Poster: Innovations in Security Mechanisms through Decomposition and Reuse of Body Functions: A Preliminary Study on Password Authentication

Takumi Takaiwa*, Seiya Kajihara*, Tsubasa Shibata*, Soichi Takigawa*, Tetsushi Ohki* and Masakatsu Nishigaki*
*Shizuoka University, Hamamatsu, Shizuoka 432-8011, Japan, Email: nisigaki@inf.shizuoka.ac.jp

***Abstract*—The human body has traditionally been perceived as a singular black box. Advancements in technology would allow the human body to be disassembled in terms of its individual organs. Exploration of the brain and five senses is already underway, enabling communication through brain–machine interfaces (BMI) [1] and sensory experience sharing [2]. In the near future, controlling bodily functions at the component level, such as the brain, memory, senses, organs, and cells, may become feasible. Furthermore, each component is API-enabled, allowing bodily functions to be freely accessed and utilized. Therefore, this study introduces the "Internet of Functions (IoF)." Within the IoF context, security technologies, previously based on the human body as a single entity, are now considered in terms of individual components (functions). The study examines new security mechanisms by focusing on user authentication at the part level as a pivotal step in IoF security research. We propose three novel user authentication mechanisms and discuss them in detail, thereafter evaluate their feasibility by conducting preliminary experiments on five participants.**

I. INTRODUCTION

In the Internet of Functions (IoF) world, security technologies that traditionally view the human body as a single entity require consideration at the component (functional) level. By dividing the human body into components, the design space is expanded, enabling new security mechanisms. However, this also increases the attack surface, leading to more complex and severe attacks by intruders. These two aspects are in a "light and shadow" relationship, and it is necessary to discuss both sides when examining IoF security. This paper serves as an initial report that focuses on its light side and contributes to IoF advancement by exploring new security mechanisms.

User authentication is the security mechanism discussed herein. Verifying individual identities when accessing various services remains essential even in the IoF world. Here, we define user authentication as "the process by which a human being, a resident of the physical world, inputs a credential into the cyber world (computer) through an input method." User authentication generally falls into three categories: knowledge-, possession-, and biometric-based. This study focuses initially on knowledge-based authentication, which involves a series of physical actions from storing to inputting credentials, making it well suited for IoF paradigms.

Password authentication is a quintessential example of knowledge-based user authentication. In password authentication, a password (human memory information) serves as physical world credentials and is typically entered into the cyber world (computer) using a keyboard. Here, a keyboard serves as a metaphor for various input devices. Just as the pen has been a fundamental device for "writing characters" since ancient times, we posit that the keyboard will continue to be essential for "computer input" in the IoF world.

Traditional password authentication follows the process of "human → keyboard typing → login." In contrast, IoF-style password authentication is decomposed into the following steps: "brain (memory area) → brain (control area) → nerves → muscles → keyboard typing → login" (Figure 1, scenario ①). This approach enables new security mechanisms, such as (i) enhancing password length and variety using external memory components (Sect. 2.A), (ii) air-gap authentication via cybernetic avatars (CAs) (Sect. 2.B), and (iii) fail-safe stop of muscle functions upon authentication failure (Sect. 2.C).

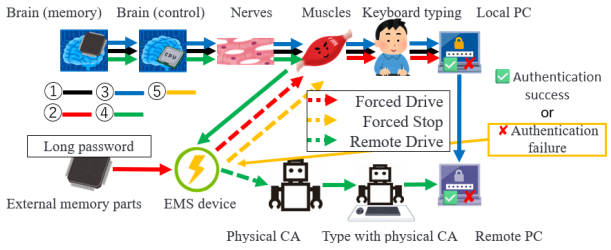


Fig. 1. New security mechanisms with IoF

II. METHODOLOGY

A. Enhancing Password Entropy Using External Memory Components

Breaking down the human body into components enables the replacement of one component by another possessing the same function. This allows password authentication to be restructured as "external memory component → EMS device → muscles → keyboard typing → login" (Figure 1, scenario ②). By moving the storage location of passwords from the brain (memory area) to an external memory, the burden and limitations of memorization can be eliminated, allowing users to increase password entropy in terms of length, character type, and randomness. Enhanced entropy can increase the effort required for manual input due to longer, more complex passwords. However, by shifting bodily control

from the brain (control area) and nerves to an electric muscle stimulation (EMS) system, involuntary finger movements can automatically input the password. This reduces the burden of password entry. Notably, the information stored in the external memory component is not the password itself but the EMS pattern necessary for password entry.

In IoF password authentication, credentials (electric stimulation for typing) are stored externally, shifting the authentication from memory-based to possession-based. Moreover, since muscle control through the EMS system is governed by the user's unique biological characteristics (muscle and nerve tissues), this approach can also be considered biometric-based. Therefore, IoF password authentication can effectively create a two-factor authentication system utilizing both possession and biometrics [3].

