**LITERATURE SURVEY**

**1) Password authentication with insecure communication**

**AUTHORS:**  L. Lamport

A method of user password authentication is described which is secure even if an intruder can read the system's data, and can tamper with or eavesdrop on the communication between the user and the system. The method assumes a secure one-way encryption function and can be implemented with a microcomputer in the user's terminal.

**2) A generic framework for three-factor authentication: Preserving security and privacy in distributed systems**

**AUTHORS:** X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng

As part of the security within distributed systems, various services and resources need protection from unauthorized use. Remote authentication is the most commonly used method to determine the identity of a remote client. This paper investigates a systematic approach for authenticating clients by three factors, namely password, smart card, and biometrics. A generic and secure framework is proposed to upgrade two-factor authentication to three-factor authentication. The conversion not only significantly improves the information assurance at low cost but also protects client privacy in distributed systems. In addition, our framework retains several practice-friendly properties of the underlying two-factor authentication, which we believe is of independent interest.

**3) Robust multifactor authentication for fragile communications**

**AUTHORS:** X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu,

In large-scale systems, user authentication usually needs the assistance from a remote central authentication server via networks. The authentication service however could be slow or unavailable due to natural disasters or various cyber attacks on communication channels. This has raised serious concerns in systems which need robust authentication in emergency situations. The contribution of this paper is two-fold. In a slow connection situation, we present a secure generic multi-factor authentication protocol to speed up the whole authentication process. Compared with another generic protocol in the literature, the new proposal provides the same function with significant improvements in computation and communication. Another authentication mechanism, which we name stand-alone authentication, can authenticate users when the connection to the central server is down. We investigate several issues in stand-alone authentication and show how to add it on multi-factor authentication protocols in an efficient and generic way.

**4) Anonymous authentication for wireless body area networks with provable security**

**AUTHORS:** D. He, S. Zeadally, N. Kumar, and J. Lee

Advances in wireless communications, embedded systems, and integrated circuit technologies have enabled the wireless body area network (WBAN) to become a promising networking paradigm. Over the last decade, as an important part of the Internet of Things, we have witnessed WBANs playing an increasing role in modern medical systems because of its capabilities to collect real-time biomedical data through intelligent medical sensors in or around the patients' body and send the collected data to remote medical personnel for clinical diagnostics. WBANs not only bring us conveniences but also bring along the challenge of keeping data's confidentiality and preserving patients' privacy. In the past few years, several anonymous authentication (AA) schemes for WBANs were proposed to enhance security by protecting patients' identities and by encrypting medical data. However, many of these schemes are not secure enough. First, we review the most recent AA scheme for WBANs and point out that it is not secure for medical applications by proposing an impersonation attack. After that, we propose a new AA scheme for WBANs and prove that it is provably secure. Our detailed analysis results demonstrate that our proposed AA scheme not only overcomes the security weaknesses in previous schemes but also has the same computation costs at a client side.

**5) A remote password authentication scheme for multiserver architecture using neural networks**

**AUTHORS:** L. Li, L. Lin, and M. Hwang

Conventional remote password authentication schemes allow a serviceable server to authenticate the legitimacy of a remote login user. However, these schemes are not used for multiserver architecture environments. We present a remote password authentication scheme for multiserver environments. The password authentication system is a pattern classification system based on an artificial neural network. In this scheme, the users only remember user identity and password numbers to log in to various servers. Users can freely choose their password. Furthermore, the system is not required to maintain a verification table and can withstand the replay attack.