Two Factors Authentication Login Examination based on The User's Fuzzy Predefined Knowledge (2FA-FDK).

- **Author(s):** Amnat Sawatnatee

- **Abstract:** The objective of this research is to presents the practical protocol of user authentication login examination. The research uses two techniques such as one-time password, and share knowledge. This protocol is designed to use in general server login activity. The protocol specifies the requester to perform two of their authentications verifying activities. The first, the one-time password (OTP), is the first mandatory activity to present their secure authenticate identity. Second, the requester has to provide their secret between requesters and servers' shared knowledge to the target server. The protocol is comprised of two stages. The first stage is shared secret preparing; the sharing secrets are password (key) and users' answers. In the second stage, the requester has to present all the sharing secrets to log in to the server. The sharing secret between requesters and servers' shared knowledge is the server-defined questions which requester has to inform their answers. The requester may give inconsistent answers; therefore, fuzzy logic is applied to obtain the. The crisp answering value is considered its lower and upper boundary. The server defines this confidence interval of crisp value to think whether the requester should be the authenticate one or not. The 2FA-FDK can prevent man in the middle attack (MITM), and password brute force attack. The suggested two-factor authentication protocol is easy to implement and rigorous an authentication examining.

- **Keywords:** MITM, practical protocol, share knowledge, confidence interval