INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

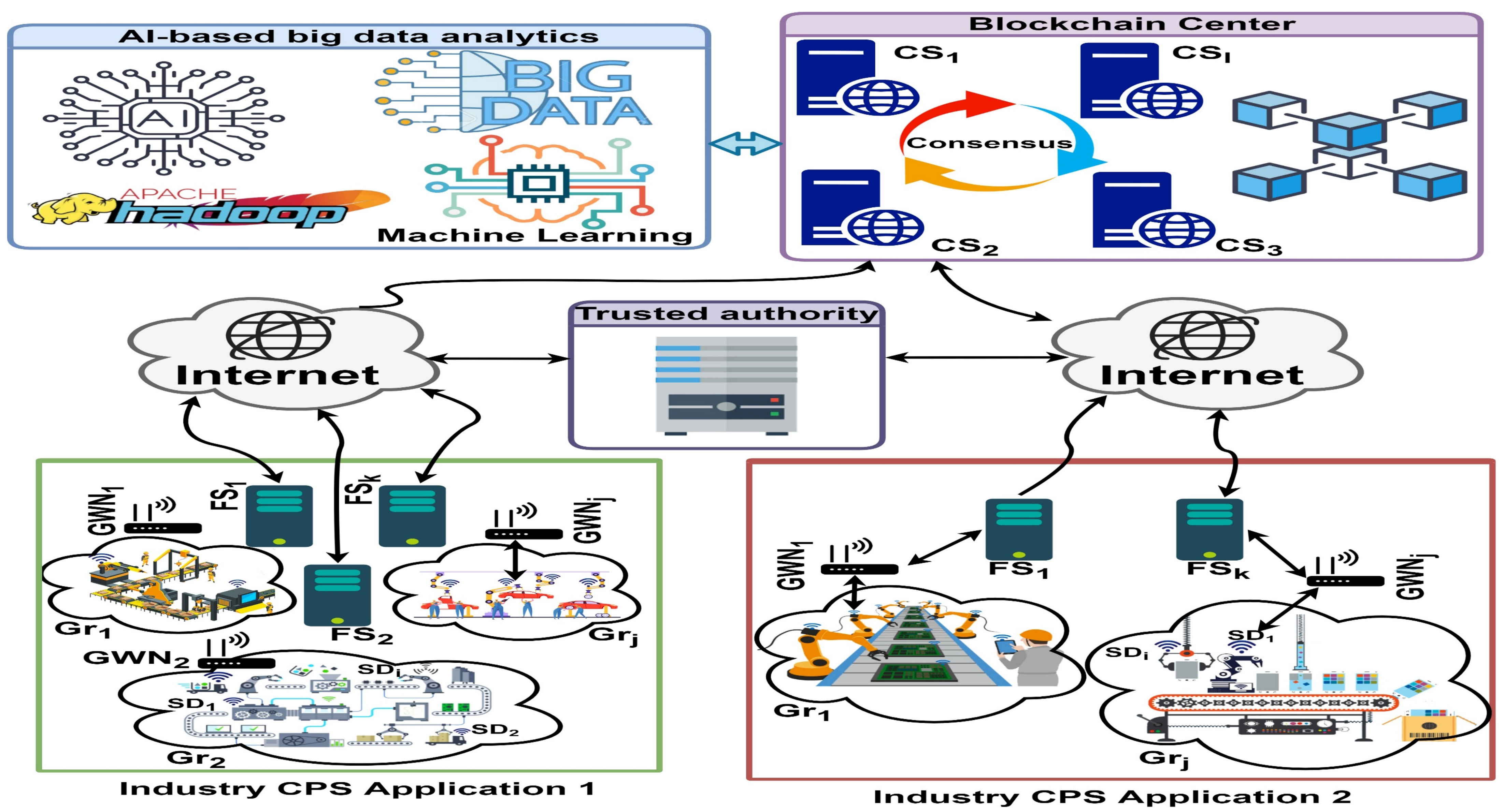
R&D SHOWCASE 2021

BLOCKCHAIN-BASED BATCH AUTHENTICATION PROTOCOL FOR INTERNET OF VEHICLES

ABSTRACT

The vehicles in Internet of Vehicles (IoV) can be used to gather and distribute data in a smart city environment. However, at the same time various security threats arise due to insecure communication among entities in an IoV-based smart city deployment. To address this issue, we aimed to design a novel blockchain-enabled batch authentication scheme in Artificial Intelligence (AI)- envisioned IoV-based smart city deployment. Incorporation of **AI/ML in blockchaining** produces a secure, efficient and intelligent blockchain based system. The proposed authentication scheme implements two types of authentications: **Vehicle to vehicle (V2V) authentication**- that allows a vehicle to authenticate its neighbor vehicles in its cluster; and **batch authentication**- that allows a group of vehicles to be authenticated by RSU simultaneously. Finally, a group key is established between a group of vehicles and RSU for future secure communication. RSU gathers secure data from its vehicles and form several transactions. Nearby fog servers associated with RSU and cloud server form a complete block. The created blocks are mined by the cloud servers in a Peer-to-Peer (P2P) cloud server network through the voting-based Practical Byzantine Fault Tolerance (PBFT) consensus algorithm (Algorithm 1). The authentic and genuine data of the blockchain are utilized for Big data analytics through AI/ML algorithms.

