IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 24, 2019, accepted October 17, 2019, date of publication October 25, 2019, date of current version November 8, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2949649

An Improved Authentication Protocol Using Smart Cards for the Internet of Things

CAO SHOUQI, LIU WANRONG, CAO LILING, HE XIN, AND JI ZHIYONG
Department of Engineering Science and Technology, Shanghai Ocean University, Shanghai 201306, China

Corresponding author: Cao Liling (llcao@shou.edu.cn)

This work was supported in part by the 2017 "Innovative Action Plan" of Science and Technology Commission of Shanghai Municipality under Grant 17050502000, in part by the 2017 Cooperative Project on Industry-Academy-Research of Shanghai Lingang Administrative Committee (Key Technology Research and Demonstration Line Construction of Advanced Laser Intelligent Manufacturing Equipment), and in part by the Doctoral Scientific Research Foundation of Shanghai Ocean University under Grant A2-0203-00-100361.

ABSTRACT With the continuous development of IoT (Internet of Things) technology, IoT has become a typical representative of the development of new generation of information technology. The IoT allows people to use our data and computing resource anytime and everywhere. In the context of the IoT, the security of the vast amount of data generated by smart devices is one of the biggest concerns. To meet the challenge, the user authentication scheme in IoT should ensure the essential security performance protection and low computing costs. A authentication protocol preserving user anonymity was proposed by Nikooghadam et al. in 2017. In this paper, we further analyze the security of Nikooghadam et al.'s protocol and propose an improved anonymous authentication protocol for IoT. We use the timestamp mechanism and rely on CDH (Computational Diffie-Hellman) problem to improve security primarily. The security of the proposed protocol is verified using BAN logic and the performance comparison and efficiency analysis are carried out. The results show that our improved protocol has higher security with little more computation cost.

INDEX TERMS Anonymous, authentication, Internet of Things, privacy.

I. INTRODUCTION

Internet of things (IoT) is the extension and expansion of the Internet. Since the first mention of IoT concept in 1999 by Ashton, IoT has become a typical representative of the development of a new generation of information and communication technologies, which has profoundly changed human production and lifestyle, such as communication through the Internet, online shopping, online games, electronic medical record systems [1]. Hence in 2012, International Telecommunication Union (ITU-T) defined IoT as "a global infrastructure for the information society, enabling advanced ser- vices by interconnecting virtual and physical things based on existing and evolving interoperable information and communication technologies [2], [3]." The ubiquitous smart society, in which the combining of the data from smart devices and various sensors enables intelligent communication, is being built in the form of the smart city [4], [5]. But the components made by different sensors limit the capacity of IoT and cannot manage the large amounts of data generated by connected devices. A powerful technology, such as a cloud, is needed to access information from anywhere. Currently, many cloud services are available from public and private servers in geographic locations. Often, public cloud platforms are essential for all users and private cloud open services because they are not accessible without authorization. Cloud computing [6], [7] plays a key role in the implementation of IoT, but cloud security is an important issue. An attacker could compromise the security of the system and illegally access user data. For example, when a doctor is a remote user and a patient communicates through IoT in the home or an attacker uses smartphones to lock or unlock doors from a distance, there will be a security risk. A variety of authentication protocols can be used to ensure information security. User authentication is required to enable user mobile devices to access various services. The user identifier can be relied upon to verify that the user is legitimate in the authentication. Identifiers such as passwords are associated with user privacy and seriously affect user security when compromised. Therefore, login and authentication requests for users who use identifiers to transfer to the public channel can easily become the target of an attacker. Due to this problem, it is necessary to

The associate editor coordinating the review of this manuscript and approving it for publication was Jagruti Sahoo.

protect the user's anonymity, intractability and other related information problems in the authentication process [8]. At the earliest, only password authentication is used [9]. However, with the continuous development of the field, especially the leakage of sensitive information such as medical care and bank branch information. The researchers found that can no longer rely on password to ensure that the network information security. So the remote user authentication scheme based on smart card has become a hotspot in the field of security protocols [10]. Chang and Wu [11] proposed the first authentication scheme that combines smart cards and passwords to protect security-critical services such as online banking and e-health. But most of the early two-factor [12], [13] security protocols relied heavily on the tamper-proof features [14]–[16] of smart cards [17]. The research results on side-channel attacks reveal that smart cards can no longer be fully trusted once in the hands of a attacker. They can be tampered by power analysis [18]. In 2016, Das [19] proposed a new three-factor [20] user authentication scheme to overcome the disadvantages in Jiang er al.'s [21] two-factor user authentication scheme. In particular, the biometric-based three- factor authentication method has become a key technology for solving the certification problem. Since biometrics represent unique human characteristics, such as iris, fingerprint, and hand geometry, it has the following advantages [22]: (1) Biometric keys cannot be lost or forgotten; (2) it is extremely difficult to forge or distribute biometric keys; (3) biometric keys maintain uniqueness; and (4) it is difficult to guess biometric keys. Thus, it is obvious that the biometric-based user authentication methods are more secure and reliable than the traditional password-based user authentication methods. However, when applying biometric-based authentication technology in practice, it is not a simple matter, and some considerations need to be paid attention to. As mentioned earlier, biometrics are a characteristic of humans, so it cannot be altered like a password. Therefore, if it is leaked, it will lead to serious privacy problems [23]. The original biometric template cannot be directly exported. In this regard, many authentication schemes based on biometric have been proposed using techniques for extracting user's biometrics into a random value such as a bio-hash or a fuzzy extractor [24], [25]. With further development, the concept of dynamic identity [26]–[28] was developed. Scholars have done a lot of research on remote user authentication scheme based on dynamic identity. How to ensure the security of users' privacy information has become an important problem restricting the development of communication network technology and anonymous authentication technology has become an effective strategy to solve the problem of communication network security.

