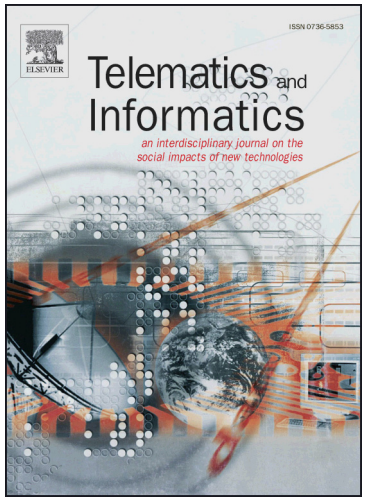
Accepted Manuscript



Authentication Systems: A Literature Review and Classification

Mohammadreza Hazhirpasand Barkadehi, Mehrbaksh Nilashi, Othman Ibrahim, Ali Zakeri Fardi, Sarminah Samad

PII: S0736-5853(18)30140-0
DOI: https://doi.org/10.1016/j.tele.2018.03.018
Reference: TELE 1100

To appear in: *Telematics and Informatics*

Received Date: 3 February 2018
Revised Date: 24 March 2018
Accepted Date: 29 March 2018

Please cite this article as: Barkadehi, M.H., Nilashi, M., Ibrahim, O., Zakeri Fardi, A., Samad, S., Authentication Systems: A Literature Review and Classification, *Telematics and Informatics* (2018), doi: https://doi.org/10.1016/j.tele.2018.03.018

Authentication Systems: A Literature Review and Classification

Mohammadreza Hazhirpasand Barkadehi [1], Mehrbaksh Nilashi [1,*], Othman Ibrahim [1], Ali Zakeri Fardi [2], Sarminah Samad [3]

[1] Faculty of Computing, Universiti Technologi Malaysia, Johor, Malaysia
[2] Department of Computer Engineering, Faculty of Engineering, University of Guilan, Rasht
[3] Department of Business and Administration, Collage of Business Administration, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia
[*] Corresponding Author E-mail Address: nilashidotnet@hotmail.com

Authentication Systems: A Literature Review and Classification

Abstract. One of the most important parts of any system is authentication. Appreciated as the first and the last line of defense in the great majority of cases, authentication systems can usually prevent the kleptomaniac from unauthorized accessing to users' data. However, the traditional text-based password is still used in many websites and applications which are vulnerable to different kinds of attacks. Accordingly, there exist some other alternative ways to boost this traditional method. In this study, we classified and identified different types of authentication systems in a variety of platforms. Their usage, similarity, usability, performance and drawbacks were discussed. The goal of this study is to provide useful, classified information with the aim of understanding of how different authentication systems work and of what their usability and drawbacks are to the readers.

Keyword: Two-factor authentication, Two-way verification, Login systems, Security, Two phases

1. Introduction

Despite the growing number of innovative ways to authenticate users, password-based authentication is still one of the most popular methods of all (Shen, Yu, Xu, Yang, & Guan, 2016). Passwords can easily be memorized and users at no cost are able to use them in their daily life (Shen et al., 2016). On the other side, passwords can be forgotten because of mixture of different passwords of various accounts (Nicholson, Coventry, & Briggs, 2013). As time passes, different methods of authentication have gradually been introduced in the forms of biological and graphical passwords. The new emerging trends of authentication systems are a combination of two or more methods. These systems employ the combination to distinguish true users from so-called users. There are three main schemes into which authentication systems fall (Almuairfi, Veeraraghavan, & Chilamkurti, 2013), namely *what you know*, *what you have*, and *what you are*.

As the researchers discuss the three mentioned categories, they will also analyze different kinds of each pertinent model. To clarify more, the username and password that are regularly used on websites are in the first group of authentication model whereas the credit card is counted as the ownership factor to check the validity during an authentication process. The last model includes biometric features with the capability of proving who the system users are. Some common samples of each model are presented in Table 1.

Table 1
Summaries of sample types of authentication based on their categories.

Ownership model	Knowledge-based model	Inherent-based model	Mix models