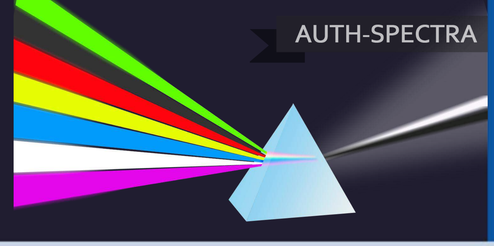
Adaptive Multifactor Authentication (A-MFA) System

Dipankar Dasgupta, Abhijit Kumar Nag, John Shrein, McKittrick Swindle, and Irfanur Rahman



Overall Concept

The Adaptive Multi-factor Authentication (A-MFA) framework identifies authorized users through an active authentication process using passwords, biometrics, cognitive behavior and other factors. This invention focuses on describing a framework where authentication factors are selected adaptively by sensing the users' operating environment (connected devices, communication media, and surrounding conditions) as well as previously selected authentication factors.

Applications:

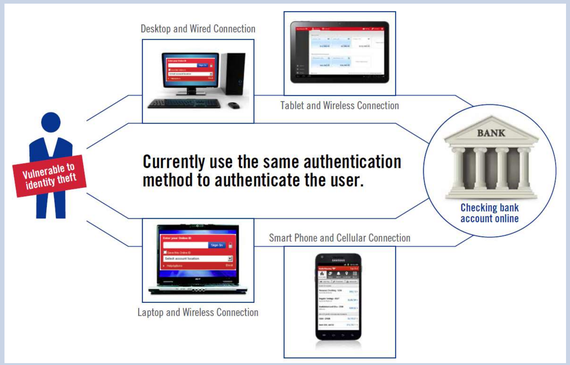
Continuous, **high-confidence**, identity authentication for:

- ✓ Banking, including online funds transfer
- ✓ Online testing in education and training settings
- ✓ Secure access to Electronic Medical Records

Deployable at different levels of Internet Computing:

- ✓ Application level (financial applications, email/business/personal applications, social applications)
- ✓ User level (root user, administrators, guest user)
- ✓ Document level (pdf containing application form, document containing proprietary information, image/video containing confidential and sensitive footage)

Sample Scenario

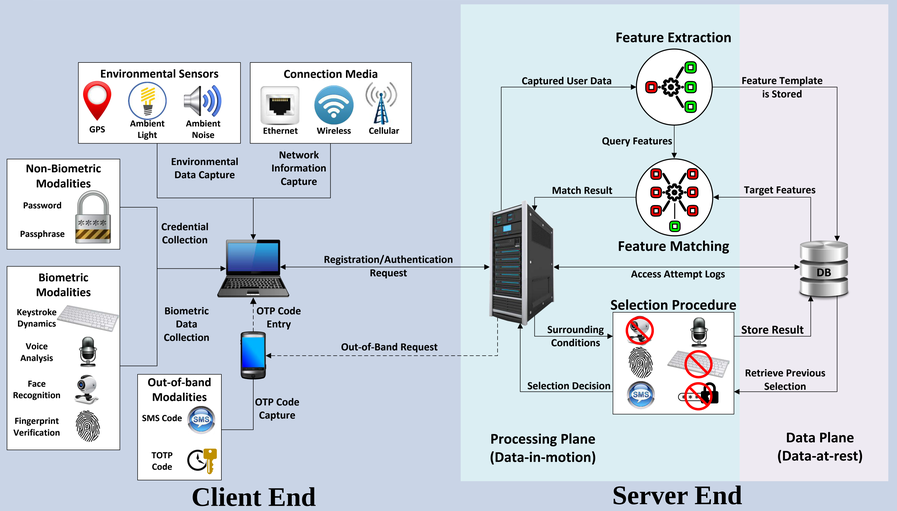


Advantages of Adaptive MFA System

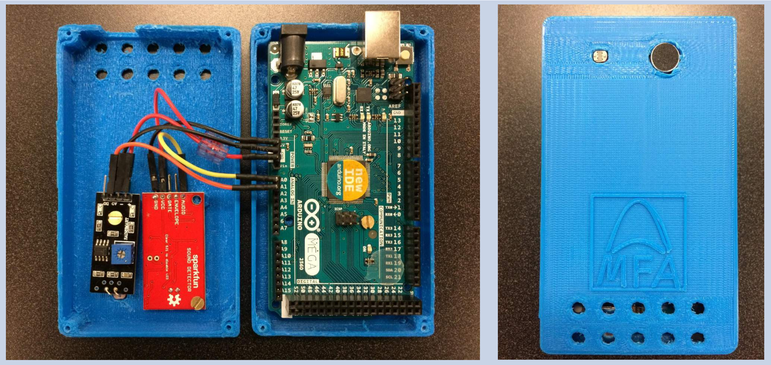
Major advantages of the implemented framework over other existing MFA technologies:

- ✓ Assures user identity during an interactive session and beyond the initial log-in.
- ✓ If an authentication modality is compromised, the system can adjust to authenticate users with the remaining non-compromised modalities.
- ✓ It ensures avoidance of repetitive selections to authenticate users if the operating conditions remain the same.
- ✓ Scalable: New authentication modalities can easily be integrated to augment the existing sets of modalities.
- ✓ Flexible: Allows for generation of the operating/configuration parameters for the added authentication modalities as they become available.
- ✓ Just-in-time selection algorithm chooses optimal authentication modalities for the user's operating environment.