Chang *et al.* [29] proposed untraceable dunamic-identity-based remote user authentication scheme in 2013. In 2014, Kumari *et al.* [30] proved that the scheme proposed by Chang et al. has serious security flaws. They illustrate that Chang et al.'s scheme violates the purpose of dynamic-identity contrary to authors' claim. To overcome the security loopholes, Kumari et al. proposed an improved remote user authentication scheme. In 2016, Wang *et al.* [17] analysed the scheme of Kumari et al. and found it is susceptible to de-synchronization attack, not attain forward secrecy. In the same year, Chen et al. claimed that the Kumari et al. scheme is vulnerable to stolen smart card attack and failed to ensure forward secrecy, user anonymity. In 2018, Limbasiya *et al.* [31] showed that the scheme proposed by Kumari et al. is vulnerable to password-guessing attack and masquerade attack. In 2017, Nikooghadam *et al.* [32] reviewed the scheme of Kumari et al. and found it failed to resist password guessing attacks and user anonymity attacks. In order to overcome the weaknesses of Kumari et al. scheme, Nikooghadam et al. then proposed an improved scheme which protects user anonymity. Their security analysis demonstrates that the proposed protocol resists various security attacks and provides user anonymity. However, Limbasiya et al. cryptanalyzed Nikooghadam et al.'s scheme and found it vulnerable to password-guessing attack, insider attack and modification attack. Limbasiya et al. then proposed an improved scheme in 2018. In the same year, Chandrakar and Om [33] claimed that the Nikooghadam et al.'s scheme is vulnerable to impersonation attack and privileged insider attack. Additionally, the scheme does not provide forward secrecy, session key verification and biometric update phase. In 2018, Sharma and Kalra [34] investigated the scheme of Nikooghadam et al. and claimed that it is insecure to malicious attack, online password guessing attack, server spoofing attack and parallel session attack. And it does not provide forward secrecy. Nikooghadam et al.'s protocol have been studied and analyzed by lots of scholars. These improved protocols are not based on Nikooghadam et al.'s protocol. It is worth making improvements based on Nikooghadam et al.'s protocol framework. Our protocol is an improved authentication protocol using smart cards for the Internet of Things based on Nikooghadam et al.'s protocol framework. Our paper summarizes the previous analysis of Nikooghadam et al.'s protocol and makes a detailed analysis of what others only mentioned briefly, such as replay attack, privileged insider attack and password guessing attack. Then, we propose an improved protocol. In terms of protocol security analysis, there are three types of typical formal analysis methods: theorem proving, logical derivation, and modei detection. Burrows-Abadi-Needham logic (BAN logic) [35], [36] is a wide logic derivation method, so we analyze our protocol by BAN logic. Many scholars also use Automated Validation of Internet Security Protocols and Applications (AVISPA) [37] to analyze the security of the protocol. In addition, by integrating ''honeywords'', traditionally the purview of system security, with a ''fuzzy-verifier'', Wang et al. hits ''two birds'': it not only eliminates the long-standing security-usability conflict that is considered intractable in the literature, but also achieves security guarantees beyond the conventional optimal security bound [38]. For better balance between security and usability,

our protocol employs the techniques of ''fuzzy-verifier'' in the login phase. In the security analysis, we have shown that the proposed protocol could withstand well-known security attacks and provide the mutual authentication between the user and the server. Furthermore, the performance comparison among the proposed scheme and other schemes and total execution time comparison among discrete systems are carried out in Table 2 and Table 4. These analyses indicate that our protocol is more secure and little more computation cost.

II. REVIEW OF NIKOOGHADAM ET AL.'S SCHEME

Nikooghadamet al.'s protocol includes three phases: registration phase, login and authentication phase, and password changing phase. The employed symbols in the proposed protocol are defined in Table 1.

TABLE 1. Notations.

Symbol	Definition
U_i	A user
ID_i	the identity of U_i
PW_i	The password for U_i
n_0	A medium integer, $2^4 \le n_0 \le 2^8$
MID_i	The masked identity for U_i
MPW_i	The masked password for U_i
SK	The session key between the user and the server
$\oplus$	The exclusive-OR operation(XOR)
$\|\|$	The concatenation operation
$E_k(\cdot)$ / $D_k(\cdot)$	The symmetric encryption/decryption with the key k
$h(\cdot)$	A secure one-way hash function
SC_i	The smart card for U_i
U_i	A user
ID_i	the identity of U_i

A. REGISTRATION PHASE

In the registration phase, the following steps are performed in order to issue a smart card that the user U_i employs it during login the server.

B. LOGIN AND AUTHENTICATION PHASE

In this phase, the user and server authenticate each other and then they agree on a session key. After the authentication and key agreement, the user and the server are able to encrypt/authenticate their messages using the agreed session key. Figure 2 illustrates the login and authentication phase of the proposed protocol.

C. PASSWORD CHANGING PHASE

In this phase, When a user decides to change the password, he/she inserts his/her smart card into the card reader and enters his/her identity and current password. Then the smart card works as follows:

Step1: This step is the same as Step 1 of the login phase of Nikooghadam et al.'s protocol.

Step2: This step is the same as Step 2 of the login phase of Nikooghadam et al.'s protocol.

Step3: When the challenge message $\{M_2\}$ is received from the server, the smart card decrypts M_2 using A_i and obtains the values of RN_i, MID_i^{New}, RN_s, *and* ID_i. Then, the smart card checks out equality of the received and the transmitted values of ID_i *and* RN_i. If their equality is verified, the smart card requests the user to enter his/her new password. When the user enters his/her new password PW_i^{New}, the smart card calculates $B_i^{New} = B_i \oplus h(ID_i||r||PW_i) \oplus h(ID_i||r||PW_i^{New}) = A_i \oplus h(ID_i||r||PW_i) \oplus h(ID_i||r||PW_i) \oplus (ID_i||r||PW_i^{New}) = A_i \oplus h(ID_i||r||PW_i^{New}) = h(ID_i||x) \oplus h(ID_i||r||PW_i^{New})\pi$. Finally, the smart card replaces B_i^{New} and MID_i^{New} with B_i and MID_i, respectively.

III. WEAKNESSES OF NIKOOGHADAM ET AL.'S SCHEME

A. WEAKNESS 1: REPLAY ATTACK

Timestamps have not been used by U_i to change M_2 or by the server to verify the response M_3 during authentication. This would cause the validation period of these message (M_2, M_3) to be endless. If A intercepts M_2, then she/he can stop or delay it longer. Consequently, if U_i asks for resources, A can use this request later to obtain unauthorized services, as the server cannot identify that a request has been sent by a legitimate user or that A has sent requests illegitimately. Such as A can request the server to calculate SK.

