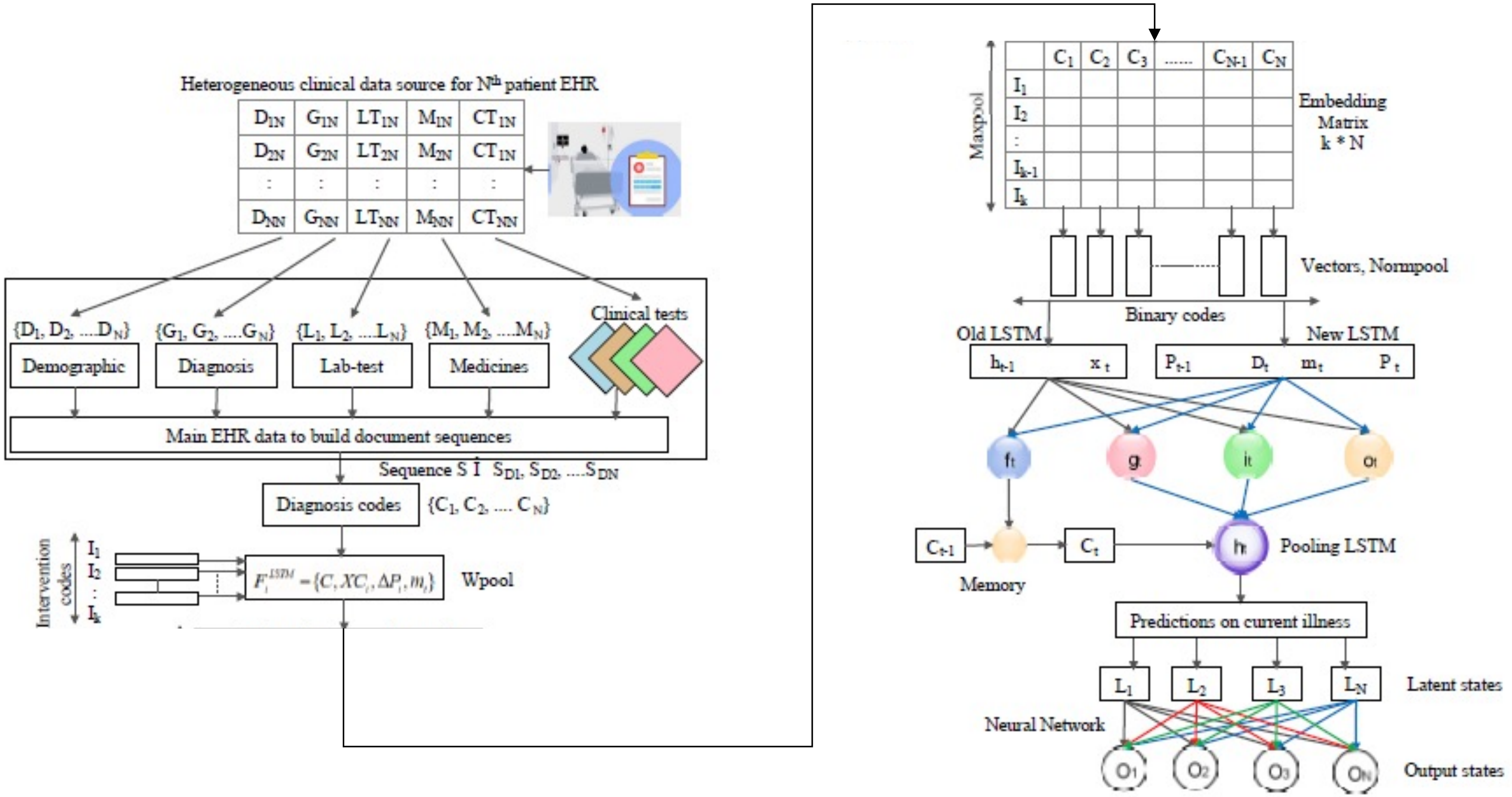
a scheme heterogeneous collective authority authentication mechanism (HCAAM, 다종 집단 권한 인증 메커니즘)

