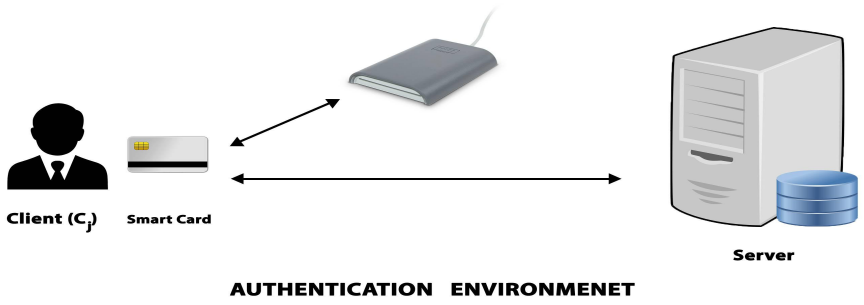
An enhanced authentication protocol for client server enviornment

Muhammad Asad SALEEM, Shafiq AHMED, Khalid MAHMOOD, Saru KUMARI, Hu XIONG

Frontiers of Computer Science, DOI: 10.1007/s11704-019-9186-x

Problems & Ideas

- Limbasiya et al.'s protocol is vulnerable to following attacks.
  - User Impersonation attack
  - Lack of authentication at server side
  - Meaningless authentication at user side
  - Failure of dynamic value updation
  - Failure of session key establishment
- Ideas: Design of secure authentication protocol
  - To mitigate flaws of Limbasiya et al.'s protocol
  - To provide secure communication between Client and Server



Main Contributions

1: Lower overhead in terms of computation, communication and storage

Table 3 Aggregated Computation , Communication and Storage cost

Protocol	Computation Cost	Communication Cost	Storage Cost
Proposed	$10T_{h(.)} + 2T_{enc/dec} + 8T_{\oplus} + 39T_{\|\|} = 0.0044$ ms	3808 bits	1280 bits
[2]	$21T_{h(.)} + 10T_{\oplus} + 1T_{ME} = 0.585$ ms	4064 bits	1760 bits
[3]	$16T_{h(.)} + 11T_{\oplus} = 0.0480$ ms	2880 bits	1152 bits
[4]	$1T_{h(.)} = 0.0030$ ms	3264 bits	960 bits
[5]	$11T_{h(.)} + 2T_{\oplus} + 7T_{enc/dec} + 33T_{\|\|} = 0.0750$ ms	3040 bits	1600 bits
[6]	$17T_{h(.)} + 10T_{\oplus} + 24T_{\|\|} = 0.510$ ms	2080 bits	736 bits

2: Aided Security features

Table 2 Security Features: Comparative Summary

Scheme→ Security Features↓	Proposed	[2]	[3]	[4]	[5]	[6]
Smart card lost Attack Resilience	✓	✓	N/A	✗	✓	✓
Password guessing Attack Resilience	✓	✓	N/A	✗	✗	✗
Stolen Verifier Attack Resilience	✓	✓	✗	✗	✗	✓
Session key Disclosure Attack Resilience	✓	✓	✗	N/A	✓	✗
Insider Attack Resilience	✓	✓	✗	✗	✗	✗
Modification Attack Resilience	✓	✓	✗	✗	✗	✓
User Impersonation Attack Resilience	✓	✓	✓	✓	✓	✓
Leak of Verifier Attack Resilience	✓	✓	✓	✓	✓	✓