EmIr-Auth: Eye-movement and Iris Based Portable Remote Authentication for Smart Grid

Zhuo Ma , Yilong Yang, Ximeng Liu , *Member, IEEE*, Yang Liu , Siqi Ma , Kui Ren, *Fellow, IEEE* and Chang Yao*

***Abstract*— With the development of Industry 4.0, the communication of smart grid has recently been taken seriously to ensure secure communication between operator and control center. However, the authentication process between them faces many challenges. Once the attacker successfully authenticated in the control center, the privacy data in the smart grid may leak and cause irreparable damage to the user. In addition, operator authentication is one of the most basic and crucial processes. Therefore, we propose the *eye-movement and iris recognition based authentication (EmIr-Auth)*, a novel biometrics-based remote operator authentication scheme. EmIr-Auth uses the recorded eye-movement trajectory and randomly selected iris image to authenticate operators, which is beneficial in that it is able to get rid of many cryptographic computations, as well as the need to minimize message exchange. Furthermore, except for a high-resolution camera, we do not require any additional biometric sensors in this scheme. Using the Burrows-Abadi-Needham logic, we demonstrate that our scheme provides secure authentication. Moreover, we analyze the attacks that EmIr-Auth can resist by informal security analysis. Experimental results show that EmIr-Auth is efficient enough to deploy on portable devices and reduce the overhead of authentication procedure.**

***Index Terms*— smart grid, biometric, authentication, eye-movement trajectory, iris recognition**

I. Introduction

THE Internet of Things (IoT) is an extension and expansion network based on the Internet. It combines thousands of information sensing devices and smart devices with the Internet in various ways (WLAN, 5G, etc.) to realize the interaction between anything. The basic trend of the development of IoT is that it tends to be open and communication. The IoT enables thousands of smart devices to connect and communicate with each other and makes the types and functions of devices in the smart grid more diversified [1]. Under the trend of the IoT, industry 4.0 uses the Cyber-Physical System (CPS) to digitally and intelligently supply, manufacture and sell the information in production, and finally achieve accurate, effective, and personalized product supply. It requires safe and flexible operations in the cloud server [2]. And Smart Grid (SG) combining with industry 4.0 can provide convenient and stable power transmission. As the most anticipated product of power grid 2.0, smart grid empowers the traditional power grid with high artificial intelligence. On the basis of integrated, high-speed two-way communication network, it realizes reliable, safe and efficient operation of power grid through advanced hardware, advanced control methods, and remote check.

Smart grid is a vast network of computers and power infrastructures. Each energy producer or power company that provides power services has its own Control Center (CC), which carries out information communication with the equipment and interacts with the operators to provide customers with rapid power demand response and real-time electricity bills. Compared with traditional power grid, smart grid under industrial control system can be connected, inquired and controlled remotely through two-way communication. Safe and efficient commands and control information transmission are provided among smart grid devices such as smart meters. Data and information for many users are also saved to the control centers, any unauthorized personnel should not access these records [3]. The identity authentication of operators is the first line of defense for the accurate and safe execution of the whole system. Therefore, the process of certification needs greater reliability and security. Once the system is attacked, hackers can carry out malicious operations and forge effective data to gain profits [4].

A. Motivation

Industry 4.0 involves different enterprises, departments, and fields, making cross-industry and cross-sector inevitable, and making the Internet-oriented structured remote network to develop rapidly. The development of remote structured networks may make the control center system an unmanned system due to resource or structural problems, and operator will use remote controls. At this time, in the smart grid industry, which is in the interest of the user, the remote authentication of the operator needs to increase the high-intensity factors, such as the biometrics currently used on the terminal. Fig. 1 shows the base structure of the smart grid. When the operator needs to interact with the control center remotely, the first step is that the control center uses the authentication protocol to authenticate the operator remotely in the open network. Iris authentication methods in biometrics have been widely used. However, when users make use of iris recognition, which is very widespread recently, they are vulnerable to forgery attacks due to the technical limitations of various extraction methods, such as using a static image with iris information of the authenticator. The security threats brought by remote authentication should not only be noticed in terms of number and scope but should also be taken into account in terms of authorization privacy and access policies [5]. Therefore, it is critical to develop security technologies for remote systems that are immune to any potential threat.

B. Contributions

In this paper, we investigate the possibility of integrating eye-movement and iris recognition as a new method for operator remote authentication. Based on this, we further propose an authentication scheme based on eye-movement and iris recognition and design it especially to support portable devices. Our contributions are summarized as below.

This work was supported by the National Natural Science Foundation of China (Grant No. U1804263, U1764263, 61872283, U1708262), the China 111 Project (No. B16037).

Z. Ma, Y. Yang and Y. Liu are with School of Cyber Engineering, Xidian University, Xi'an 710071, China (e-mail: mazhuo@mail.xidian.edu.cn, echotoken@gmail.com, bcds2018@foxmail.com,).

X. Liu is with College of Mathematics and Computer Science, Fuzhou University, China and Key Laboratory of Information Security of Network Systems, Fujian Provincial (e-mail: snbnix@gmail.com).

S. Ma is with Data 61, CSIRO, Marsfield Site, NSW,2122 (e-mail: siqi.ma@csiro.au).

K. Ren is with the Institute of Cyberspace Research, Zhejiang University, Zhejiang, China (e-mail: kuiren@zju.edu.cn).

C. Yao is with National Natural Science Foundation of China Beijing, CN 100085 (e-mail: yaochang@nsfc.gov.cn).

∗ Corresponding author.

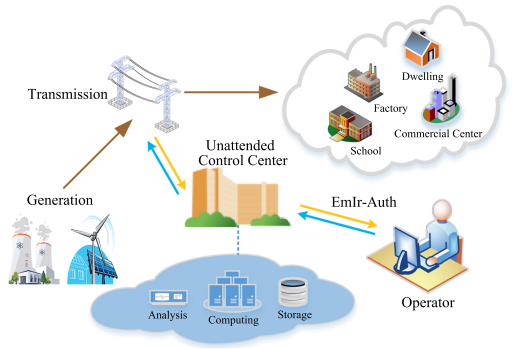


Fig. 1. The base structure of smart grid.

1) We propose EmIr-Auth, a novel biometrics-based remote operator authentication mechanism in the smart grid. Our work is the effort that makes it possible to authenticate operator through eye-movement trajectory combined with iris recognition remotely.
2) Instead of performing identity authentication in existing eye-movement-based authentication methods, EmIr-Auth only uses eye-movement trajectory to achieve freshness verification. This leads to the generation of our visual stimulus independent of the biological properties. Moreover, the visual stimulus generation of our scheme contains cryptographic attributes.
3) Our approach is able to circumvent inherent drawbacks in traditional iris recognition-based authentication schemes and defend against direct attacks using fake iris image.
4) We build the prototype of EmIr-Auth on Android smartphone with no hardware requirement except for a high-resolution camera, and perform comprehensive experiments to evaluate the performance of EmIr-Auth in terms of accuracy, efficiency, and security.

