Wide-ranging Survey on Authentication Mechanisms

R. Thandeeswaran
School of Information Technology and Engineering, VIT University, Vellore-632 014, Tamil Nadu, India.
Corresponding author

Saleem Durai M A
School of Computing Science and Engineering, VIT University, Vellore-632 014, Tamil Nadu, India.

Abstract
More than storing a huge volume of data in Datacenters, protecting them from threats is a major concern in our heterogeneous networks. From local host to cloud, finding a space to store data was the issue in the earlier whereas retrieving by the right person is the issue in the later. But in both the scenarios, protecting the data from illegal use and unethical access is dispute. Access to a sensitive data like bank account details, medical records and defense data must be restricted. Mere access privileges cannot serve the purpose. Identify the user before allowing him/her to access the data. Authenticating the user and authorize him to access the data every time could control the illegitimate accesses. This paper analysed the wide-range of authentication mechanisms irrespective of the networks.

Keywords: Authentication; mobile networks; cloud computing; security threats; illegitimate access.

Introduction
Anonymous authentication is to hide the originality or identification. Identification is very vibrant in a cloud environment [1]. As the technology grows fraudulent users also grow in an exponential proportion. In the year 2015, passwords of Drop boxes have been hacked and the users lost their confidentiality. Google also lost his password and faced a huge profit loss. Hence, the technology has the responsibility to identify a procedure that could prevent the resources from illegitimate access.

Authentication is the procedure to identify the right personality to access the data [2]. There are many factors that influence to verify the identity of the originator. Authentication takes multiple faces, as shown in Figure 1, in the form of
- Password Authentication
- Biometric Authentication
- Multi-factor Authentication
- Phase Authentication
- Identity based authentication
- Recognizing and solving puzzle based authentication

In this paper, the different authentication factors and authentication schemes are discussed in detail. Rest of the paper is organized as section II presents identity based authentication, section III displays the biometric authentication, section IV presents the types of authentications and followed by a conclusion work in section III.

Identity based Authentication Schemes
There are multiple identities to legalize the end user’s identity. Among them, what you have, what you know and who are you are the most populous ones. Authenticity is the parameter that announces the eligibility of the user if they are not reproduced or fabricated [3]. Even with the valid credentials the data is vulnerable to
- Replay attack
- Repudiation
- IP spoofing
- M-I-M (Man-in-Middle) and
- Brute force attack
- Phishing attack
- DDoS attacks

The most preferred target of an intruder is through remote login where the attacker can use the back doors and trap doors to invade into the network and gain access to multiple resources as if he is the legitimate user. Hence, the corporate are in pressure to deploy additional security mechanisms to protect their resources not only form illegitimate user but also from legitimate credentials. Some of the more commonly deployed technologies include virtual private networking.
Virtual private networking takes advantage of encryption technologies to help minimize the exposure of allowing outside users to have access to the network.

Universally used authentication comes from the Hardware tokens, Software tokens
- **what you know** includes: Passwords, PINs, Passphrases
- **what you have** includes: Smart cards, Magnetic cards,
- **who are you** includes: Biometric components such as Fingerspints, Retina patterns, Hand geometry, Palm prints

Few Attribute Based Signature (ABS) methods features and their consequences are analysed and tabulated in Table 1.

**Table 1: Attribute Based Signature (ABS) Methods**

<table>
<thead>
<tr>
<th>Method</th>
<th>Feature</th>
<th>Effectiveness Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server-aided anonymous ABS [8]</td>
<td>Half signature generated by the system and the rest by the user</td>
<td>Computation cost of key generation is reduced.</td>
</tr>
<tr>
<td>Hidden ABS [14]</td>
<td>Signature Attributes based on the signer possess</td>
<td>More Secured</td>
</tr>
<tr>
<td>Identity based Cryptosystems [15]</td>
<td>What the user possesses</td>
<td>Reduces the complexity and the cost for establishing PKI</td>
</tr>
</tbody>
</table>

### Biometric based Authentication Schemes

Biometric based authentication schemes incorporate:
- Verifying the captured and stored fingerprint
- Verifying the captured and stored Palm print
- Verifying the captured and stored Hand geometry
- Verifying the captured and stored Facial recognition
- Verifying the captured and stored iris pattern

By fact, there are only three possible biometrics [4] could uniquely discriminate such as Fingerprints, Retina of the eye (blood vessel pattern) and Iris of the eye (random pattern of features found in the iris, including freckles, pits, striations, vasculature, coronas, and crypts)

Figure 2, depicts approximate recognition characteristics. Current technology advancement could change all the biometric pattern that could forge these characteristics. Also these features are dynamic due to normal and accidental growth and situations.