Network Model



Signing & Authentication Phases

Signing Phase

Vehicle (V_j)	Road-side Unit (RSU_i)/Vehicle (V_l)
Select random $rn_{V_j}, a_{V_j}, b_{V_j} \in Z_q^*$ and current timestamp value TS_{V_j}. Compute $Sig_{V_{j1}} = a_{V_j} \cdot (RID_{V_j} + Pub_{V_j})$, $Sig_{V_{j2}} = b_{V_j} \cdot (pr_{V_j} \cdot G)$, $h_{2j} = H_2(ma_j \| Sig_{V_{j1}})$, $h_{3j} = H_3(ma_j \| Sig_{V_{j1}} \| Sig_{V_{j2}})$, $Prox_{V_j} = H_4(X_k)$, Generate signature as $Sig_{V_j} = (a_{V_j} + h_{2j})(pp_{V_{j0}} + pp_{V_{j1}}) + (b_{V_j} + h_{3j})\, pr_{V_j} \cdot Prox_{V_j}$. $Hello_{Msg_{V_j}} = \{ma_j, Sig_{V_{j1}}, Sig_{V_{j2}}, Sig_{V_j}\}$ ⟶ (via public channel)	

V2V Authentication Phase

Vehicle (V_j)	Vehicle (V_l)
	Receive message $Hello_{Msg_{V_j}} = \{ma_j, Sig_{V_{j1}}, Sig_{V_{j2}}, Sig_{V_j}\}$. Check if $\lvert TS^*_{V_j} - TS_{V_j}\rvert \le \Delta T$? If valid, verify if $Cert_{V_j} \cdot G = Pub_{TA_k} + h(RID_{V_j} \| Pub_{V_j} \| R_{V_j}) \cdot R_{V_j}$? If legitimate, compute $h_{2j} = H_2(ma_j \| Sig_{V_{j1}})$, $h_{3j} = H_3(ma_j \| Sig_{V_{j1}} \| Sig_{V_{j2}})$, $Prox_{V_j} = H_4(X_k)$. Verify if $e(G, Sig_{V_j}) = e(Pub_{TA_k}, Sig_{V_{j1}} + h_2(RID_{V_j} + Pub_{V_j}))\cdot$ $e(Prox_{V_j}, Sig_{V_j2} + h_3 \cdot PB_{V_j})$? If it is valid, V2V authentication is successful.