C. Paper organization

The rest of this paper is organized as follows: Section II gives the related works of our study. In Section III, we briefly introduce the theoretical preliminaries of our work. Section IV describes EmIr-Auth, a novel biometric authentication scheme. In Section V, we analyze the security properties of our approach using BAN logic. Section VI performs a series of comprehensive experiments and the advantage of our scheme is illustrated by comparing with several classic approaches. Finally, we conclude the paper in Section VII.

II. Related Work

Biometric authentication refers to the process of establishing an identity based on biometric traits. Generally, current biometric user authentication techniques can be categorized into two types: Physiological and Behavioral methods [6]. Physiological methods utilize biometrics based on stable body features [7], such as fingerprint recognition, facial recognition, iris scan, and retina recognition. These biometrics offer many advantages over traditional cryptographic keys [8]. However, a potential risk is that these biometric traits can be obtained or duplicated by adversaries, rendering a stable biometric trait alone not secure enough in a single-factor model. Recently, multi-factor user authentication based on stable biometrics has become a trending topic of research [9]–[11]. In contrast, behavioral methods leverage alterable biometric traits [7], [12], including biometrics based on the patterns users behave. Researchers have employed alterable biometric traits in different user authentication schemes [13], [14]. In contrast to stable biometric traits, the alterable biometric traits are resistant to forgery and replay. In addition, compared with stable biometric technology, it has the advantage of providing stronger non-repudiation. However, the potential downside of this scheme is that the recognition rate may not be high enough to provide security for remote user authentication [7].

Eye-movement analysis researches have been conducted for a long time. Kasprowski and Ober [15] first began to study the biological feature of human eye-movement. They proposed a breakthrough new eye recognition technology based on eye-movement features. The system can measure the coordinates of the points that the user is gazing at on the computer screen, that is, where the user is looking, and collect the information of eye-movement at the same time. C. Holland and O. V. Komogortsev [16] have studied many experiments and many factors on eye-movement-based human identification. The results verified that eye-movement biometric identification holds promise as a behavioral biometric technique. Recently, Y. Zhang et al. [17] proposed a scheme to authenticate the user using the eye-movement continuously. However, this method not only requires complicated algorithms but also needs gaze tracking equipment to capture eye-movement trajectory, which is impractical especially for the usage of mobile user remote authentication.

Recently, many user authentication schemes for smart grid have been proposed. Mahmood et al. [18] optimized it and proposed a hybrid Diffie–Hellman based lightweight authentication scheme using AES and RSA for session key generation. However, because RSA algorithm is used in this scheme, the computation of the scheme is very high. In 2018, Li et al. [19] proposed a three-element authentication scheme for Intelligent City global mobile network based on biological characteristics. Later, N.Kumar et al. [20] proposed a protocol allowing establishment of secret session key between a SG device and a UC after mutual authentication. In this paper, we propose a novel remote authentication for smart grid with biometric features.

III. Theoretical Preliminaries

A. Elliptic Curve Over F_p

let $p \geq 3$ be a prime number. A non-singular elliptic curve E over F_p is defined to be the set of solutions $(x, y) \in F_p$ to the equation

$$y^2 = x^3 + ax^2 + b$$

where $a, b \in F_p$ are constants such that $4a^3 + 27b^2 \neq 0(mod\ p)$, together with the point at infinity or zero point denoted by $\mathcal{O}$. The set of points $E(F_p)$ forms a abelian group under addition modulo p operation [21].

Definition 1 (Elliptic Curve Discrete Logarithm Problem(ECDLP)): Given an elliptic curve E defined over a finite field F_p, a point $P \in E(F_p)$, and a point $Q \in E(F_p)$, find the integer $k \in [1, p-1]$ such that $Q = kP$.

Definition 2 (Computational Diffie-Hellman Problem(CDHP)): Given $P, xP, yP \in F_p$, compute $xyP \in F_p$ without the knowledge of $x \in Z_p^*$ or $y \in Z_p^*$ where $z_p^* = \{a | 0 < a < p, gcd(a, p) = 1\}$.

B. Fuzzy Extractor

A fuzzy extractor $(\mathcal{M}, m, \ell, t, \epsilon)$ is given by two procedures (Gen, Rep) [22].

1) Gen is a probabilistic generation procedure, which on input $\omega \in \mathcal{M}$ outputs an extracted string $\sigma \in \{0,1\}^\ell$ and a public string θ. For any distribution W on $\mathcal{M}$ of min-entropy m, if $\langle \sigma, \theta \rangle \leftarrow Gen(W)$, the statistical distance $SD(\langle \sigma, \theta \rangle, \langle U_\ell, \theta \rangle) \leq \epsilon$, where $\mathcal{M}$ is a set containing biometric elements with a distance function $dis()$, U_ℓ represents the

uniform distribution on ℓ-bits binary strings and ϵ denotes the statistical distance between two given probability distributions $\langle \sigma, \theta \rangle$ and $\langle U_\ell, \theta \rangle$.

2) Rep is a deterministic reproduction procedure that allows to recover σ from the corresponding public string θ and any vector ω' close to ω: for all $\omega, \omega' \in \mathcal{M}$ satisfying $dis(\omega, \omega') \leq t$, if $\langle \sigma, \theta \rangle \leftarrow Gen(\omega)$, then $Rep(\omega', \theta) = \sigma$.

IV. Novel biometric-based Portable Device Authentication Scheme

In this section, we give the detail of our novel biometrics-based authentication scheme for portable devices. Our scheme consists of three phases, which are the initialization phase, the user registration phase, and the authentication phase. For convenience, notations used in this paper are summarized in Table I.

TABLE I
NOTATIONS

Notation	Description
n, p	Two large prime numbers
F_p	A finite prime field
E	A non-super singular elliptic curve over a finite field F_p
G	The additive group consisting of points on E
P	A generator of G with order n
$H(\cdot)$	A secure hash function
$\|\|$	The concatenation operation
$\oplus$	The bit-wise exclusive-or -.(XOR) operation
O_i	Operator i
C_j	Control center j
ID_i/ID_j	The identity of O_i/C_j
k_i	Authentication parameter of O_i
k	The secret key of C_j
P_{pub}	The public key of C_j
$E_k(\cdot)/D_k(\cdot)$	Symmetric encryption/decryption using the key k
ψ	The string used to generate the sequential flashing points
ζ	Captured operator's eye-movement trajectory

A. Initialization Phase

In this phase, the control center C_j selects a non-singular elliptic curve E_p over a finite filed $GF(p)$, a base point $P \in G$, where P is a large prime and G is an additive cyclic group of order n consisting of points on E_p, a secure collision-resistant one-way hash function $H(\cdot)$, and a symmetric-key crypto system Φ. Also, the control center chooses its private key k which is assumed to be 2048-bit, and then computes its public key $P_{pub} = kP$. Finally, the control center C_j declares its public parameters $\{p, E_p, P, P_{pub}, n, H(\cdot), \Phi\}$

B. Operator Registration Phase

In this phase, an operator O_i registers to the control center C_j using the following steps and the phase is summarized in Fig. 3.

