

S1 Table Comparative analysis of eminent AKE schemes

AKE scheme	Shortcoming	Year	Operations
Qui and Ma [21]	Unsafe against sinkhole and chosen plaintext attacks	2016	XOR, ECC, and SHA-160
Challa <i>et al.</i> [22]	Prone to replay, DoS, forgery and UI attacks	2017	ECC, XOR, and SHA-160
Vijayakumar <i>et al.</i> [23]	Cannot resist replay attack and does not provide strong privacy	2017	XOR, AES, and SHA-160
Jung <i>et al.</i> [24]	Cannot resist against UI and ESL attacks	2017	XOR and SHA-160
Qi <i>et al.</i> [25]	Fragile to PC, PI, UI, UA and offline PG attacks and also does not provide MA	2017	XOR and SHA-160
Chaudhry <i>et al.</i> [26]	Vulnerable to offline PG, SSC, UI, and UA attacks	2018	XOR and SHA-160
Chen <i>et al.</i> [27]	Does not render MA and anonymity features. Prone to replay, SSD, PI, PG, UI, and DoS attacks	2018	XOR, ECC, and SHA-160
Amin <i>et al.</i> [28]	Cannot resist PI, UI, PG, and IG attacks	2018	XOR and SHA-160
Das <i>et al.</i> [29]	Does not render the SK's security. Fragile to SSD and traceability attacks	2018	XOR and SHA-160
Das <i>et al.</i> [30]	Susceptible to device impersonation and MITM attacks	2018	XOR, ECC, and SHA-160
Shin <i>et al.</i> [31]	Unprotected against de-synchronization attack and suffers a design flaw	2019	XOR and SHA-256
Lu <i>et al.</i> [32]	Prone to UI and SCC and does not provide a login phase	2019	XOR, ECC, and SHA-160
Srinivas <i>et al.</i> [33]	Does not scale well. Susceptible to traceability, UI, and DI attacks	2019	XOR and SHA-160
Mishra <i>et al.</i> [34]	Prone to SSD, stolen verifier, UI, and UA attacks and unable to ensure SN's anonymity	2018	XOR, AES, and SHA-160
Wazid <i>et al.</i> [35]	Prone to UI, IG, and DI attacks	2018	XOR and SHA-160
Shuai <i>et al.</i> [36]	Prone to parallel session, UI, PG, PI, and SSD attacks	2019	XOR, ECC, and SHA-160
Shin <i>et al.</i> [31]	Suffers a design flaw and prone to de-synchronization	2019	XOR and SHA-160
Barman <i>et al.</i> [37]	Fragile to SI, UI, ESL, SK leakage, and UA attacks	2019	XOR and SHA-160
Singh <i>et al.</i> [38]	Susceptible to UA, MITM, UI, SI, and modification attacks, and does not render untraceability, MA, and SK agreement features	2019	XOR and SHA-160
Sadhukhan <i>et al.</i> [39]	does not provide password change mechanism. Vulnerable to replay, UA, DoS, and MITM attacks	2021	XOR, ECC, and SHA-160
Ali <i>et al.</i> [40]	Unprotected against DoS, forgery, PI, SSD, and SI attacks, and does not render PFS and key freshness features	2020	XOR, AES, and SHA-16
Vinoth <i>et al.</i> [34]	Unable to restrain SSD, DoS, replay, and SN capture attacks	2020	XOR, AES, and SHA-160
Tanveer <i>et al.</i> [41]	Cannot resist de-synchronization attack	2020	XOR, ASCON, and SHA-256
The proposed scheme (SRUA-IoT)	Can withstand all known attacks. However, the computational cost can be reduced further	2021	XOR, AES-192, and SHA-160

MA: Mutual authentication, PC: Password change, PG: Password guessing, PI: Privileged insider.