Batch Authentication Phase

Vehicles $V_1, V_2, \cdots, V_n$	Road-side Unit (RSU_i)
	Check if $\lvert TS^*_{V_j} - TS_{V_j}\rvert \le \Delta T$? for all vehicles $V_1, V_2, \cdots, V_n$. If valid, select random $w_1, w_2, \cdots, w_n \in Z_q^*$. Compute $h_{2j} = H_2(ma_j \| Sig_{V_{j1}})$, $h_{3j} = H_3(ma_j \| Sig_{V_{j1}} \| Sig_{V_{j2}})$, $Prox_{V_j} = H_4(X_k)$, for all $j = 1, 2, \cdots, n$. Verify if $e(G, \sum_{j=1}^{n} wj\, Sig_{V_j}) = e(Pub_{TA_k}, \sum_{j=1}^{n} wj\, Sig_{V_{j1}}$ $+ wj\, h_{2j}(RID_{V_j} + Pub_{V_j}))\cdot e(Prox_{V_j}, \sum_{j=1}^{n} wj\, Sig_{V_{j2}} + wj \cdot h_{3j} \cdot PB_{V_j})$? If it is valid, batch authentication is successful, and all the vehicles $V_1, V_2, \cdots, V_n$ in the cluster are authenticated by (RSU_i).

Blockchain Consensus Algorithm

Algorithm 1 Consensus for block verification and addition in blockchain

Input: A full block, $FullBlock = \{BVer, PBHash, TS_{Block}, MTR_{Block}, PB_{RSU_i}, \{Tx_l \mid l = 1, 2, \cdots, n_t\}, Sig_{Block}, CBHash\}$; private–public key pairs $(pr_{CS_w}, Pub_{CS_w} = pr_{CS_w} \cdot G)$ of all other cloud servers CS_w in the P2P CS network; $n_{f_{CS}}$: number of faulty cloud servers (nodes) in the P2P CS network.
Output: Commitment for block addition.

```
L_CS generates a random number rn_{L_CS} ∈ Z_q^*, a current timestamp TS_{L_CS}
  and a voting request VReq_{L_CS}.
for each peer cloud server node CS_w do
    L_CS encrypts rn_{L_CS}, TS_{L_CS} and VReq_{L_CS} using the ECC-based encryption
    algorithm with the help of the public key Pub_{CS_w} of CS_w as EncVreq =
    EP_{Pub_{CS_w}}[rn_{L_CS}, TS_{L_CS}, VReq_{L_CS}] and sends a block verification request
    message {FullBlock, EncVreq, TS_{L_CS}} to CS_w via open channel.
end for
for each follower node CS_w in the P2P CS network do
    Let the message {FullBlock, EncVreq, TS_{L_CS}} be received at time TS*_{L_CS}
    by CS_w.
    CS_w checks validity of TS_{L_CS} by the condition: |TS*_{L_CS} − TS_{L_CS}| ≤ ΔT.
    if timestamp is valid then
        CS_w decrypts EncVreq using its own private key pr_{CS_w} to retrieve
        [rn'_{L_CS}, TS'_{L_CS}, VReq'_{L_CS}] = DP_{pr_{CS_w}}[EncVreq].
        if TS'_{L_CS} = TS_{L_CS} then
            CS_w verifies MTR_Block, Sig_Block and CBHash on the block
            FullBlock.
            if all the verifications by CS_w are successful then
                CS_w sends a voting response cum block verification sta-
                tus message {EP_{Pub_{L_CS}}[rn'_{L_CS}, VRep_{CS_w}, VerStat_{CS_w}]} to the
                leader L_CS, where VRep_{CS_w} and VerStat_{CS_w} are the voting
                response corresponding to VReq'_{L_CS} and block verification status,
                respectively.
            end if
        end if
    end if
end for
Initialize VCount = 0, where VCount represents the number of valid votes.
for each voting response cum block verification status message {EP_{Pub_{L_CS}}
  [rn'_{L_CS}, VRep_{CS_w}, VerStat_{CS_w}]} from the follower peer nodes CS_w do
    L_CS decrypts the message using its own private key pr_{L_CS} to re-
    trieve [rn*_{L_CS}, VRep_{CS_w}, VerStat_{CS_w}] = DP_{pr_{L_CS}}[EP_{Pub_{L_CS}}[rn'_{L_CS}, VRep_{CS_w},
    VerStat_{CS_w}]].
    if ((rn*_{L_CS} = rn_{L_CS}) and (VRep_{CS_w} = valid) and (VerStat_{CS_w} = valid))
    then
        Set VCount = VCount + 1.
    end if
end for
if (VCount ≥ 2 * n_{f_CS} + 1) then
    Add the block FullBlock to the blockchain.
    Broadcast commitment message to the P2P CS network.
end if
```