1) O_i first inputs his/her identity ID_i, and imprints his/her personal iris biometrics B_i using high-resolution camera. Then O_i computes $(\sigma_i, \theta_i) \leftarrow Gen(B_i)$ and sends the registration request $Reg = \{ID_i || H(ID_i||\sigma_i)\}$ to control center C_j via a secure channel.
2) After receiving the request message Reg, C_j computes $k_i = H(ID_i||k)$, $z_i = k_i \oplus H(ID_i||\sigma_i)$. Then, center C_j sends $\{z_i\}$ to O_i via a secure channel.
3) Finally, after receiving $\{z_i\}$ from C_j, O_i securely stores $\{z_i, \theta_i\}$ into the device.

C. Authentication and Key Establishment Phase

In this phase, both O_i and C_j execute the following steps to mutually authenticate each other and agree on a session key for the following communication over insecure public channels.

1) O_i generates random numbers $x, r_i \in Z_n^*$ and computes $X = xP$, $K_1 = xP_{Pub}$, $CID_i = ID_i \oplus H(K_1||r_i)$, and $h_1 = H(ID_i||ID_j||r_i||X||K_1)$. And then, O_i sends the message $M_1 = \{CID_i, X, r_i, h_1\}$ to C_j via a public channel.
2) After receiving the message M_1, C_j computes $K_2 = kX(= K_1)$, $ID_i = CID_i \oplus H(K_2||r_i)$, and checks whether $h_1 = H(ID_i||ID_j||r_i||X||K_2)$ holds or not. If it does not hold, C_j terminates the session. Otherwise, C_j chooses random numbers $y, r_j \in Z_n^*$, and computes $Y = yP$, $k_i = H(ID_i||k)$, $k_{ij} = H(k_i||K_2||r_i||r_j)$, session key $SK = H(yX||k_{ij})$. Then C_j computes $\psi = H(ID_i||ID_j||X||Y||k_{ij})$, and encrypts ψ with k_{ij} ($C_1 = E_{k_{ij}}(\psi)$). Then C_j computes $h_2 = H(ID_j||Y||r_j||C_1||k_{ij}||SK)$. Finally, C_j sends the message $M_2 = \{ID_j, Y, r_j, C_1, h_2\}$ to O_i via a public channel.
3) Upon receiving M_2 from C_j, O_i captures the personal iris biometrics B_i', and computes $\sigma_i{}' = Rep(B_i', \theta_i)$, $k_i{}' = z_i \oplus H(ID_i||\sigma_i{}')$, $k_{ij}' = H(k_i'||K_1||r_i||r_j)$, session key $SK = H(xY||k_{ij}')$, and checks whether $h_2 = H(ID_j||Y||r_j||C_1||k_{ij}'||SK')$ holds or not. If it does not hold, O_i terminates the session. Otherwise, O_i obtains ψ by decrypting C_1 with k_{ij}', that is, $\psi = D_{k_{ij}'}\{C_1\}$. And then, ψ is transferred into a Sequential flashing points which will be displayed on the O_i's portable device. O_i needs to follow the flashing points, and the portable device will capture and analyze the O_i's eye-movement trajectory ζ. During this period, O_i's personal iris biometrics B_i'' will be randomly captured. Details on the eye-movement trajectory and randomly iris biometric capture procedure will be given in Subsection IV-D. And then, O_i checks whether $\sigma_i{}' \leftarrow Rep(B_i'', \theta_i)$. If it does not hold, O_i terminates the session. Finally, O_i encrypts ζ with SK, that is, $C_2 = E_{SK}(\zeta)$, computes $h_3 = H(ID_i||ID_j||X||Y||r_i||r_j||k_i'||SK||C_2)$, and sends the message $M_3 = \{C_2, h_3\}$ to C_j via a public channel.
4) After receiving the message M_3 from O_i, C_j checks whether the condition $h_3 = H(ID_i||ID_j||X||Y||r_i||r_j||k_i||SK||C_2)$ holds or not. If it does not hold, C_j terminates the session. Otherwise, C_j obtains ζ by decrypting C_2 with SK, that is, $\zeta = D_{SK}\{C_2\}$. And then, C_j compares the received eye-movement strings to the stored pattern. If it holds, C_j confirms that O_i is a legitimate operator. Otherwise, C_j terminates the session.

Finally, after mutual authentication and key establishment phase, both O_i and C_j negotiate the session key SK. The phase of our proposed scheme is summarized in Fig. 2.

D. Eye-movement Trajectory Capture and Random Iris Recognition Procedure

In the present research, we use the information of eye-movement trajectory and iris recognition to achieve the biometric authentication. To start with, different video segments corresponding to the eye-movement trajectory ζ are recorded by a high-resolution camera.

In order to automatically acquire information of eye-movement, we first empirically initialize a rectangle to select the sclera and pupil in the first frame and regard the center coordinates of the rectangular frame as the pupil center. Then, the particle filter algorithm [23] is used to track the eye-movement and record the trajectory of the pupil center. During this procedure, to address the problem of baseline drift,