B. WEAKNESS 2: PRIVILEGED INSIDER ATTACK AND OFFLINE PASSWORD GUESSING ATTACK

Nikooghadam et al.'s protocol is not adequate to secure against insider threat:

Step1: Insider A knows the $U_i's$ identity ID_i from the received registration request $\{ID_i, MPW_i\}$ where $MPW_i = h(ID_i||r||PW_i)$. And A can get the message $\{B_i, MID_i, r, E_{key}(\cdot)/D_{key}(\cdot), h(\cdot)\}$ stored in the smart card.

Step2: Next, A guesses a password PW_i' from a dictionary.

Step3: A computes $A_i' = h(ID_i||r||PW_i')$.

Step4: $A_i = B_i \oplus MPW_i$, if $A_i' = A_i$ is true, A obtains the correct PW_i of the U_i. Otherwise, A compiles Step2 to 4, until the correct PW_i is not obtained.

C. WEAKNESS 3: KNOWN SESSION SPECIFIC TEMPORARY INFORMATION

If A steals or finds the smart card of U_i, then A can extract $\{B_i, MID_i, r, E_{key}(\cdot)/D_{key}(\cdot), h(\cdot)\}$ from SC_i. As a co-worker in the same organization. A has knowledge of MPW_i as well as r (from SC_i). A can compute $A_i = B_i \oplus MPW_i = A_i^*$. Next, if A knows the ephemeral secrect information such as a random number, then A can evaluate a session key. The Nikooghadam et al.'s protocol's session key is

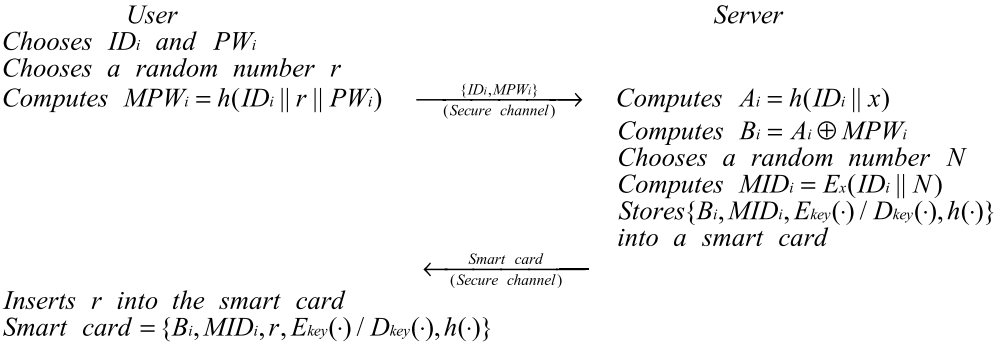


FIGURE 1. Registration phase of the proposed protocol.

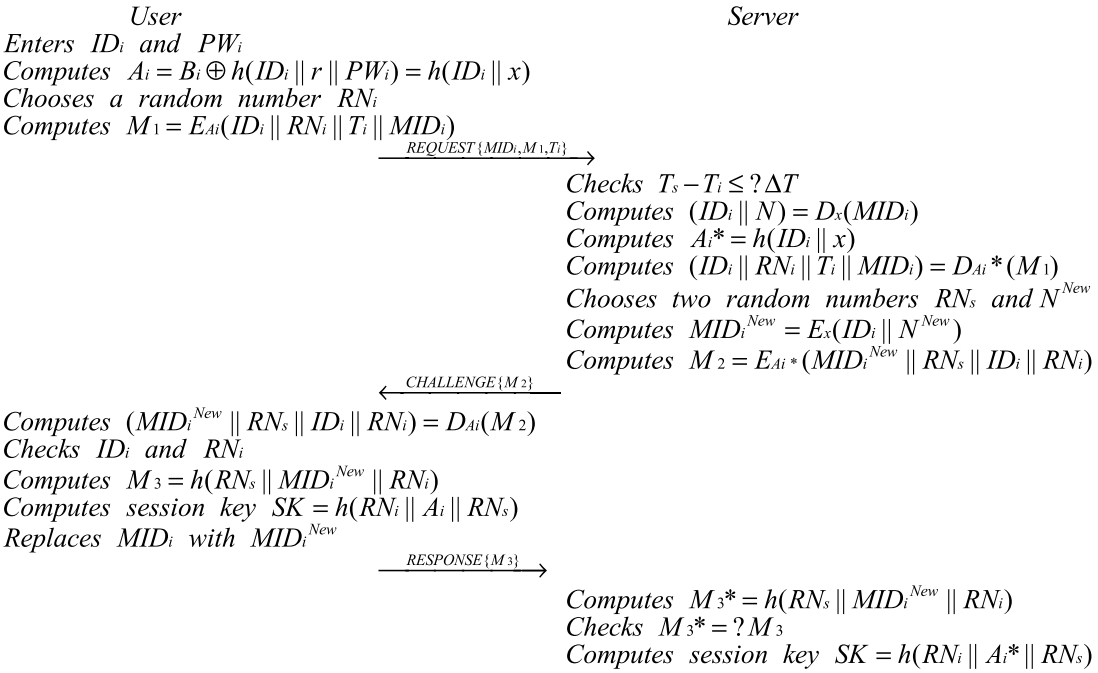


FIGURE 2. Login and authentication phase of the proposed protocol.

$SK = h(RN_i||A_i^*||RN_s)$, where RN_i and RN_s are random numbers produced by U_i and server, respectively. If these random numbers are disclosed to A, then A can compute the SK. Therefore, the Nikooghadam et al.'s protocol cannot defend against known key temporary information attacks.