B. Air-gap Authentication via Cybernetic Avatar Operation

A cybernetic avatar (CA) is "a type of avatar that are designed to enhance people's physical, cognitive, and perceptual abilities through the integration of advanced technologies such as robotics and AI" [4]. In the IoF world, where body components can be replaced, physical robotic CAs can serve as substitutes for the human body, thereby transforming the concept of remote login. Traditional remote login uses the process of "human→ keyboard typing → login to local PC → Internet → login to remote PC" (Figure 1, scenario ③). With the prevalence of CAs, remote login in the IoF world can follow the sequence "brain (memory area) → brain (control area) → nerves → muscles → EMS device → physical CA → keyboard typing on remote PC by physical CA → login to remote PC via physical CA" (Figure 1, scenario ④).

This mechanism is valuable for the secure remote maintenance of isolated systems. Imagine an isolated system and a physical robotic avatar located remotely. Instead of directly logging into the isolated system via the Internet, remote login is limited to the physical robotic CA. Furthermore, the input device of the isolated system is restricted to a keyboard at the remote location, allowing maintenance to be conducted through the physical robotic CA's keystrokes. By limiting the potential entry points for intruders and malware over the Internet to the body of the physical robotic CA itself, physical constraints are imposed on the attack paths leading to the isolated system (i.e., unauthorized login to the isolated system is only possible through the keystrokes of the physical robotic CA). Monitoring the physical robotic CA is easier since it can be seen, unlike the invisible nature of cyberspace attacks.

C. Fail-safe Stop of Muscle Functions upon Authentication Failure

Traditionally, password authentication failure prompts reattempts, and repeated failures result in temporary lockouts. In the IoF world, not only can the authentication system be disabled, but also any bodily activities attempting unauthorized login can be suspended. For example, repeated authentication failures may stop energy to muscles or nerve signals, preventing further login attempts by halting muscle activity (Figure 1, scenario ⑤).

In this approach, failure results in the attacker's body losing mobility, potentially increasing the psychological pressure and deterring further attempts. Although interventions in human bodily autonomy raise ethical considerations, fail-safe stops can be reasonably justified when a user's (or victim's) safety is at risk due to user's careless behavior or attacker's deliberate harmful intent.

III. PRELIMINARY EXPERIMENT

As a preliminary experiment on the three new mechanisms, we developed a device for involuntary control of fingers using an EMS device with multi-pad electrodes (corresponding to the dotted arrows in Figure 1, scenarios ②④⑤).

In the experiments for Mechanisms (i) and (ii) (Experiment I), electrodes were attached to the left forearms of five participants. The aim was to identify the ideal electrode sets for controlling the fingers of the left hand. Experiment I was repeated twice for each of the five participants. The results of the first trial were considered as the template, and the second served as a query for each participant to simulate user authentication, thereby allowing the evaluation of true acceptance and false acceptance rates.

For Mechanism (i), Experiment I assessed the feasibility of achieving correct keystrokes during authentication by applying the EMS signals in the external memory to user arms. Mechanism (ii) explored whether keystrokes could be performed using a physical robotic CA artificial arm by transferring the user's electromyographic signal to the CA's EMS device. This envisions the human arm as a sophisticatedly crafted artificial arm for CA that is indistinguishable from a human arm in composition. Experiment I confirmed that impersonation is currently challenging (low false acceptance rate) and that authentication accuracy requires improvement (insufficient true acceptance rate caused by factors such as forearm fatigue and improper hand positioning contribute to false rejection).

In the experiments for Mechanism (iii) (Experiment II), the electrode sets determined in Experiment I were used to administer EMS. This tested the participants' ability to resist electrical stimulation and move their fingers. The aim of Experiment II was to determine whether EMS control can enforce a fail-safe halt of finger movements. The results showed that none of the participants could move their fingers against the electrical stimulation, supporting the feasibility of implementing fail-safe mechanisms for human body control.

REFERENCES

[1] WIRED. "Watch Neuralink's First Human Subject Demonstrate His Brain-Computer Interface," https://www.wired.com/story/neuralink-implant-first-human-patient-demonstration

[2] Y. Ju *et al.* "Haptic Empathy: Conveying Emotional Meaning through Vibrotactile Feedback," Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, 2021.

[3] T. Takaiwa *et al.* "Electrical Muscle Stimulation System for Automatic Reproduction of Secret Information Without Exposing Biometric Data," International Conference on Human-Computer Interaction, 2024.