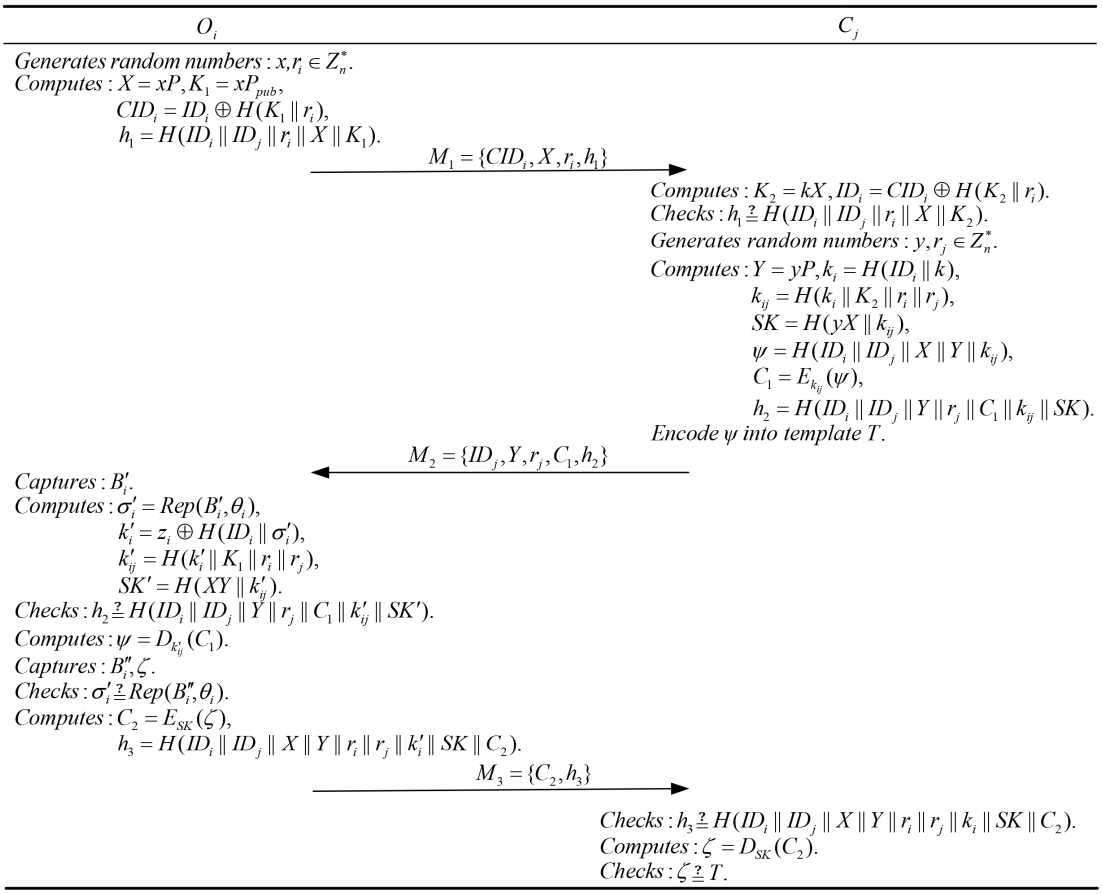


Fig. 2. Authentication and Key Establishment Phase

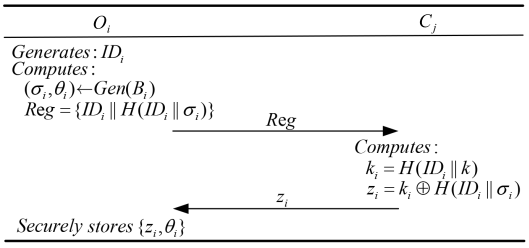


Fig. 3. Operator Registration Phase

we utilize the Least Square Algorithm to suppress it from the results of video detection. On this basis, we further develop a new saccade detection algorithm to detect the saccadic activities, which includes three main steps, i.e.,

Preprocessing: To preserve the effective saccadic component as much as possible, and suppress the noise more than 8Hz (such as the acquiring equipment noises, micro-movement of a camera, etc.), a 32-order IIR filter with the cut-off frequency of 0.01-8HZ is used to process the trajectory of the pupil center.

Wavelet Packet Decomposition (WPD): Because of less decomposition redundancy and better performances in time-frequency localization analysis, we perform the WPD algorithm to decompose the processed signals. In this way, the wavelet packet coefficients at level three are computed using a Haar mother wavelet. Considering the similarity of the decomposed components and the raw input signals, we selected the coefficients of the 3rd node at level three (see Fig. 4 b)) as the new analyzing object.

Encoding: Two sets of thresholds (HS1, HS2, HL1, HL2 and VS1, VS2, VL1, VL2) are applied to determine the input WPD coefficients as small saccade (the saccadic distance equals one box, i.e., the position of next highlight point is adjacent to the current one), large saccade (the distance equals two boxes) and non-saccade (gaze is held upon a fixed point) according to horizontal and vertical directions respectively. Furthermore, each saccadic activity is encoded into a character which represents the amplitude and direction of eye-movement. Specifically, "r" and "R" mean small and large right-oriented saccade and "l" and "L" represent small and large left-oriented saccade according to the horizontal channel; similarly, "u" and "U" are up-oriented saccade, and "d" and "D" are left-oriented saccade according to the vertical channel. Consequently, the ongoing eye- movement can be characterized as a series of strings which is composed of "r", "l", etc. According to the above description, each sequence will produce different paths and strings and one-to-one correspondence, that is, ζ in Table I and the meaning of the stored pattern in Section IV-C. After operator conducts original video recording and performs eye-movement trajectory capture and random iris recognition procedure, the stored pattern will be obtained. The procedure of the detection and encoding are shown in Fig. 4.

Considering the computational load and the robustness in the illumination-controlled environments, we adopt the CSUM (Cumulative SUMs) method [24] to recognize the iris image selected from the video. In addition, this method focuses on the variations of gray levels in the iris image, it is achievable in the portable devices. Moreover, we transfer the extracted iris features vectors into the Support Vector Machine (SVM) classifier for recognizing. To reduce the training time considerably while retaining identification performance, we choose a

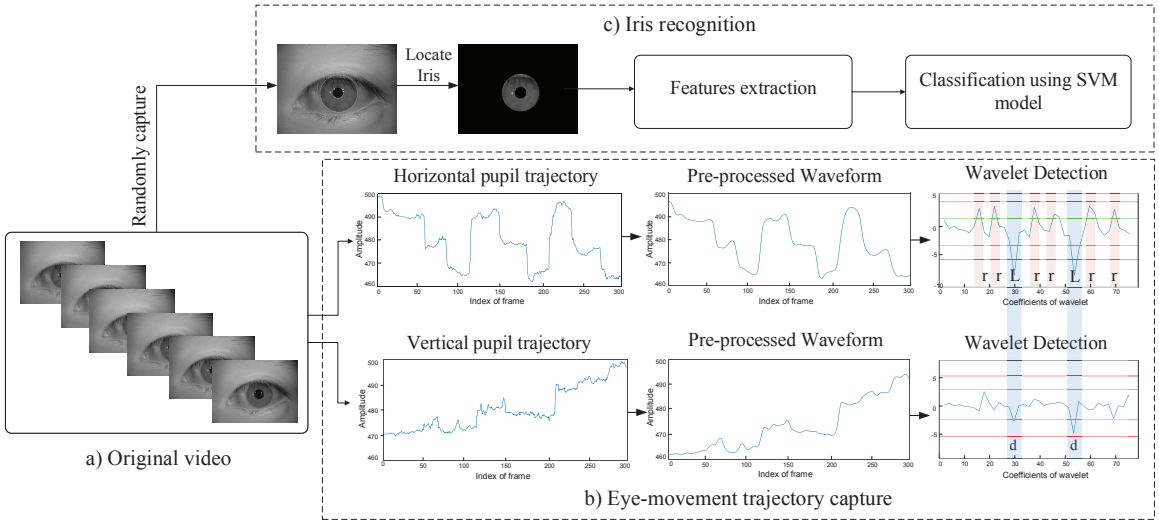


Fig. 4. The fundamental principle of eye-movement trajectory and random iris biometric capture. It consists of three units, i.e., a) Original video. It is captured by high-resolution camera; b) Eye-movement trajectory capture. This procedure is performed by tracking the center point of pupil in both horizontal and vertical directions; c) Iris recognition. The image used for iris recognition is randomly selected from the original video.

linear SVM model which uses a fast sequential dual algorithm [25] for handling the problem of multi-class.

V. Security Analysis

A. Authentication Proof Based on the BAN logic

The notations of the BAN logic are as follows:

- $P| \equiv X$: P belives X.
- $\#(X)$: X is fresh.
- $P \Rightarrow$: P has jurisdiction over X.
- $P \triangleleft X$: P sees X.
- $P| \sim X$: P once said X.
- (X, Y): X or Y is one part of (X, Y).
- X_K: X encrypted under the key K.
- $< X >_Y$: X combined with Y
- $(X)_K$: X is hash with the key K
- $P \overset{K}{\longleftrightarrow} Q$: K is a good key for communicating between P and Q.
- SK: The session key used in the current session.