D. WEAKNESS 4: SERVER SPOOFING ATTACK

An intruder exploits recorded information of authorized users by counterfeiting as a server. To successfully impersonate as a legitimate server and forge a valid response message. A acquires the information $\{B_i, MID_i, r, E_{key}(\cdot)/D_{key}(\cdot), h(\cdot)\}$ from the smart card. As a co-worker in the same organization, A has knowledge of ID_i and MPW_i as well as r. Then, A computes $A_i = B_i \oplus MPW_i$. A computes $D_{Ai}(M_1) = (ID_i||RN_i||Ti||MID_i)$ and intercepts the log-in message $\{MID_i, M_1, Ti\}$. Timestamps have not been used by U_i to challenge M_2 or by the server to verify the response M_3 during authentication. A chooses random number RN' and computer $M_2' = E_{Ai}(MID_i||RN_s'||ID_i||RN_i)$. Finally, A sends $\{M_2'\}$ to user. A can act as the legal server.

E. WEAKNESS 5: USER IMPERSONATION ATTACK

In this threat, A acts as a legal U_i after generating the $U_i's$ correct log-in message. The Nikooghadam et al.'s protocol cannot protect from user impersonation attack, which is illustrated as follows:

Step1: A acquiers the information $\{B_i, MID_i, r, E_{key}(\cdot)/D_{key}(\cdot), h(\cdot)\}$ from the smart card.
Step2: A intercepts the log-in message $\{MID_i, M_1, Ti\}$.
Step3: As a co-worker in the same organization, A has knowledge of ID_i and MPW_i as well as r. A can compute $A_i = B_i \oplus MPW_i$.
Step4: A creats a random nonce RN_i' and calculates $M_1' = E_{Ai}(ID_i||RN_i'||Ti||MID_i)$. After that, she/he sends the log-in request message $\{MID_i, M_1', Ti\}$ to the server.

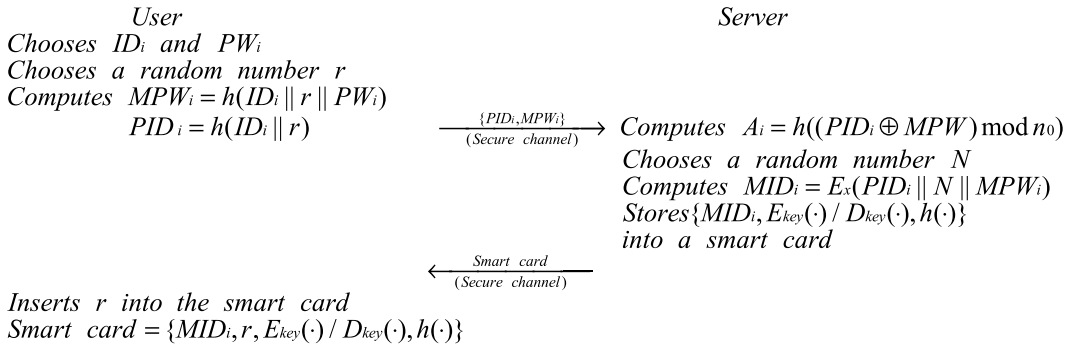


FIGURE 3. Registration phase.

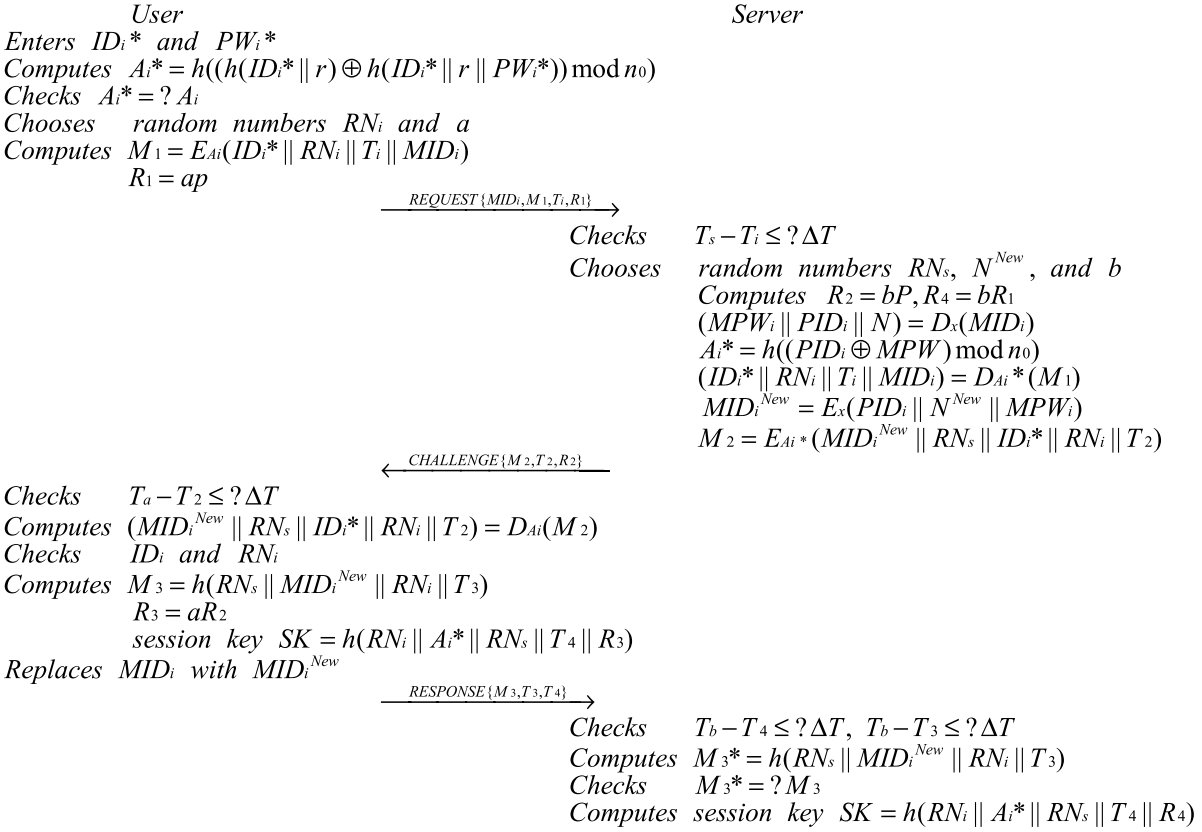


FIGURE 4. Login and authentication phase.

Step5: The server authenticates the message $\{MID_i, M_1', Ti\}$ as valid owing to the true ID_i. A can act as the legal U_i.