Overall Architecture of Adaptive MFA



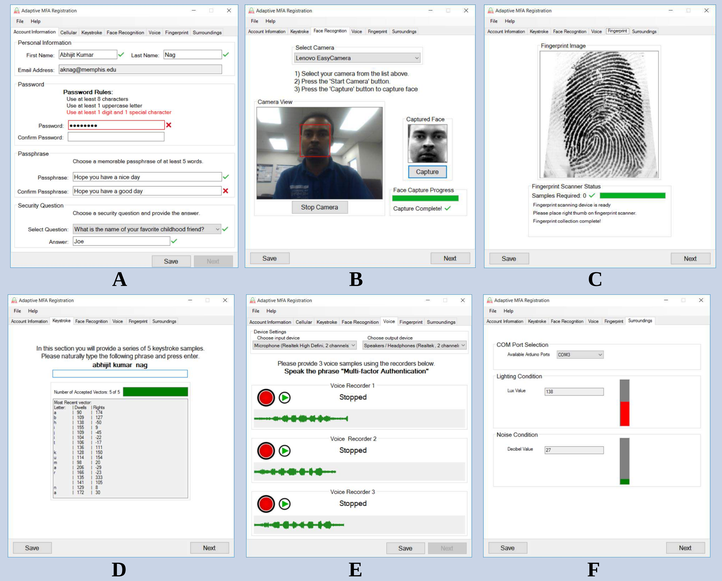
Customized Ambient Light and Noise Sensor Device



Comparison with Other Existing MFA Approaches

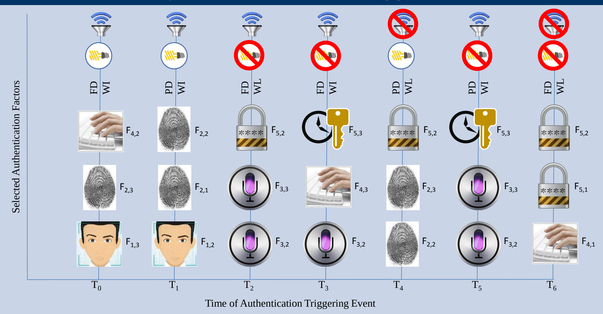
Product Name	Vendor	Factors	Features
SecureAuth IdP	SecureAuth	Two factors and SSO (out of 20)	Mobile, cloud, web or VPN
RSA SecureID	RSA	Two factors	Software (smartphones, tablets and PC) and Hardware authenticators
Safenet	SafeNet	Two factors	Cloud, Password + SMS/Hardware Token
SecurEnvoy	SecurEnvoy	Two Factor	Tokenless (One-swipe, SMS Preload, Soft Token, Voice Call, Email Preload)
Microsoft Azure MFA	Microsoft	Multi factor (Phone call, SMS and Password)	On premises and Cloud authentications Mobile Device + User-ID and Password
Deepnet DualShield	Deepnet Security	Two factors	SMS, Voice, Mobile App, Face, Keystroke, Smart Cards
Swivel Secure	Swivel Secure	SSO + two factor	Mobile App, SMS, Software/Hardware Tokens, Telephony
Duo Security	Duo Security	Two factor	Duo Push, Mobile Passcode, SMS, Phone callback, Hardware token
Adaptive MFA		Multi factor(Adaptively selected by sensing the environment conditions and considering the previous selection history)	Face, Fingerprint, Voice, Keystroke, Passwords, SMS, TOTP

User Registration and Authentication GUI



A. User Basic Information (Password, SMS); **B.** Face; **C.** Fingerprint;
D. Keystroke; **E.** Voice; **F.** Surrounding conditions (Light and Noise)

Sample Authentication Trigger Events



Implemented Adaptive MFA System Performance

	Valid Users		Invalid Users	
Surrounding conditions	**Two-Factor A-MFA**	**Three-Factor A-MFA**	**Two-Factor A-MFA**	**Three-Factor A-MFA**
Light and Noise are in range	94%	93%	0%	0%
Light is in range	92%	90%	0.5%	0%
Noise is in range	90%	88%	0.45%	0%
None are in range	86%	84%	3%	0%

Acknowledgements

This work is supported by the National Security Agency under Grant Number :H98230-15-1-0266. Points of view and opinions on this paper are those of the author(s) and do not Necessarily represent the position or policies of the United States.

For details, contact Dr. Dipankar Dasgupta,
Professor of Computer Science,
Director of Center for Information Assurance (CfIA)
Email: dasgupta@memphis.edu