Group Key Management Phase

Group Key Management Phase

Vehicles (V_j)	Road-side Unit (RSU_i)
	Generate a $rn_{RSU_i}, sk \in Z_q^*$ timestamp value TS_{RSU_i}. Compute $RN_{RSU_i} = rn_{RSU_i}.G$. Generate group key $GK_k = h(RID_{V_1} \| RID_{V_2} \| \cdots \| RID_{V_n} \| rn_{V_1} \| rn_{V_2} \| \cdots \| rn_{V_n} \| Cert_{V_1} \| Cert_{V_2} \| \cdots \| Cert_{V_n} \| RID_{RSU_i} \| rn_{RSU_i} \| Cert_{RSU_i} \| pr_{RSU_i} \| sk)$, Encrypted group key $E_{PB_{V_j}}(GK_k \| rn_{V_j} \| TS_{RSU_i})$ Form message $mb_j = \{TS_{RSU_i}, Cert_{RSU_i}, Pub_{RSU_i}, PB_{RSU_i}, R_{RSU_i}, RN_{RSU_i}, Pub_{TA_k}, rn_{V_j}, E_{PB_{V_j}}(GK_k \| rn_{V_j} \| TS_{RSU_i})\}$, signature $Sig_{RSU_i,V_j} = pr_{RSU_i} + h(mb_j \| RN_{RSU_i} \| Cert_{V_j} \| RID_{V_j} \| TS_{V_j} \| TS_{RSU_i}) * rn_{RSU_i} \pmod q$. $Res_{RSU_i,V_j} = \{mb_j, Sig_{RSU_i,V_j}\}$ ⟵
Check if $\lvert TS^*_{RSU_i} - TS_{RSU_i}\rvert \le \Delta T$? If valid check $Cert_{RSU_i} \cdot G = Pub_{TA_k} + h(RID_{RSU_i} \| Pub_{RSU_i}) \cdot R_{RSU_i}$? Verify the signature by $Sig_{RSU_i,V_j} \cdot G = PB_{RSU_i} + h(mb_j \| RN_{RSU_i} \| Cert_{V_j} \| RID_{V_j} \| TS_{V_j} \| TS_{RSU_i}) \cdot RN_{RSU_i}$? If valid extract group key by $(GK_k \| rn'_{V_j} \| TS'_{RSU_i}) = D_{pr_{V_j}}[E_{PB_{V_j}}(GK_k \| rn_{V_j} \| TS_{RSU_i})]$ Check if $rn'_{V_j} = rn_{V_j}$ and $TS'_{RSU_i} = TS_{RSU_i}$? If both are valid, the group key GK_k is authentic.	

All vehicles $V_1, V_2, \cdots, V_n$ and RSU in their cluster share the group key GK_k

Results

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/palak/Desktop/span
  /testsuite/results/batch.if
GOAL
  As specified
BACKEND
  CL-AtSe

STATISTICS
  Analysed   : 844 states
  Reachable  : 64 states
  Translation: 0.35 seconds
  Computation: 0.01 seconds
```

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS

PROTOCOL
  /home/palak/Desktop/span
  /testsuite/results/batch.if

GOAL
  as specified
BACKEND
  OFMC

STATISTICS
  TIME 168 ms
  parseTime 0 ms
  visitedNodes: 16 nodes
  depth: 4 plies
```

Authors: Palak Bagga, Ashok Kumar Das, Anil Kumar Sutrala, and Pandi Vijayakumar. "Blockchain-based batch authentication protocol for Internet of Vehicles," in Journal of Systems Architecture (Elsevier), Vol. 113, pp. 1-23, Article No. 101877, 2021, DOI: 10.1016/j.sysarc.2020.101877. (2019 SCI Impact Factor: 2.552)

Research Center Name: Center for Security, Theory and Algorithmic Research