이전 페이지의 그림에서 요청은 아래에서 위로, 시큐리티 파라미터는 위에서 아래로 이동

아래 레이어(AO 등)에서는 다양한 위 레이어(AL 등)의 요청을 처리해야 하기에 다종 집단의 권한에 대한 인증이 필요함

이것을 HCAAM이 처리

DaaS integration in BinDaaS using LSTM for future risk predictions from EHR



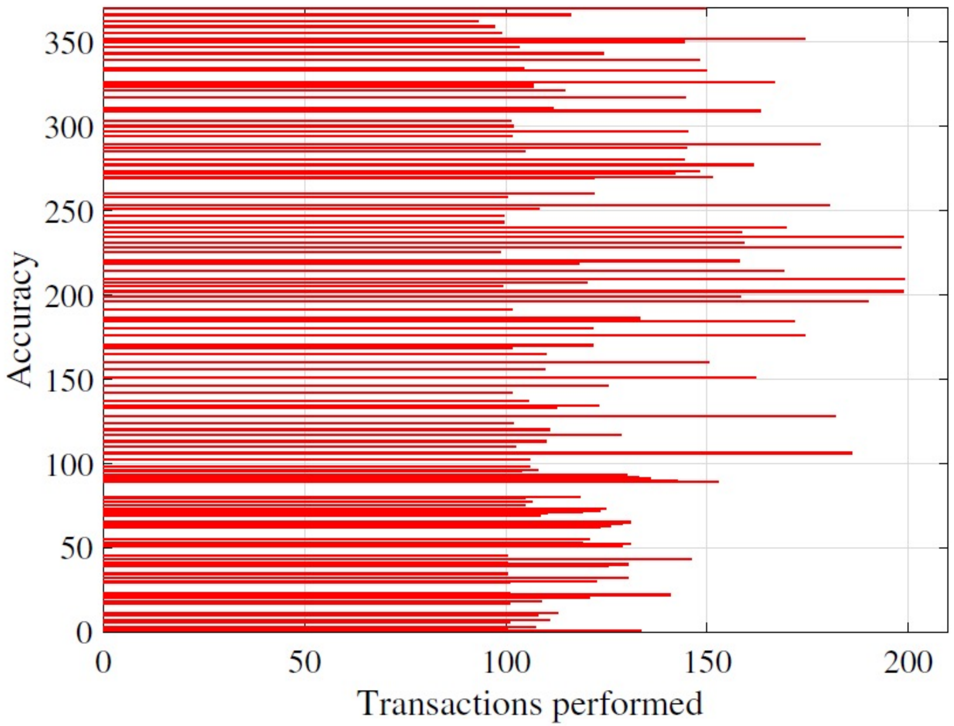
LSTM DaaS for future prediction of disease