Rules: The rules of the BAN logic are described as follows:

- $\frac{P| \equiv P \overset{K}{\longleftrightarrow} Q, P \triangleleft X_K}{P| \equiv Q| \sim X}$: The message-meaning rule.
- $\frac{P| \equiv \#(X)}{P| \equiv \#(X,Y)}$: The freshness-conjuncatenation rule.
- $\frac{P| \equiv \#(X), P| \equiv Q| \sim X}{P| \equiv Q| \equiv X}$: The nonce-verification rule.
- $\frac{P| \equiv Q \Rightarrow X, P| \equiv Q| \equiv X}{P| \equiv X}$: The jurisdiction rule.

Goals: According to the analytic procedures of the BAN logic, the proposed scheme need to satisfy the following goals.

- Goal 1: $O_i| \equiv (O_i \overset{SK}{\longleftrightarrow} C_j)$.
- Goal 2: $O_i| \equiv C_j| \equiv (O_i \overset{SK}{\longleftrightarrow} C_j)$.
- Goal 3: $C_j| \equiv (O_i \overset{SK}{\longleftrightarrow} C_j)$
- Goal 4: $C_j| \equiv O_i| \equiv (O_i \overset{SK}{\longleftrightarrow} C_j)$

Idealized form: The arrangement of the proposed scheme to the idealized form is as follows:

- Message 1:
  $O_i \Rightarrow C_j : \langle ID_i, r_i, X, O_i \overset{K_1}{\longleftrightarrow} C_j \rangle_{O_i \overset{k_i}{\longleftrightarrow} C_j}$
- Message 2:
  $C_j \Rightarrow O_i : \langle ID_j, r_j, Y, C_1, O_i \overset{SK}{\longleftrightarrow} C_j \rangle_{O_i \overset{k_{ij}}{\longleftrightarrow} C_j}$
- Message 3:
  $O_i \Rightarrow C_j : \langle ID_j, ID_i, X, Y, C_2, O_i \overset{SK}{\longleftrightarrow} C_j \rangle_{O_i \overset{k_{ij}}{\longleftrightarrow} C_j}$

Hypotheses: In order to analyze the proposed scheme, we make the following assumptions about the initial state of our scheme:

- $H_1 : O_i| \equiv O_i \overset{k_{ij}}{\longleftrightarrow} C_j$
- $H_2 : O_i| \equiv \#(r_j)$
- $H_3 : C_j| \equiv O_i| \Rightarrow O_i \overset{SK}{\longleftrightarrow} C_j$
- $H_4 : O_i| \equiv C_j| \Rightarrow O_i \overset{SK}{\longleftrightarrow} C_j$
- $H_5 : C_j| \equiv O_i \overset{k_i}{\longleftrightarrow} C_j$
- $H_6 : S_i| \equiv \#(r_i)$
- $H_7 : C_j| \equiv O_i| \Rightarrow O_i \overset{K_1}{\longleftrightarrow} C_j$

The idealized form of the proposed protocol is analyzed based on the BAN logic rules and the assumptions. The main proofs are stated as follows:

From message 2,we have

$S_1 : O_i \triangleleft \langle ID_j, r_j, Y, C_1, O_i \overset{SK}{\longleftrightarrow} C_j \rangle_{O_i \overset{k_{ij}}{\rightleftharpoons} C_j}$

From H_1, S_1, and $Rule(1)$, we get

$S_2 : O_i| \equiv C_j| \sim \langle ID_j, r_j, Y, C_1, O_i \overset{SK}{\longleftrightarrow} C_j \rangle$

From $message2, H_2, Rule(4)$, we have

$S_3 : O_i| \equiv \#(ID_j, r_j, Y, C_1, O_i \overset{SK}{\longleftrightarrow} C_j)$

From $S_2, S_3, Rule$, we obtain

$S_4 : O_i| \equiv C_j| \equiv (ID_j, r_j, Y, C_1, O_i \overset{SK}{\longleftrightarrow} C_j)$

According to H_2, we apply the BAN logic rule to break conjunctions to produce

$S_5 : O_i| \equiv C_j| \equiv O_i \overset{SK}{\longleftrightarrow} C_j \ GoleG_2$

From H_4, S_5, and $Rule(3)$, we get

$S_6 : O_i| \equiv O_i \overset{SK}{\longleftrightarrow} C_j$

From Message 1, we obtain

$S_7 : C_j \triangleleft \langle ID_i, r_i, X, O_i \overset{K_1}{\longleftrightarrow} C_j \rangle_{O_i \overset{k_i}{\longleftrightarrow} C_j}$

From H_5, S_7, and $Rule_1$, we have

$S_8 : C_j| \equiv O_i| \sim \langle ID_i, r_i, X, O_i \overset{K_1}{\longleftrightarrow} C_j \rangle$

From $H_6, S_8, Rule_2$ and $Rule_4$, we get

$S_9 : C_j| \equiv O_i| \equiv (ID_i, r_i, X, O_i \overset{K_1}{\longleftrightarrow} C_j)$

According to H_6, we apply the BAN logic rule to break conjunctions to produce

$S_{10} : C_j| \equiv O_i| \equiv O_i \overset{K_1}{\longleftrightarrow} C_j$
From H_7, S_10, and $Rule_3$, we obtain
$S_{11} : C_j| \equiv O_i \overset{K_1}{\longleftrightarrow} C_j$
According to H_5, H_6, S_11, and $k_{ij} = H(k_i||K_1||r_i||r_j)$, we could have
$S_{12} : C_j| \equiv O_i \overset{k_{ij}}{\longleftrightarrow} C_j$
From message 3, we get
$S_{13} : S_i \triangleleft \langle ID_j, ID_i, X, Y, C_2, O_i \overset{SK}{\longleftrightarrow} C_j \rangle_{O_i \overset{k_{ij}}{\longleftrightarrow} C_j}$
From S_{12}, S_{13}, and $Rule(1)$, we get
$S_{14} : C_j| \equiv O_i| \sim \langle ID_j, ID_i, X, Y, C_2, O_i \overset{SK}{\longleftrightarrow} C_j \rangle$
From $message3, H_6, Rule(4)$, we have
$S_{15} : C_j| \equiv \#(ID_j, ID_i, X, Y, C_2, O_i \overset{SK}{\longleftrightarrow} C_j)$
From $S_{14}, S_{15}, Rule_2$, we obtain
$S_{16} : C_j| \equiv O_i| \equiv (ID_j, ID_i, X, Y, C_2, O_i \overset{SK}{\longleftrightarrow} C_j)$
According to H_6, we apply the BAN logic rule to break conjunctions to produce
$S_{17} : C_j| \equiv O_i| \equiv O_i \overset{SK}{\longleftrightarrow} C_j \ GoleG_4$
From H_4, S_17, and $Rule(3)$, we get
$S_6 : C_j| \equiv O_i \overset{SK}{\longleftrightarrow} C_j$

B. Informal Security Analysis

In terms of functional analysis, we focus on the security against replay attack, privileged insider attack, stolen verifier attack, modification attack, man-in-the-middle attack, known-key attack, perfect forward secrecy, anonymity, mutual authentication. The detailed analysis of each above functions are as follows:

- *Reply Attack*: Suppose the adversary $\mathcal{A}$ intercepts the message $M_1 = CID_i, X, r_i, h_1$, and tries to impersonate O_i by replaying this message to the center C_j. But adversary $\mathcal{A}$ cannot compute the valid $h_3 = H(ID_i||ID_j||X||Y||r_i||r_j||k_i||SK||C_2)$ without knowing x and k_i. Therefore, the proposed scheme could withstand the replay attack.
- *Privileged Insider Attack*: In the registration phase of the proposed scheme, O_i sends ID_i and $H(ID_i||\sigma)$ to the control center C_j. The operator's password is not sent at this phase. Therefore, our scheme does not have the risk of a privileged insider attack.
- *Stolen Verifier Attack*: In the operator registration phase of the proposed phase, the center C_j stores the identity information $H(ID_i||k)$ of the operator O_i. The identity is combined with C_j's secret key k using a secure one-way hash function $H(\cdot)$. The adversary $\mathcal{A}$ cannot obtain the identity ID_i. Therefore, the proposed scheme is secure against stolen verifier attack.
- *Modification Attack*: Suppose that the adversary modifies the message $\{CID_i, X, r_i, h_1\}$ and sends it to the center C_j, where $CID_i = ID_i \oplus H(K_1||r_i)$, $h_1 = H(ID_i||ID_j||r_i||X||K_1)$, and $X = xP$. The center C_j could find the modification by checking the h_1 in Step 2 of the authentication phase. Using a similar method, two participants could find the modification of any messages. Therefore, our scheme could withstand the modification attack.
- *Man-in-the-Middle Attack*: From the above discussion, we know that our scheme provides mutual authentication between O_i and C_j. Hence, the proposed scheme could against the man-in-the-middle attack.
- *Known-key Security*: In our scheme, the session key is computed as $SK = H(yX||k_{ij})$ where $k_{ij} = H(k_i||K_2||r_i||r_j)$. It depends on the nonces $\{y, r_i, r_j\}$, and the generation of $\{y, r_i, r_j\}$ is independent in all sessions. Furthermore, the nonces are randomly selected and cannot be recovered from the protocol transcript. That is, the knowledge of one session key gives no advantage over the calculation of other session keys. Therefore, our scheme could provide known-key security.
- *Perfect Forward Secrecy*: In our scheme, the session key between O_i and C_j is computed using the session random number r_i, r_j, y: $SK = H(yX||k_{ij})$ where $k_{ij} = H(k_i||K_2||r_i||r_j)$. Even if all participants' secret keys k_i have been compromised, it is computationally infeasible for the adversary $\mathcal{A}$ to obtain the previous session keys without r_i, r_j, and y. This is because the ECDL problem is hard to solve and the collision-resistant property of the one-way hash function. Therefore, the proposed scheme could provide perfect forward secrecy.
- *Anonymity*: In our scheme, the identity of O_i is included in $CID_i = ID_i \oplus H(K_1||r_i)$ of the message 1, where $K_1 = xP_{pub} = kX$. To obtain the real identity of ID_i, the adversary $\mathcal{A}$ requires x or k to compute K_1. Without knowledge of x or k, the adversary $\mathcal{A}$ has no ability to compute the identity ID_i except he/she can solve ECDL or CDH problems.
- *Mutual Authentication*: From the goals $G_2 \sim G_5$ in Subsection V-A, we can get that O_i and C_j mutually authenticate each other in our scheme. Therefore, the proposed scheme could provide mutual authentication between O_i and C_j.

VI. Evaluation

In this section, we conduct experiments to demonstrate the efficiency of EmIr-Auth. The experiment setup is composed of a smartphone (Huawei P30 Pro) with a high-resolution camera and a desktop computer. The hardware platform is Intel Core CPU i7-7700K 4.2GHz and 8GB DDR4-2133 RAM.

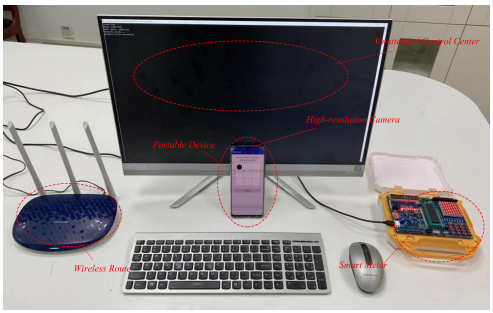


Fig. 5. The testbed in smart grid. From left to right are wireless router, portable device with a high-resolution camera, unattended control center, and the smart meter.

A. The Smart Grid Testbed

The proposed scheme is made into a mobile application and deployed at the portable device and hardware. From left to right in Fig. 5 there are wireless router, portable device, unattended control center and the smart meter. We connect the portable device and the hardware with wireless router to simulate operator and unattended control center in smart grid. The single-chip microcomputer on the right is used to simulate a smart meter. After the control center authenticates the operator through this scheme, the operator can read and control the smart meter through the control center for auditing or maintenance purposes.

B. Experiment of eye-movement trajectory capture and iris recognition

To demonstrate the feasibility of integration of eye-movements capture and iris recognition, we carry out a series of experiments.

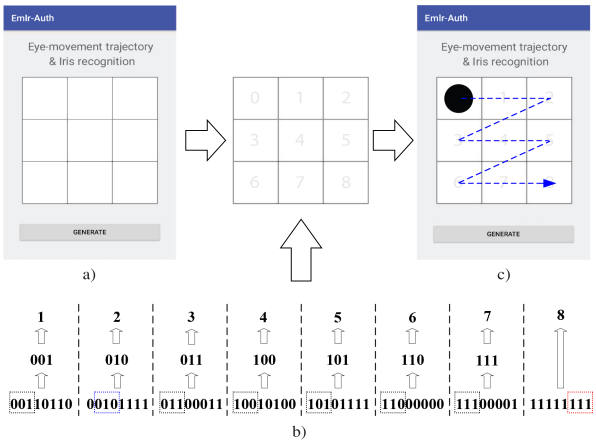


Fig. 6. Eye-movement stimulus. After the subjects click the GENERATE button, eight solid circles would sequentially appear in the $\mathbf{3} \times \mathbf{3}$ grids, and each solid circle would exist for one second. Note that the initial position of the solid circle start at grid 0.

Firstly, we develop a mobile application which contains 3×3 grids. These grids are marked using numbers 0 to 8 respectively(see Fig. 6a).

And then, the 64 bits value, for simplicity, are generated by the mobile application (not transfer from the control center). We divide the 64 bits value into eight groups such that each group contains eight bits. Furthermore, we use a three-slot sliding window to select three bits from each group and convert it to a decimal number. Note that if the three bits selected in a group are the same as the values selected in the previous group, the sliding window would move one bit to the right to re-select three bits. If five times slide to the right still cannot find different three bits, this group would be marked as a decimal number 8. Subsequently, a decimal sequence is obtained. We illustrate our points with an example shown in Fig. 6b). Finally, according to the decimal sequence, solid circles are sequentially appeared in the grids.

