Abstract

In this era of big data, an unprecedented amount of data is being produced, collected and stored at an alarming rate. Apart from other issues, privacy and cyber-security have become serious as an overwhelming amount of data is collected about users both knowingly and unknowingly. The design of secure remote user authentication and key agreement schemes for big data applications is still open and challenging. Therefore, this paper proposes a robust smart card based mutual authentication and key agreement scheme for big data environment which not only resolves the security weaknesses of schemes proposed till date but also extends the scheme to provide user anonymity which is one of the most desired features of big data systems. Furthermore, the proposed scheme requires lower computation cost and provides
more security and functionality features than the existing schemes. The proposed scheme thus provides more efficiency and security from any type of system intrusion.

References

- Wang, R. C., Juang, W. S., Lei, C. L., Robust authentication and key agreement scheme preserving the privacy of secret key, Computer Communications 34 (3) 274–280 (2011).
- C. T. Li, A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card, IET Information Security 7 (1) 3-10 (2012).
- Toan-Thinh Truong, Tran, M. -T, Anh-Duc Duong, Improvement of more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on ECC, 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA) 698-703 (2012).
- Kalra S, Sood SK. Secure authentication scheme for IoT and cloud servers. Pervasive

**Index Terms**

Computer Science  
Information Science

**Keywords**

Big Data  Elliptic Curve Cryptography  Remote User Authentication  Session Key  
Smart Card  
User Anonymity