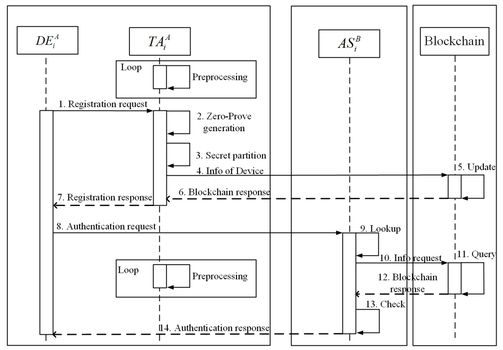
LBCZA: Lightweight Blockchain-assisted Cross-domain Zero-Knowledge Authentication for the Industrial Internet of Things (Some Information)

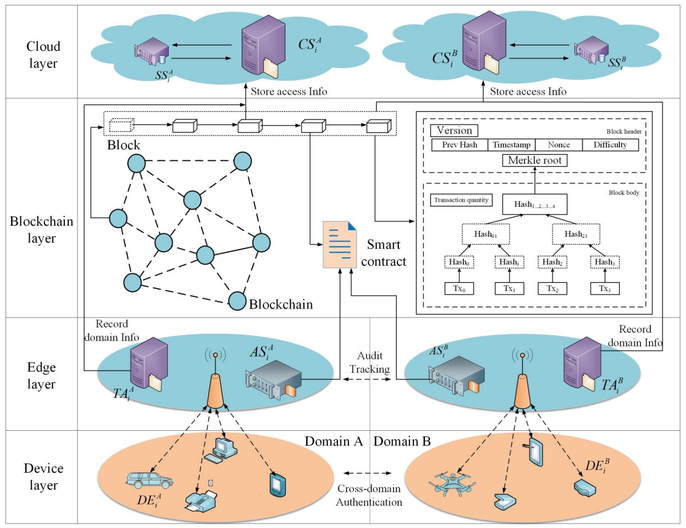
This manuscript presents original research that addresses key challenges in the Industrial Internet of Things (IIoT), particularly in secure and efficient cross-domain authentication. The proposed **Lightweight Blockchain-assisted Cross-domain Zero-Knowledge Authentication (LBCZA)** scheme provides a novel solution for ensuring privacy protection, security, and scalability in IIoT systems.

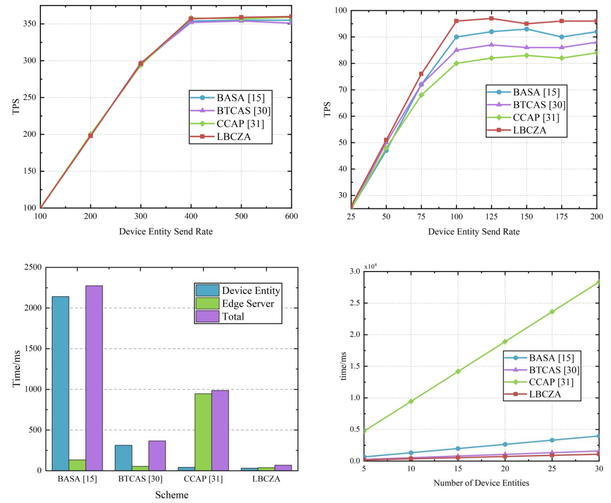
Key contributions of the paper include:

1. **A lightweight and flexible authentication framework** that supports secure cross-domain interactions in IIoT environments, while minimizing computational and communication overheads for resource-constrained devices.
2. **Integration of Pedersen and Fujisaki-Okamoto commitment protocols** to establish a zero-knowledge proof mechanism, ensuring anonymous cross-domain access and protecting device privacy during authentication.
3. **A novel identity tracking protocol based on threshold variable secret sharing**, which not only identifies and tracks malicious devices but also introduces a dynamic threshold adjustment mechanism to prevent collusion attacks. This mechanism ensures that a small number of compromised entities cannot manipulate secret sharing to reveal the identities of legitimate devices, thus enhancing system security against collusion attempts.
4. **Extensive theoretical and experimental evaluations**, demonstrating that LBCZA offers better scalability and lower overhead compared to state-of-the-art methods, while maintaining strong security guarantees, including resistance to replay attacks and forward secrecy.

Currently under review for IEEE Internet of Things Journal







$$
\begin{aligned}
&D_1Q_1 + DP_1 - cE \\
&= (\eta_1 + cr_1)Q_1 + (\omega + cx)P_1 - c(xP_1 + r_1Q_1) \\
&= \eta_1 Q_1 + cr_1Q_1 + \omega P_1 + cxP_1 - cxP_1 - cr_1Q_1 \\
&= \eta_1 Q_1 + \omega P_1 \\
&= W_1.
\end{aligned}
$$

$$
\begin{aligned}
&D_1Q_1 + DP_1 - c(E + \Delta xP_1 + \Delta r_1Q_1) \\
&= (\omega + c(x + \Delta x))P_1 + (\eta_1 + c(r_1 + \Delta r_1))Q_1 \\
&\quad - c(xP_1 + r_1Q_1 + \Delta xP_1 + \Delta r_1Q_1) \\
&= \omega P_1 + (x + \Delta x)P_1 + \eta_1 Q_1 + c(r_1 + \Delta r_1)Q_1 \\
&\quad - cxP_1 - cr_1Q_1 - c\Delta xP_1 - c\Delta xQ_1 \\
&= \eta_1 Q_1 + \omega P_1 \\
&= W_1.
\end{aligned}
$$

$$
\begin{aligned}
c' = H((&\eta_1' + c'r_1)Q_1 + (\omega' + c'x)P_1 \\
&- c'(xP_1 + r_1Q_1)\|(\eta_2' + c'r_2)Q_2 + (\omega' + c'x)P_2 \\
&- c'(xP_2 + r_2Q_2)\|H(r'||H_{root}))
\end{aligned}
$$

TABLE II
COMPARISON OF DIFFERENT SECURITY SCHEMES

Scheme	Cross-Domain	Decentralized Trust	Anonymity	Traceability	Interoperability	Anti-collusion	High Scalability
IRBA [28]	✓	✓	×	×	×	×	×
XAuth [27]	✓	✓	✓	×	×	×	×
BASA [15]	✓	✓	✓	×	×	×	✓
BTCAS [30]	✓	✓	×	×	✓	×	✓
CCAP [31]	✓	✓	✓	✓	✓	×	×
LBCZA	✓	✓	✓	✓	✓	✓	✓