IV. PROPOSED PROTOCOL

In this section, we propose a secure authentication and key agreement protocol to overcome the weaknesses of Nikooghadam et al.'s protocol. The proposed protocol includes four phases: registration phase, login phase, authentication phase, and password change phase. The employed symbols in the proposed protocol are defined in Table 1.

A. REGISTRATION PHASE

In this phase, a user can register with the server. When the registration process is completed, the user obtains a personalized smart card from the server. The user's private information that is required for the next phase will save in the smart card. The registration process is illustrated in Fig. 3.

B. LOGIN AND AUTHENTICATION PHASE

A legal user can access to the services of the server when inserts the smart card into a card reader and enters identity, and password. The registration process is illustrated in Fig. 4.

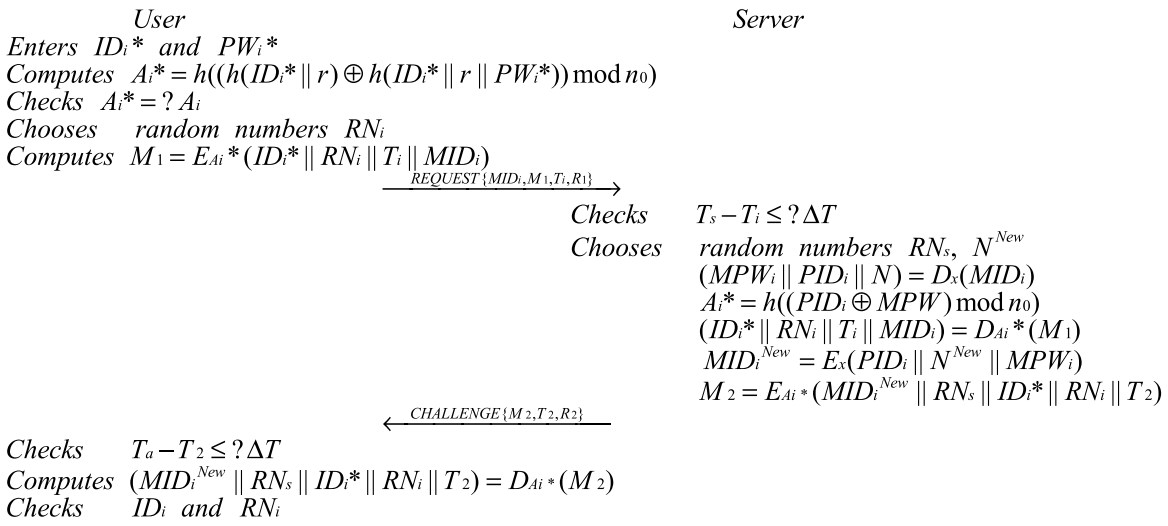


FIGURE 5. Password changing phase.

C. PASSWORD CHANGING PHASE

If $ID_i{}^*$ and RN_i are verified, the smart card requests the user to enter new password. When the user enters his/her new password PW_i^{New}, the smart card calculates $A_i{}^* = h((h(ID_i{}^*||r) \oplus h(ID_i{}^*||r||PW_i{}^*)) \bmod n_0)$. Finally, the smart card replaces A_i^{New} and MID_i^{New} with A_i and MID_i, respectively.

V. SECURITY ANALYSIS

In this section, the security analysis of the proposed scheme is presented. The analysis confirms that the proposed scheme is resistant against the all the major network attacks.

A. REPLAY ATTACK

Timestamps have been used by U_i to change M_2 and by the server to verify the response M_3 during authentication. If A intercepts M_2, she/he cannot stop or delay it longer. If U_i asks for resources, A cannot use this request later to obtain unauthorized services, as the server can identify that a request has been sent by a legitimate user or that A has sent requests illegitimately. Hence, we can say that the proposed system is secure against replay attack.

B. PRIVILEGED INSIDER ATTACK AND OFFLINE PASSWORD GUESSING ATTACK

The proposed scheme is adequate to secure against privileged insider attack and password guessing attack. In the registration phase, $PID_i = h(ID_i||r)$, ID_i is never sent in plaintext. Insider A cannot get the $U_i's$ identity ID_i from the received registration request $\{PID_i, MPW_i\}$ where $PID_i = h(ID_i||r)$. A cannot compute $A_i = h((h(ID_i||r) \oplus h(ID_i||r||PW_i)) \bmod n_0)$ without ID_i. A cannot make password guesses and the proposed protocol is secure.

C. KNOWN SESSION SPECIFIC TEMPORARY INFORMATION ATTACK

In the authentication phase, the proposed protocol uses the timestamp mechanism and Computational Diffie-Hellman to provide session specific information attack. The session key $SK = h(RN_i||A_i{}^*||RN_s||T_4||R_4)$, where RN_i and RN_s are generated freshly for each session. And the timestamp mechanism means the session message is not the latest. It is a computational difficult problem to guess abP provided aP and bP.

D. SERVER SPOOFING ATTACK

An intruder cannot exploit recorded information of authorized users by counterfeiting as a server. A acquires the information $\{MID_i, r, E_{key}(\cdot)/D_{key}(\cdot), h(\cdot)\}$ from the smart card. A does not have knowledge of ID_i as well as r. Because ID_i is never sent in plaintext. Timestamps have been used by U_i to challenge M_2. Therefore, A cannot send false information $\{M_2{}'\}$ to user and cannot act as the legal server.

E. USER IMPERSONATION ATTACK

A cannot calculate $M_1{}' = E_{Ai}{}^*(ID_i{}^*||RN_i{}'||Ti||MID_i)$ without the non-plaintext message ID_i. A cannot act as the legal U_i by sending the log-in request message $\{MID_i, M_1{}', Ti\}$ to the server. The anonymity of users is also realized to a certain extent. The proposed system is secure against user impersonation attack.

VI. AUTHENTICATION PROOF BASED ON BAN LOGIC

In this section, we use the BAN logic, which is a formal method for analyzing authentication protocols, to prove the correctness of the proposed protocol. This logic has some rules that are defined in the following.