[4] H. Ishiguro *et al.* "Cybernetic Avatar," https://link.springer.com/book/10.1007/978-981-97-3752-9

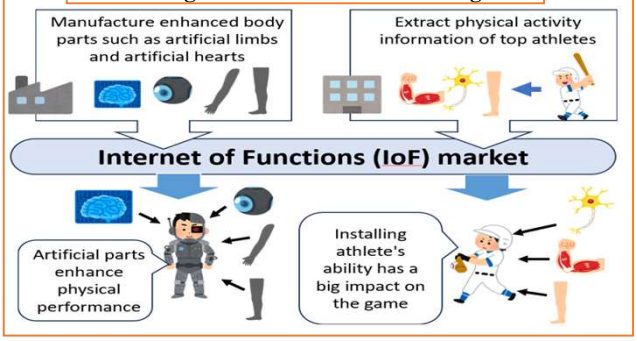
Poster: Innovations in Security Mechanisms through Decomposition and Reuse of Body Functions: A Preliminary Study on Password Authentication

Takumi Takaiwa*, Seiya Kajihara*, Tsubasa Shibata*, Soichi Takigawa*, Tetsushi Ohki*, Masakatsu Nishigaki* *Shizuoka University

1. Motivation

- **Internet of Functions (IoF):**
  - In the near future, controlling bodily functions at the component level, such as the brain, memory, senses, organs, and cells, may become feasible.
  - Each component is API-enabled, allowing bodily functions to be freely accessed and utilized.
- **Benefits and Drawbacks in IoF Security are in a "Light and Shadow" Relationship:**
  - **Benefits (Lights)**: Expansion of design space makes new security mechanisms possible.
  - **Drawbacks (Shadows)**: Increasing attack surfaces makes attacks by adversaries more complex and severe.
- **Objective of This Study:**
  - A balanced discussion considering both benefits and drawbacks is necessary when examining IoF security. We begin with exploring the former, contributing to the advancement of the IoF world.
- **This Study focuses initially on:**
  - **User Authentication**: The process of a human being, a resident of the physical world, inputting a **credential** into the cyber world (computer) through an **input method**. Verifying individual identities when accessing various services remains essential even in the IoF world.
    - **Password Authentication**: Involves a series of physical actions from storing to inputting credential (password), making it suited for IoF paradigms.
      - A password (human memory information) serves as physical world credentials and is typically entered into the cyber world (computer) using a keyboard.
      - Here, a keyboard serves as a metaphor for various input devices.

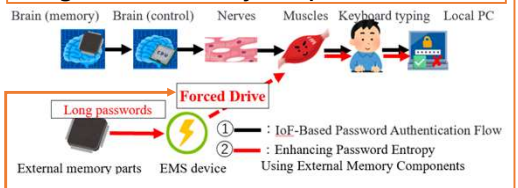
Human Augmentation Achieved Through IoF



Contribution: We propose three novel IoF-style user authentication mechanisms and discuss them in detail, thereafter evaluate their feasibility by conducting preliminary experiments on five participants.

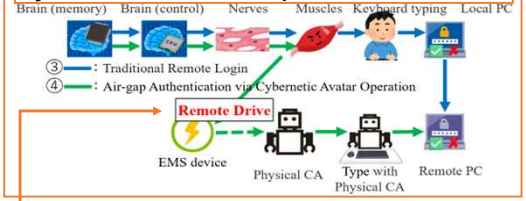
2. Three New Security Mechanisms

Mechanism (i): Enhancing Password Entropy Using External Memory Components



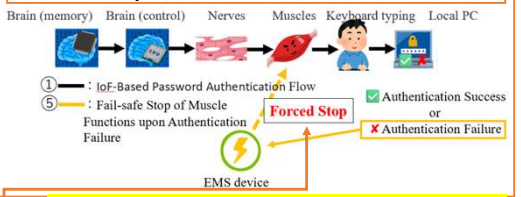
Contribution: External memory increases password length, character type, randomness, frequency of changes. Electric muscle stimulation (EMS) system helps automatically input the password.

Mechanism (ii): Air-gap Authentication via Cybernetic Avatar (CA) Operation



Contribution: Limiting entry points to the physical robotic CA makes monitoring easier, as it is visible unlike cyberspace attacks.

Mechanism (iii): Fail-safe Stop of Muscle Functions upon Authentication Failure



Contribution: Failure immobilizes the attacker, increasing psychological pressure and deterrence. While interventions in bodily autonomy raise ethical issues, fail-safe stops can be justified for user.

3. Preliminary Experiment

Forced Drive

1. EMS signal for password typing stored in external memory parts transmitted to the user's arm via EMS device.
2. EMS signals are applied from the user EMS device to the arm, causing forced drive.
3. The arm moves involuntarily, typing on a PC keyboard to log in.

Experiment I

- Verified whether controlling user's fingers via EMS signals is possible.

Remote Drive

1. Electromyographic (EMG) signals are sensed from the operator's arm.
2. EMS signals to replicate finger movements of CA are calculated from EMG signals.
3. Transfer EMS signals to artificial arm of CA.
4. EMS device of CA drives CA's artificial arm.
5. CA types on remote PC keyboard to log in.