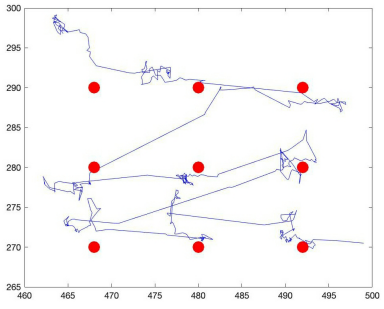
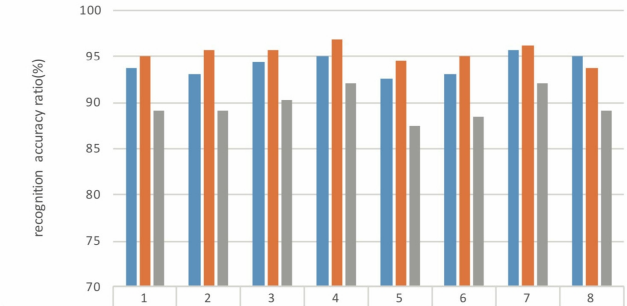


Fig. 7. Gaze saccade path. Points of gaze are marked as the blue path, while appeared circles are marked as red solid circles.

We perform experiments with eight subjects, including four females and four males in the age between 22-24 years. The smartphone and the camera are placed at 40cm ahead of the subject. Each subject observes the screen of the smartphone, keeping their head stable as much as possible, and follow the sequential appeared circles. The camera would record the whole process. Then we get the coordinates of eye gaze at smaller intervals and mark them with the reference sequential appeared circles on the screen, as shown in Fig. 7. In accordance with the method of Section IV-D, we obtain the eye-movement trajectory and randomly select a frame of Iris image from the recorded video. All the experimental data are transferred



	1	2	3	4	5	6	7	8
Eye-movement	93.75	93.13	94.38	95	92.5	93.13	95.63	95
Iris	95	95.63	95.63	96.88	94.48	95	96.25	93.75
Average	89.06	89.06	90.26	92.04	87.39	88.47	92.04	89.06

Fig. 8. Recognition accuracy ratio. The blue and orange column represent the recognition rate of eye-movement and iris experiment respectively, and the gray column represents the recognition rate of our scheme.

to the desktop computer for analyzing and recognizing based on the MATLAB platform. We apply the LibSVM package [30] to identify the iris image, the penalty factor is empirically set to 1.0. In the experiment, 300 iris images are collected from each subject as a training data set. And then, each subject performs 160 times of experiments. Thus, 160 eye-movement trajectories and 160 iris images are collected from each subject.

Recognition results of the eye-movement detection algorithm are compared with the pre-computed templates for acquiring the classification accuracy ratio. If the output result is the same as the pre-computed template, we consider that it is a success validation; otherwise, it is failing. Similarly, we calculate the recognition ratio of iris identification algorithm by comparing the output with data label. If they are the same, the classification is turned out to be true; otherwise, it is wrong. According to the above rules, the accuracy of iris and eye-movement and the scheme experiments are shown in Fig. 8.

C. Performance Comparison

In this section, we evaluate the computational costs of our scheme and compare it with the related schemes [26]–[29]. As shown in Table II, the notations T_h and T_s denote the time for executing a one-way hash operation or a symmetric key encryption/decryption operation respectively. And let T_m and T_a be the time for executing a scalar multiplication or a point addition operation of an elliptic curve. We carry out a simulation of these operations with the latest Miracl library. The simulation result shows that one hash operation requires for 0.019 ms (millisecond), one block encryption/decryption requires for 0.233 ms, one scalar multiplication on elliptic curve requires for 2.037 ms, and one point addition on elliptic curve requires for 0.451 ms. Accordingly, we evaluate the estimated running time of the related schemes in each session.

In Table III, we summarize the statistics of communication cost of related schemes in the registration phase, login&authentication phase, and password change phase respectively. Note that the password change phase just needs to be performed only when the user needs to change his/her password. The login&authentication phase should be executed every time. For consistency and simplicity, we assume that the length of the identity or the random number are 32 bits, the output size of a hash function or block encryption/decryption(e.g. SHA-1 and AES-256) are 160 bits and 256 bits respectively. In addition, we assume that the length of an elliptic curve point is 160 bits.

According to Table II, we know the proposed scheme has higher computational overhead than Khan et al.'s scheme [28] and Li et al.'s

TABLE II
COMPUTATIONAL COST COMPARISON

	[26]	[27]	[28]	[29]	Ours
Operator	$4T_s + 8T_h$	$2T_m + 6T_a$	$6T_h$	$2T_m + 2T_s + 5T_h$	$2T_m + 2T_s + 7T_h$
Control center	$1T_m + 10T_s + 10T_h$	$2T_m + 6T_a + 2T_h$	$7T_h$	$2T_m + 2T_s + 6T_h$	$1T_m + 2T_s + 7T_h$
Total	$1T_m + 14T_s + 18T_h$	$4T_m + 12T_a + 2T_h$	$13T_h$	$4T_m + 4T_s + 11T_h$	$3T_m + 4T_s + 14T_h$
Estimated execute time	5.641ms	13.598ms	0.247ms	9.289ms	7.252ms

TABLE III
COMMUNICATIONAL COST COMPARISON

Phase	[26]	[27]	[28]	[29]	Ours
Registration phase	704 bits	1248 bits	800 bits	832 bits	352 bits
Login&authentication phase	1156 bits	2496 bits	1152 bits	1344 bits	1600 bits
Password change phase	512 bits	–	416 bits	958 bits	–
Total without password change	1860 bits	3744 bits	1952 bits	2176 bits	1952 bits
Total	2372 bits	3744 bits	2368 bits	3134 bits	1952 bits

scheme [26]. But compared with Yeh et al.'s scheme [27] and Wu et al.'s scheme [29], the computational overhead of our scheme has great advantages. Meanwhile, in Table IV, we can see that Li et al.'s scheme cannot withstand stolen verifier attack and provide perfect forward secrecy. Yeh et al.'s scheme has many security flaws. Khan et al.'s scheme cannot resist to user impersonation attack and provide anonymity. And Wu et al.'s scheme cannot against insider attack. Taken security features into consideration, it is worth to achieve a high-security level with a slightly increased computational cost. Furthermore, as shown in Table III, we can see that our scheme outperforms the related schemes in terms of total communication cost. Without regard to the password change phase, our scheme costs only 92 bits more than the smallest one, which will not increase the burden of network communication.

D. Security Functionality Comparison

TABLE IV
SECURITY FUNCTIONALITIES COMPARISON

	[26]	[27]	[28]	[29]	Ours
Replay attack	√	√	√	√	√
Privileged insider attack	√	√	√	×	√
Stolen verifier attack	×	√	√	√	√
Modification attack	√	√	√	√	√
User impersonation attack	√	×	×	√	√
Man-in-the-middle attack	√	×	√	√	√
Known-key security	√	—	√	√	√
Perfect forward secrecy	×	×	√	√	√
Anonymity	√	—	×	√	√
Mutual authentication	√	√	√	√	√
Session key agreement	√	—	√	√	√
Dependence on the smart card	√	√	√	√	×

In the comparison of functionalities, we focus on the security against replay attack, insider attack, stolen verifier attack, modification attack, user impersonation attack, man-in-the-middle attack, known key attack, and anonymity, perfect forward secrecy, mutual authentication and session key agreement, and dependence on the smart card. We use $\surd$, $\times$ and — to denote that the scheme satisfies, does not satisfy and has no relation to the corresponding functionalities.