The message-meaning rule:

$$\frac{P| \equiv P \xleftrightarrow{K} Q, \quad P \lhd \{X\}_K}{P| \equiv Q| \sim X}$$

The freshness rule:

$$\frac{P| \equiv \#(X)}{P| \equiv \#(X, Y)}$$

TABLE 2. Performance comparison among the proposed scheme and other schemes.

Performance	Kumari et al. 2014	Nikooghadam et al. 2017	Chaudhry et al. 2017	Wu et al. 2017	Chandrakar et al. 2018	Ours
F1	Yes	No	Yes	Yes	Yes	Yes
F2	No	No	Yes	Yes	Yes	Yes
F3	No	No	No	Yes	No	Yes
F4	Yes	No	No	Yes	Yes	Yes
F5	Yes	No	Yes	Yes	Yes	Yes
F6	Yes	No	Yes	Yes	Yes	Yes
F7	No	No	Yes	Yes	Yes	Yes
F8	No	No	Yes	No	Yes	Yes
F9	No	Yes	No	Yes	Yes	Yes
F10	Yes	No	Yes	Yes	No	Yes
F11	Yes	No	Yes	Yes	Yes	Yes
F12	Yes	No	Yes	Yes	No	Yes
F13	Yes	No	Yes	Yes	Yes	Yes
F14	No	Yes	No	Yes	Yes	Yes

F1: defend against impersonation attack; F2: defend against privileged attack; F3: facilitate forward secrecy; F4: facilitate session key verification; F5: facilitate biometric update phase; F6: malicious user attack; F7: password guessing attack; F8: stolen verifier attack; F9: provides user anonymity; F10: replay attack; F11: sever spoofing attack; F12: parallel session attack; F13: session specific temporary information attack ; F14: stolen smart card attack.

Nonce-verification rule:

$$\frac{P| \equiv \#(X), \quad P| \equiv Q| \sim X}{P| \equiv Q| \equiv X}$$

Jurisdiction rule:

$$\frac{P| \equiv Q \Rightarrow X, \quad P| \equiv Q| \equiv X}{P| \equiv X}$$

According to the procedure of the BAN logic, the proposed protocol must access the following goals:

$$Goal\ 1: \quad User| \equiv (User \overset{SK}{\longleftrightarrow} Server)$$
$$Goal\ 2: \quad Server| \equiv (User \overset{SK}{\longleftrightarrow} Server)$$

The proposed protocol is transformed to the idealized form as follows.

Message 1: $User \rightarrow Server$:
$(\{PID_i, N, MPW_i\}x, \{ID_i{}^*, RN_i, Ti, \{PID, N\}x\}A_i)$

Message 2: $Server \rightarrow User$:
$(\{MID_i^{New}, RN_s, ID_i{}^*, RN_i, T_2\}A_i)$

Message 3: $User \rightarrow Server$:
$(\{RN_s, RN_i, T_3\}_{MID_i^{New}}, T_3, T_4)$

We made the assumptions about the initial state of the proposed protocol.

$$H_1: \quad User| \equiv (User \overset{A_i}{\longleftrightarrow} Server)$$
$$H_2: \quad Server| \equiv (Server \overset{A_i}{\longleftrightarrow} User)$$
$$H_3: \quad User| \equiv \#(RN_i)$$
$$H_4: \quad Server| \equiv \#(RN_s)$$
$$H_5: \quad User| \equiv Server \Rightarrow (User \overset{SK}{\longleftrightarrow} Server)$$
$$H_6: \quad Server| \equiv User \Rightarrow (User \overset{SK}{\longleftrightarrow} Server)$$
$$H_7: \quad Server| \equiv (Server \overset{MID_i^{New}}{\longleftrightarrow} User)$$

Based on the BAN logic rules and the assumptions, we analyze the idealized form of the proposed protocol as follows.

According to the Message 1, we have:

$$R1: \quad Server \triangleleft (\{PID_i, N, MPW_i\}x, \{ID_i, RN_i, Ti, \{PID, N\}x\}A_i)$$

From H_7, R_1, we have:

$$R2: \quad Server| \equiv User| \sim (\{ID_i{}^*, RN_i, Ti, \{PID, N\}x)$$

According to the Message 2, we have:

$$R3: \quad User \triangleleft (\{MID_i^{New}, RN_s, ID_i{}^*, RN_i, T_2\}A_i)$$

From H_1, R_3, we have:

$$R4: \quad User| \equiv Server| \sim (MID_i^{New}, RN_s, ID_i{}^*, RN_i, T_2)$$

From H_3, R_4, we have:

$$R5: User| \equiv Server| \equiv (MID_i^{New}, RN_s, ID_i{}^*, RN_i, T_2)$$

From H_2, the session key $SK = h(RN_i||A_i{}^*||RN_s||T_4||R_3)$, and R_5, we have:

$$R6: \quad User| \equiv Server| \equiv (User \overset{SK}{\longleftrightarrow} Server)$$

From H_5, R_6, we have:

$$R7: \quad User| \equiv (User \overset{SK}{\longleftrightarrow} Server)$$

According to the Message 3, we have:

$$R8: \quad Server \triangleleft (\{RN_s, RN_i, T_3\}_{MID_i^{New}}, T_3, T_4)$$

From H_7, R_8, we have:

$$R9: \quad Server| \equiv User| \sim (\{RN_s, RN_i, T_3\}_{MID_i^{New}}, T_3, T_4)$$

From H_4, R_9, we have:

$$R10: \quad Server| \equiv User| \equiv (\{RN_s, RN_i, T_3\}_{MID_i^{New}}, T_3, T_4)$$

TABLE 3. Required cryptographic operations comparison with different schemes.