Algorithm 3 *LSTM DaaS* for future prediction of diseases

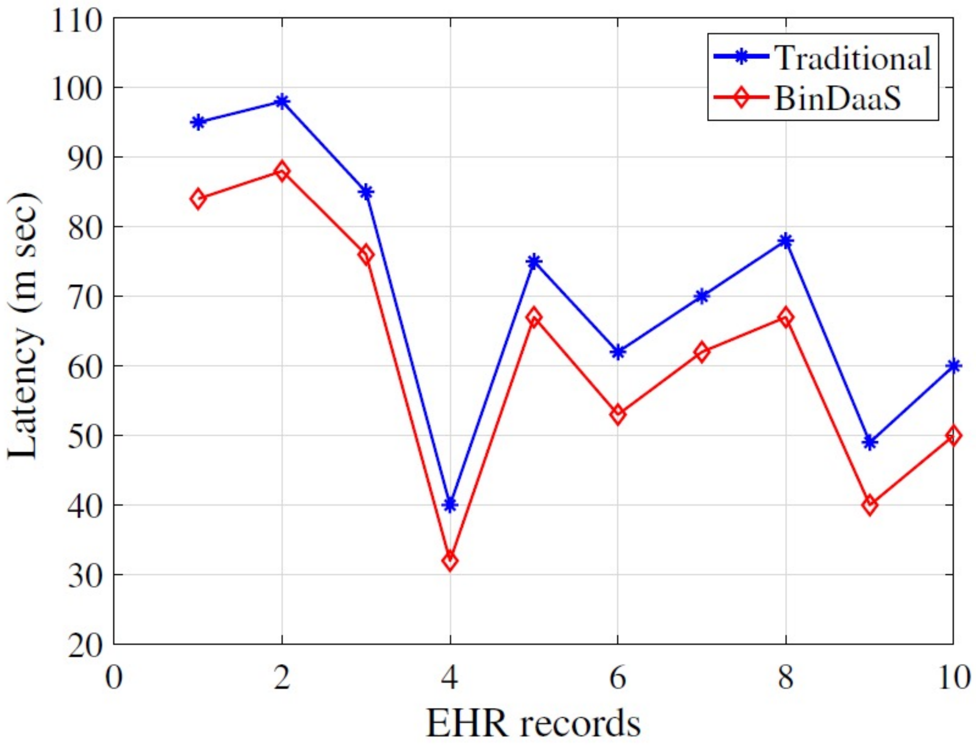
Input: Patient EHR records $D_1, D_2, \ldots, D_n$ as sequence of admissions $S = \{S_{D_1}, S_{D_2}, \ldots, S_{D_n}\}$ for n users.
Patient diagnosis codes $C = \{C_1, C_2, \ldots, C_n\}$ as feature vectors $x_{c_i} \in R^m$
Patient interventions $I = \{I_1, I_2, \ldots, I_k\}$ as feature vectors $x_{I_i} \in R^m$, where m is vector dimension length, elapsed time Δt for each i^{th} patient.
Admission codes from *WPool* with associated probabilities P(*WPool*)
Output: Future prediction of patient health based on outcome probability $P(y|h_{1,2,\ldots,n})$.
Initialization: $i = 0$, $j = 0$, memory state of LSTM $c = 0$;

for $(i \leftarrow 1 \text{ to } n)$ **do**
  $F^i_{LSTM} \leftarrow \{x_{c_i}, x_{I_i}, \Delta p_i, m_i\}$
  $R^m \leftarrow WPool(\varrho_1, \varrho_2, \ldots, \varrho_n)$
  $K \leftarrow Compute\_length\ P(y|\varrho_{1,2,\ldots,n})$
  $\Delta P^t_i \leftarrow D^t_i - D^{t-1}_i$
end for
for $(i \leftarrow 1 \text{ to } n)$ **do**
  for $(j \leftarrow 1 \text{ to } k)$ **do**
    $W_{ij} \leftarrow Embed\_Matrix\ ((D, Z))$
    $B = \{b_0, b_1, \ldots, b_n\}$
    $x^i_t \leftarrow max\{A^{d_1}, A^{d_2} \ldots, A^{d_n}\}$
    $p^j_t \leftarrow max\{B^{I_1}_s, B^{I_2}_s \ldots, B^{I_k}_s\}$
  end for
end for
for $(i \leftarrow 1 \text{ to } n)$ **do**
  $NormPool \leftarrow m_t + \log(1 + \Delta t)^{-1}$
end for
for $(j \leftarrow 1 \text{ to } k)$ **do**
  $WPool \leftarrow \sigma(\sum_{f=0}^{k-1} w_i x_t + U_t h_{t-1})$
  $A_t \leftarrow \frac{1}{m_t}$ (WPool$+b_i$)
  if $(m_t == 1)$ **then**
    $A_t > 0$
  else
    $A_t < 0$
  end if
end for
while $(z>0)$ **do**
  if $(P > A_t)$ **then**
    $\Delta_{t-1:t} \leftarrow |\log(e + \delta_{t-1:t})^{-1}|$
    $\aleph_i \leftarrow \sigma(w_f x_t + u_f h_{t-1} + Q_f q_{\Delta t-1:t} + p_f p_{t-1} + b_f)$
    $SoftMax(z) \leftarrow e^z / \sum_{z t} e^{Z t}$
    $P(d_{t+1} = c|f_t) \leftarrow SoftMax(z)$
    $MeanPool \leftarrow h_{1,2,\ldots,n}$
  else
    $MeanPool \leftarrow -\log P(y|u_{1,2,\ldots,n})$
  end if
end while
$e_h \leftarrow \sigma(h_t + b_h)$
$x_y \leftarrow h_t a_n + b_y$
$P(y|h_{1,2,\ldots,n}) \leftarrow f_{prob}(x_y)$

