ABSTRACT

In the contemporary world, Internet based services undoubtedly plays a vital role in supporting business processes. Yet, these services suffer from poor authentication methods, leading to intensive attacks. To address this issue and to enhance the security, in this research, various forms of foolproof two-server Password Authenticated Key Exchange (PAKE) protocols are devised, analyzed and implemented using geometrical shape based properties - circumcenter (ω) and the angle between the medians (θ) of the triangle (2D) and tetrahedron (3D). PAKE is an interactive method to establish secret session key based on the involved party's knowledge of a password. PAKE designed under the single server model is commonly prone to vulnerable attacks, whereas, the multi-server model is quite expensive in terms of communication and computation. Hence, two-server PAKE model is preferred for deployment and an extensive literature survey is carried out to show the importance of two-server PAKE protocols. With the aid of these properties, obtaining a password/key from the ciphertext is infeasible. The metrics considered in the research work for examining the protocols include communication complexity, computational complexity, security defensive rate and attack resistance rate.

The significant contributions of the research work include devising and analyzing 2D Diffie-Hellman (DH) based two-server PAKE protocol, 3D DH based two-server PAKE protocol, 3D ElGamal DH two-server PAKE protocol and finally 3D Elliptic Curve Cryptography (ECC) DH two-server PAKE protocol. 2D DH based two-server PAKE protocol uses circumcenter (ω) and the angle between the medians (θ) of the triangle as its base property to avert all possible offline dictionary attacks and

impersonation attacks caused by an inside/outside adversary. Similarly, 3D DH based two-server PAKE protocol uses the properties of the tetrahedron to augment security in three dimension. 3D ElGamal DH based two-server PAKE protocol is developed with the notion to balance the load among the servers and to provide an additional layer of security by encrypting the password based variants. Finally, 3D ECC DH two-server PAKE protocol is framed to increase the speed and is tested for a health care application to prove its rigidity against attacks. 3D ECC DH based two-server based PAKE protocol is ideal for environments that need high security with less key length. Security is addressed by utilizing the hard-core properties to protect the password, when the servers are subjected to attacks. As circumcenter (ω) and the angle between the medians (θ) are derived from geometrical shapes, strong authentication is guaranteed.

A substantial security analysis of 2D and 3D two-server PAKE protocols is provided including proof of correctness. The performance of the proposed protocols is reliable and comparatively fair in terms of communication and computation. Security defensive rate and attack resistance rate shows drastic improvement when compared to the existing schemes. 3D ECC DH based two-server based PAKE protocol yields a higher security defensive rate and attack resistance rate followed by 3D ElGamal DH based two-server PAKE protocol, 3D DH based two-server PAKE protocol and 2D DH based two-server PAKE protocol. This assures the robustness of the proposed protocols against attacks and compliance with key security principles. The two-server based 2D and 3D PAKE models can be incorporated in Secure Sockets Layer (SSL) protocol to secure the data transmission between applications across the network by providing sufficient mutual authentication.