Schemes/Phase	Registration	Login	Authentication	Total
Kumari et al.	$5T_{\oplus} + 7T_{\Box} + 5T_{h(\cdot)}$	$10T_{\oplus} + 16T_{\Box} + 10T_{h(\cdot)}$	$3T_{\oplus} + 23T_{\Box} + 11T_{h(\cdot)}$	$18T_{\oplus} + 46T_{\Box} + 26T_{h(\cdot)}$
Nikooghadam et al.	$1T_{\oplus} + 4T_{\Box} + 2T_{h(\cdot)} + 1T_{E/D}$	$1T_{\oplus} + 6T_{\Box} + 2T_{h(\cdot)} + 1T_{E/D}$	$23T_{\Box} + 7T_{h(\cdot)} + 5T_{E/D}$	$2T_{\oplus} + 33T_{\Box} + 11T_{h(\cdot)} + 7T_{E/D}$
Chaudhry et al.	$2T_{\oplus} + 3T_{\Box} + 5T_{h(\cdot)}$	$4T_{\oplus} + 4T_{\Box} + 4T_{h(\cdot)}$	$2T_{\oplus} + 14T_{\Box} + 9T_{h(\cdot)} + 4T_{E/D}$	$8T_{\oplus} + 21T_{\Box} + 18T_{h(\cdot)} + 4T_{E/D}$
Wu et al.	$3T_{\oplus} + 6T_{\Box} + 4T_{h(\cdot)}$	$1T_{\oplus} + 5T_{\Box} + 1T_{h(\cdot)}$	$9T_{\oplus} + 34T_{\Box} + 15T_{h(\cdot)} + 2T_{E/D}$	$13T_{\oplus} + 45T_{\Box} + 20T_{h(\cdot)} + 2T_{E/D}$
Chandraker et al.	$2T_{\oplus} + 6T_{\Box} + 5T_{h(\cdot)}$	$4T_{\oplus} + 7T_{\Box} + 7T_{h(\cdot)}$	$4T_{\oplus} + 18T_{\Box} + 9T_{h(\cdot)}$	$10T_{\oplus} + 31T_{\Box} + 21T_{h(\cdot)}$
Ours	$1T_{\oplus} + 5T_{\Box} + 3T_{h(\cdot)} + 1T_{E/D}$	$1T_{\oplus} + 6T_{\Box} + 3T_{h(\cdot)} + 1T_{E/D}$	$30T_{\Box} + 5T_{h(\cdot)} + 4T_{E/D}$	$2T_{\oplus} + 38T_{\Box} + 10T_{h(\cdot)} + 6T_{E/D}$

$T_{h(\cdot)}$: Time to perform one-way hash function; $T_{E/D}$: Time to execute an encryption/decryption; $T_{||}$: Concatenated execution time ; $T_{\oplus}$: Time to perform an XOR primitive.

TABLE 4. Total execution time comparison among discrete systems.

Schemes/Phase	Registration	Login	Authentication	Total
Kumari et al.	0.0115ms	0.0230ms	0.0253ms	0.0598ms
Nikooghadam et al.	0.0092ms	0.0092ms	0.0391ms	0.0575ms
Chaudhry et al.	0.0015ms	0.0092ms	0.0391ms	0.0498ms
Wu et al.	0.0092ms	0.0023ms	0.0437ms	0.0552ms
Chandraker et al.	0.0115ms	0.0161ms	0.0207ms	0.0483ms
Ours	0.0115ms	0.0115ms	0.0299ms	0.0506ms

According to the session key $SK = h(RN_i||A_i^*||RN_s||T_4||R_3), H_1, R_{10}$, we have:

$$\text{R11:} \quad Server| \equiv User| \equiv (User \overset{SK}{\longleftrightarrow} Server)$$

From H_6, R_{11}, we have:

$$\text{R12:} \quad Server| \equiv (User \overset{SK}{\longleftrightarrow} Server)$$

VII. PERFORMANCE COMPARISON AND EFFICIENCY ANALYSIS

To evaluate the computational time analysis, we account $T_{h(\cdot)} \approx 0.0023ms$, $T_{E/D} \approx 0.0046ms$, $T_{||}$ and $T_{\oplus}$ require very little to perform and are not included in the total time calculation. According to the Table3 and Table4, our protocol provides more security features with the addition of a small amount of computation.

VIII. CONCLUSION

In this paper, we have cryptanalyzed Nikooghadam et al.'s scheme and found that it is vulnerable to various security threats, such as replay attack, privileged insider attack and password guessing attack, session specific temporary information attack, server spoofing attack, and user impersonation attack. In addition, we have designed an improved authentication protocol using smart cards for the Internet of things based on Nikooghadam et al.'s protocol framework. The proposed protocol uses the timestamp mechanism and relies on CDH (Computational Diffie-Hellman) problem to improve security primarily. We have used BAN logic, which validates that the proposed protocol could withstand well-known security attacks and provide the mutual authentication between the user and the server. The performance comparison and efficiency analysis indicate that our protocol is more secure and little more computation cost.

ACKNOWLEDGMENTS

The authors would like to thank and acknowledge the anonymous reviewers for their valuable comments.

REFERENCES

[1] P. Kumar, S. G. Lee, and H. J. Lee, "E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks," *Sensors*, vol. 12, no. 2, pp. 1625–1647, 2012.

[2] *Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks*, Standard Y.3000-Y.3499, ITU, Geneva, Switzerland, 2012, pp. 1–6.

[3] V. Rao and K. V. Prema, "Light-weight hashing method for user authentication in Internet-of-Things," *Ad Hoc Netw.*, vol. 89, pp. 97–106, Jun. 2019.

[4] J. Lambrechts and S. Sinha, *Microsensing Networks for Sustainable Cities* (Smart Sensors, Measurement and Instrumentation), vol. 18. 2016.

[5] S. M. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[6] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[7] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generat. Comput. Syst.*, vol. 25, no. 6, pp. 599–616, 2009.

[8] S. A. Chaudhry, M. S. Farash, H. Naqvi, S. Kumari, and M. K. Khan, "An enhanced privacy preserving remote user authentication scheme with provable security," *Secur. Commun. Netw.*, vol. 8, no. 18, pp. 3782–3795, 2015.

[9] J.-K. Jan and Y.-Y. Chen, "'Paramita wisdom' password authentication scheme without verification tables," *J. Syst. Softw.*, vol. 42, no. 1, pp. 45–57, 1998.

[10] H.-M. Sun, "An efficient remote use authentication scheme using smart cards," *IEEE Trans. Consum. Electron.*, vol. 46, no. 4, pp. 958–961, Nov. 2000.