Evaluation Results



((a)) Improved accuracy in the *LSTM_DaaS* model



((b)) End-to-end latency over traditional schemes in *BinDaaS*

Evaluation Results

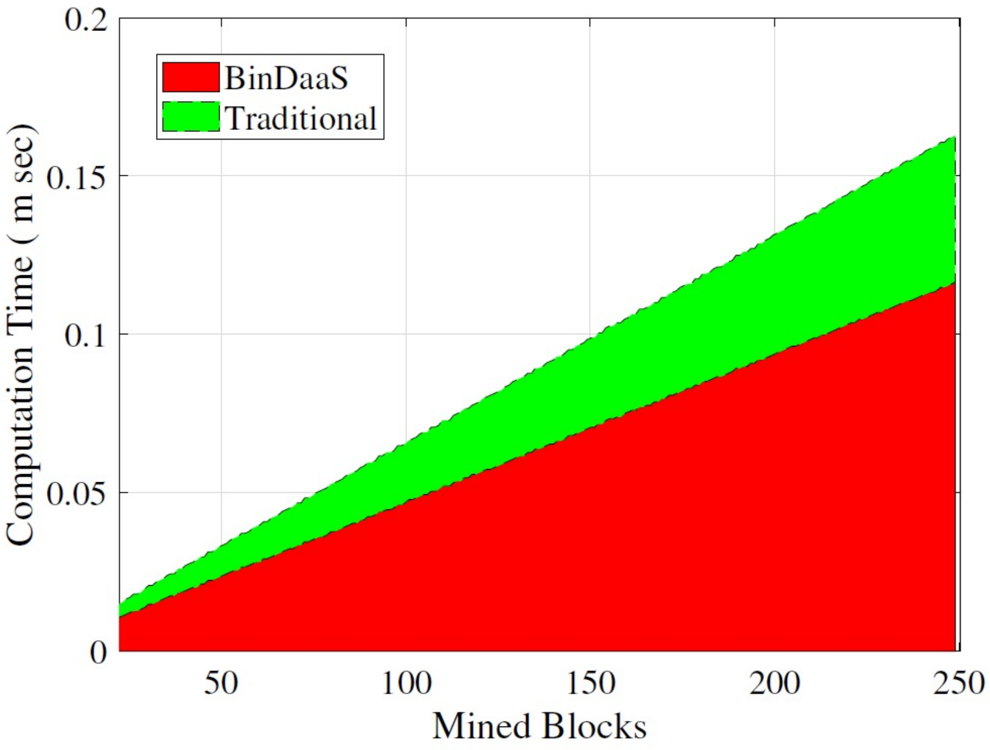


TABLE IV: Comparative Analysis with existing schemes

Parameters	**Bao** *et al.* [48]	**Li** *et al.*[49]	**Hathaliya** *et al.*[46]	**Aujla** *et al.* [47]	**Proposed** *BinDaaS*
A1	✓	✕	✓	✓	✓
A2	✕	✕	✓	✓	✓
A3	✕	✕	✓	✓	✓
A4	✕	✕	✓	✓	✓
A5	✕	✕	✕	✕	✓
A6	-	✓	✓	✕	✓
A7	✕	✕	✕	✕	✓
A8	✕	-	✕	✓	✓
A9	✕	✕	✕	✓	✓
A10	-	✕	✓	✓	✓

A1: Replay Attacks; A2: Side-Channel Attacks; A3:Distributed Denial-of-Service(DDoS) attacks; A4: Session-based attacks A5: Provenance and auditability attacks; A6: Tracebility of attacks; A7: Signature-forgery attacks; A8: Signature verificability; A9; Quantum attacks; A10: Known ciphertext attack; ✓ shows scheme is safe; ✕ shows scheme is not safe; & - shows attack is not considered in the scheme.

Q & A