### Multi-Factor Authentication

Budding up technologies and services are not without internet connection. When the system is remotely connected to a global server, user loses his control over the data and the applications.

**Table 2: Multi-factor authentication and their downsides**

<table>
<thead>
<tr>
<th>Method</th>
<th>Working Principle</th>
<th>Downsides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-factor Authentication scheme for Cloud [21]</td>
<td>Based on dynamic secure multi-factor out-of-band secret-splitting mechanism</td>
<td>Works on the basic assumption that all the new registrants are truthful, which is unimaginable. Addresses only a kind of preliminary attacks such as brute-force and intent-based attacks.</td>
</tr>
<tr>
<td>Privacy preserving multi-factor authentication [22]</td>
<td>Based on the assumption that intruder knows the victim’s password and profile</td>
<td>Privacy alone focussed.</td>
</tr>
<tr>
<td>Multi-level Authentication [23]</td>
<td>Generate one password and concatenate at several locations.</td>
<td></td>
</tr>
</tbody>
</table>
Now the on-line shopping also dominates the e-transaction and e-governance which involves handling of money across the boundaries. A minor vulnerability can also lead to a major threat and heavy loss to both the ends, the customer and merchants. Hence, identifying the right user and validating the user at multiple levels could mitigate the level of attack and its consequences. List of existing methodologies and their downsides are quoted in Table 3.

Most of the on-line shopping is through apps in their mobile phones. During their travel time, in different travel mode, people are shopping the products and make payments. Hence, authentication over mobile networks also became a demanding concern. Existing handover authentication mechanisms and their sensitiveness are analysed and presented in table 4.

### Table 4: Hand-over authentication in Mobile networks

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Domain</th>
<th>Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Novel Pre-Authentication Scheme [17]</td>
<td>IEEE802.11 WLAN</td>
<td>Authentication Delay, Signalling cost</td>
</tr>
<tr>
<td>Usim based authentication tested for Handover [18]</td>
<td>UMTS-WLAN</td>
<td>Reduction in processing time</td>
</tr>
<tr>
<td>Fast and Secure Handover Authentication [19]</td>
<td>WiMAX and Wi-Fi Heterogeneous Networks</td>
<td>Fast and Security based on credential tickets</td>
</tr>
<tr>
<td>Uniform handover authentication [20]</td>
<td>e-UTRAN and non-3GPP access networks</td>
<td>Perfect Forward Secrecy, Master Key Forward Secrecy and user anonymity</td>
</tr>
</tbody>
</table>

### Recognizing and solving puzzle based authentication

Discriminating the man and machine is the major challenge in the internet world. Distinction can be achieved by proper authentication and user validation though multiple phases. Solving puzzles is one among the popular existing approach widely adopted by the end-users.

Reduced cost and exponential growth in the technology attracted even the lay man to purchase a smart phone with internet connectivity which ultimately increased the number of internet users. Impersonation and spoofing are unavoidable and non-traceable with this exploration. There are many malicious users which are using machine to crack the system, to avoid that harm many CAPTCHAs are using by the internet sites. CAPTCHA is the best way to find the whether the user is human or machine. Variants of CAPTCHA and their limitations are

1. **Text Based CAPTCHA:** The text image which are presented in front of user is sometimes not recognizable because of some issues like multiple fonts, blurred letters etc.

2. **Audio CAPTCHA:** Played audio has to be heard by the user and Phonetics and accent mismatch could occur.

3. **Puzzle Based CAPTCHA:** Solving a puzzle is not an easy task for a machine and at the same time it consumes processing time as well.

4. **Image Based CAPTCHA:** Low vision and blurred images create discrepancies which causes multiple trial sessions.

### Conclusion

Distributed computing, Grid computing, Ubiquitous computing, Cloud computing, sensor systems, RFID and the current Internet of Things (IoT) are all vulnerable to illegal access. Identifying the legitimate user and assigning proper access rights with authorization is a major challenge. Authentication could resolve portion of the issues but not complete eradication. This paper analysed the exiting authentication mechanisms in a heterogeneous network domain and presented their pitfalls too. Future objective is to propose a suitable authentication mechanism that could reduce the processing time and the cost incurred without compromising the quality of data delivery.

### References