As shown in Table IV, the related schemes [26]–[29] have some security flaws and cannot satisfy all the functionalities. Li et al.'s scheme [26] cannot provide perfect forward secrecy and against stolen verifier attack. Yeh et al.'s scheme [27] suffers from user impersonation and man-in-the-middle attacks and fails to achieve perfect forward secrecy. Khan et al.'s scheme [28] ignores the anonymity and user impersonation attack. Wu et al.'s scheme [29] satisfies most of the security functionalities, however, it suffers from insider attack. Based on the above analysis and table, our solution achieves all these security functionalities without dependence on smart card.

VII. Conclusion

In this paper, we proposed a novel biometrics-based remote authentication scheme on the operator's portable devices of smart grid. The core idea of our approach was to combine human eye-movement trajectory together with iris recognition. Additional biometric sensors and smart-cards were not required except for a high-resolution camera. Informal security analysis, using BAN logic, had proven that our scheme provides secure authentication and can withstand various known attacks. Furthermore, our scheme maintained high efficiency in terms of computational as well as communication cost. Therefore, the proposed scheme was more suitable for the operators using remote authentication in smart grid. Considering the limitation of the resources of the industrial control system, we will further reduce the computation and communication overhead of our scheme at the operator's side. On the other hand, we will further improve the strategy of combining eye-movement trajectory and iris recognition.

References

[1] Z. Ma, Y. Liu, X. Liu, J. Ma, and F. Li, "Privacy-preserving outsourced speech recognition for smart iot devices," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[2] J. Ning, J. Xu, K. Liang, F. Zhang, and E. Chang, "Passive attacks against searchable encryption," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 789–802, March 2019.

[3] H. Wang, J. Ning, X. Huang, G. Wei, G. S. Poh, and X. Liu, "Secure fine-grained encrypted keyword search for e-healthcare cloud," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2019.

[4] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy*, vol. 7, no. 3, pp. 75–77, 2009.

[5] J. Ning, Z. Cao, X. Dong, K. Liang, H. Ma, and L. Wei, "Auditable σ -time outsourced attribute-based encryption for access control in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 94–105, Jan 2018.

[6] H. Gunasinghe and E. Bertino, "Privbiomtauth: Privacy preserving biometrics-based and user centric protocol for user authentication from mobile phones," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 1042–1057, 2017.

[7] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021–2040, 2003.

[8] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," *IEEE transactions on information forensics and security*, vol. 1, no. 2, pp. 125–143, 2006.

[9] P. K. Dhillon and S. Kalra, "Secure multi-factor remote user authentication scheme for internet of things environments," *International Journal of Communication Systems*, vol. 30, no. 16, p. e3323, 2017.

[10] M. Sajjad, S. Khan, T. Hussain, K. Muhammad, A. K. Sangaiah, A. Castiglione, C. Esposito, and S. W. Baik, "Cnn-based anti-spoofing two-tier multi-factor authentication system," *Pattern Recognition Letters*, 2018.

[11] Z. Ma, Y. Liu, X. Liu, J. Ma, and K. Ren, "Lightweight privacy-preserving ensemble classification for face recognition," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5778–5790, June 2019.

[12] A. Alzubaidi and J. Kalita, "Authentication of smartphone users using behavioral biometrics," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1998–2026, 2016.

[13] A. Buriro, B. Crispo, and M. Conti, "Answerauth: A bimodal behavioral biometric-based user authentication scheme for smartphones," *Journal of information security and applications*, vol. 44, pp. 89–103, 2019.

[14] K. Tse and K. Hung, "Behavioral biometrics scheme with keystroke and swipe dynamics for user authentication on mobile platform," in *2019 IEEE 9th Symposium on Computer Applications Industrial Electronics (ISCAIE)*, April 2019, pp. 125–130.

[15] P. Kasprowski and J. Ober, "Eye movements in biometrics," in *International Workshop on Biometric Authentication*. Springer, 2004, pp. 248–258.

[16] C. Holland and O. V. Komogortsev, "Biometric identification via eye movement scanpaths in reading," in *2011 International joint conference on biometrics (IJCB)*. IEEE, 2011, pp. 1–8.

[17] Y. Zhang, W. Hu, W. Xu, C. T. Chou, and J. Hu, "Continuous authentication using eye movement response of implicit visual stimuli," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 1, no. 4, p. 177, 2018.

[18] K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon, and H. F. Ahmad, "A lightweight message authentication scheme for smart grid communications in power sector," *Computers & Electrical Engineering*, vol. 52, pp. 114–124, 2016.

[19] X. Li, J. Niu, S. Kumari, F. Wu, and K.-K. R. Choo, "A robust biometrics based three-factor authentication scheme for global mobility networks in smart city," *Future Generation Computer Systems*, vol. 83, pp. 607–618, 2018.

[20] N. Kumar, G. S. Aujla, A. K. Das, and M. Conti, "Eccauth: Secure authentication protocol for demand reponse management in smart grid systems," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2019.

[21] W. Stallings and M. P. Tahiliani, *Cryptography and network security: principles and practice*. Pearson London, 2014, vol. 6.

[22] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *International conference on the theory and applications of cryptographic techniques*. Springer, 2004, pp. 523–540.

[23] B. Borschinger and M. Johnson, "A particle filter algorithm for bayesian wordsegmentation," *Proceedings of the Australasian Language Technology Association Workshop 2011*, pp. 10–18, 2011, version archived for private and non-commercial use with the permission of the author/s and according to publisher conditions. For further rights please contact the publisher.

[24] J.-G. Ko, Y.-H. Gil, J.-H. Yoo, and K.-I. Chung, "A novel and efficient feature extraction method for iris recognition," *ETRI journal*, vol. 29, no. 3, pp. 399–401, 2007.

[25] R.-E. Fan, K.-W. Chang, C.-J. Hsieh, X.-R. Wang, and C.-J. Lin, "Liblinear: A library for large linear classification," *Journal of machine learning research*, vol. 9, no. Aug, pp. 1871–1874, 2008.

[26] X. Li, W. Qiu, D. Zheng, K. Chen, and J. Li, "Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards," *IEEE Transactions on industrial electronics*, vol. 57, no. 2, pp. 793–800, 2010.

[27] H.-L. Yeh, T.-H. Chen, K.-J. Hu, and W.-K. Shih, "Robust elliptic curve cryptography-based three factor user authentication providing privacy of biometric data," *IET Information Security*, vol. 7, no. 3, pp. 247–252, 2013.

[28] M. K. Khan, S. Kumari, and M. K. Gupta, "More efficient key-hash based fingerprint remote authentication scheme using mobile device," *Computing*, vol. 96, no. 9, pp. 793–816, 2014.

[29] F. Wu, L. Xu, S. Kumari, and X. Li, "A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks," *Computers & Electrical Engineering*, vol. 45, pp. 274–285, 2015.

[30] C.-C. Chang and C.-J. Lin, "Libsvm: A library for support vector machines," *ACM Trans. Intell. Syst. Technol.*, vol. 2, no. 3, pp. 27:1–27:27, May 2011. [Online]. Available: http://doi.acm.org/10.1145/1961189.1961199