Experiment I (Envisions the human arm as a sophisticatedly crafted CA arm, indistinguishable from a human arm in composition.)

- Verified whether controlling CA's fingers using EMG to EMS signal transfer is possible.

Forced Stop

1. An authentication failure is detected.
2. Authentication system instructs the user's EMS device to halt finger muscle activity.
3. EMS device applies EMS signals to the user's arm to enforce stop.
4. Muscle function ceases, rendering the user immobile.

Experiment II

- Verified whether forcibly stopping movement of human fingers using EMS signals is possible.

3-1. Experimental Objectives

- We conduct preliminary experiments (Experiments I and II) to explore the feasibility of the proposed methods.
  - We constructed an experimental system.
  - We recruited 5 participants.

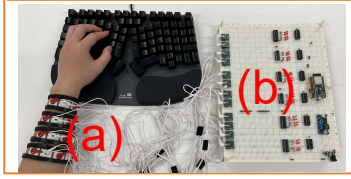
Experiment I: (Steps 1, 2, 3, 4, 5 in "3-3. Experimental Details")

- For Mechanism (i): Assesses the feasibility of achieving correct keystrokes during authentication by applying the EMS signals in the external memory to user arms.
- For Mechanism (ii): Explores whether keystrokes could be performed using a physical robotic CA artificial arm by transferring the user's EMG signal to the CA's EMS device.

Experiment II: (Steps 1, 2, 3, 6 in "3-3. Experimental Details")

- For Mechanism (iii): Tests the participants' ability to resist EMS signals and move their fingers to determine whether EMS control can enforce a fail-safe halt of finger movements.

3-2. Multi-Pad Electrodes and Multi-Channel EMS Generator



(a) Multi-Pad Electrodes
(b) Multi-Channel EMS Generator (EMS device)

3-3. Experimental Details

- For controlling the movement of the fingers, multiple electrodes are attached to the forearm, and two of them are used as the active electrode and the return electrode, respectively, to apply electrical stimulation.
- Electrodes placed on the left forearm of 5 participants to identify the electrode pairs required to control each finger.

1. The little/ring/middle/index/thumb fingers are placed on the keys q/w/e/r/v, respectively.
2. EMS signal are applied using all combinations of active and return electrodes.
   - Use a biphasic pulse with a pulse width of 200 μs, a cycle of 30 ms, and a voltage of 18 volts.
3. If a specific electrode combination results in a finger pressing down on a keyboard key, that combination is recorded as the electrode set for moving that finger.
4. Steps 1-3 are repeated twice for each of the 5 participants.
   - A 10-min break is provided between trials, during which electrodes are not removed.
5. Using the result of the first trial as the template and the second as the query for each participant, user authentication is simulated to calculate the true acceptance rate and the zero-effort false acceptance rate. (See the table below.)
   - Since this is a preliminary study, the experiments did not apply electric stimuli to participants. Instead, user authentication was simulated by comparing the electrode pairs identified in Step 4.
6. Using the electrode pairs identified in Steps 1-3, EMS signals are applied to forcibly move each finger into a specific position and hold it there.

4. Experimental Results and Discussion

	User1					User2					User3					User4					User5				
	L	R	M	I	T	L	R	M	I	T	L	R	M	I	T	L	R	M	I	T	L	R	M	I	T
Simulated "True Acceptance Rate"	0.08	0.5	0.55	0	0.33	N/A	0	0.48	0.67	0	0.6	0.5	0.43	0	0.33	0	0.38	0.86	N/A	N/A	0.5	0.67	0.49	0	N/A
Simulated "False Acceptance Rate"	0.08	0.09	0.1	0	0	N/A	0	0.07	0	0	0	0	0.14	0	0	0	0.16	0.11	N/A	N/A	0.06	0.16	0.08	0	N/A

* L: Little finger, R: Ring finger, M: Middle finger, I: Index finger, T: Thumb

Experiment I Results

- Impersonation is currently challenging (low false acceptance rate) and that authentication accuracy requires improvement (insufficient true acceptance rate caused by factors such as forearm fatigue and improper hand positioning contribute to false rejection).

Experiment II Results

- None of the participants could move their fingers against the electrical stimulation, supporting the feasibility of implementing fail-safe mechanisms for human body control.

Acknowledgments
This research was partially supported by the JST Moonshot Research and Development Program JPMJMS2215 and JSPSKAKENHI 23K28084. We would like to express our gratitude to Dr. Ryoya Shibaike from Kyoto University for his valuable advice regarding the new security Mechanism (iii) discussed in Chapter 2. We also appreciate the support of Mr. Masakatsu Takayanagi from Shizuoka University for designing the EMS device.