[11] C.-C. Chang and T.-C. Wu, "Remote password authentication with smart cards," *IEE Proc. E—Comput. Digit. Techn.*, vol. 138, no. 3, pp. 165–168, May 1991.

[12] D. Wang, D. He, P. Wang, and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 4, pp. 428–442, Jul./Aug. 2015.

[13] G. Yang, D. S. Wong, H. Wang, and X. Deng, "Two-factor mutual authentication based on smart cards and passwords," *J. Comput. Syst. Sci.*, vol. 74, no. 7, pp. 1160–1172, Nov. 2008.

[14] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009.

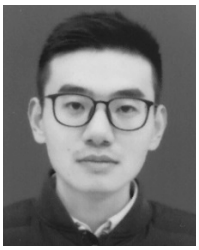
[15] I.-E. Liao, C.-C. Lee, and M.-S. Hwang, "A password authentication scheme over insecure networks," *J. Comput. Syst. Sci.*, vol. 72, no. 4, pp. 727–740, Jun. 2006.

[16] N. Mavrogiannopoulos, A. Pashalidis, and B. Preneel, "Security implications in kerberos by the introduction of smart cards," in *Proc. ACM Conf. Ubiquitous Comput.*, 2012, pp. 59–60.
[17] D. Wang, Q. Gu, H. Cheng, and P. Wang, "The request for better measurement: A comparative evaluation of two-factor authentication schemes," in *Proc. 11th ACM Asia Conf. Comput. Commun. Secur.*, 2016, pp. 475–486.
[18] J. Liu, Y. Yu, F.-X. Standaert, Z. Guo, D. Gu, W. Sun, Y. Ge, and X. Xie, "Small tweaks do not help: Differential power analysis of milenage implementations in 3G/4G USIM cards," in *Proc. ESORICS*, vol. 9326, 2015, pp. 468–480.
[19] A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," *Peer-Peer Netw. Appl.*, vol. 9, no. 1, pp. 223–244, Jun. 2014.
[20] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for Internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017.
[21] Q. Jiang, J. Ma, X. Lu, and Y. Tian, "An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks," *Peer-Peer Netw. Appl.*, vol. 8, no. 6, pp. 1070–1081, Jun. 2014.
[22] A. Chaturvedi, D. Mishra, S. Jangirala, and S. Mukhopadhyay, "A privacy preserving biometric-based three-factor remote user authenticated key agreement scheme," *J. Inf. Secur. Appl.*, vol. 32, pp. 15–26, Feb. 2017.
[23] T. Ignatenko and F. M. J. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 956–973, Dec. 2009.
[24] M. Wazid, A. K. Das, S. Kumari, X. Li, and F. Wu, "Provably secure biometric-based user authentication and key agreement scheme in cloud computing," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4103–4119, 2016.
[25] V. Odelu, A. K. Das, S. Kumari, X. Huang, and M. Wazid, "Provably secure authenticated key agreement scheme for distributed mobile cloud computing services," *Future Gener. Comput. Syst.*, vol. 68, pp. 74–88, Mar. 2017.
[26] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab, "An efficient OFDM-based encryption scheme using a dynamic key approach," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 361–378, Feb. 2019.
[27] M. Turkanovic and M. Holbl, "An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *Elektronika Elektrotechnika*, vol. 19, no. 6, pp. 109–116, 2013.
[28] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Proc. IEEE Int. Conf. Sensor Netw., Ubiquitous, Trustworthy Comput.*, Jun. 2006, p. 8.
[29] Y.-F. Chang, W.-L. Tai, and H.-C. Chang, "Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update," *Int. J. Commun. Syst.*, vol. 27, no. 11, pp. 3430–3440, 2013.
[30] S. Kumari, S. A. Chaudhry, F. Wu, X. Li, M. S. Farash, and M. K. Khan, "An improved smart card based authentication scheme for session initiation protocol," *Peer-Peer Netw. Appl.*, vol. 10, no. 1, pp. 92–105, Jan. 2017.
[31] T. Limbasiya, M. Soni, and S. K. Mishra, "Advanced formal authentication protocol using smart cards for network applicants," *Comput. Electr. Eng.*, vol. 66, pp. 50–63, Feb. 2018.
[32] M. Nikooghadam, R. Jahantigh, and H. Arshad, "A lightweight authentication and key agreement protocol preserving user anonymity," *Multimedia Tools Appl.*, vol. 76, no. 11, pp. 13401–13423, 2017.
[33] P. Chandrakar and H. Om, "An extended ECC-based anonymity-preserving 3-factor remote authentication scheme usable in TMIS," *Int. J. Commun. Syst.*, vol. 31, no. 11, 2018, Art. no. e3540.
[34] G. Sharma and S. Kalra, "A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications," *J. Inf. Secur. Appl.*, vol. 42, pp. 95–106, Oct. 2018.
[35] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.
[36] L. L. Cao and W. C. Ge, "Formal analysis of an efficient handover authentication scheme for eap-based wireless networks with extending BAN logic," *Appl. Mech. Mater*, vols. 401–403, pp. 1864–1867, Sep. 2013.
[37] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna. J. Cuellar, P. H. Drielsma, P. C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron, "The AVISPA tool for the automated validation of Internet security protocols and applications," in *Proc. 17th Int. Conf. Comput. Aided Verification, Comput. Aided Verification*, 2005, pp. 281–285.
[38] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 4, pp. 708–722, Jul./Aug. 2018.

CAO SHOUQI received the bachelor's degree in mechanical manufacturing technology and equipment, and the M.S. degree in mechanical manufacturing and automation from Sichuan University, in 1996 and 1999, respectively, and the Postdoctoral degree in control science and engineering from Shanghai University, in 2009. He is currently a Professor and a Doctoral Supervisor with the College of Engineering Science and Technology, Shanghai Ocean University. His main research interests include the marine Internet of Things engineering, fisheries engineering, and automation technology research.

LIU WANRONG received the bachelor's degree in electrical engineering and automation from the Luoyang Institute of Technology, in 2018. She is currently pursuing the master's degree with the College of Engineering Science and Technology, Shanghai Ocean University. Her main research interests include communication security and the Internet of Things technology.

CAO LILING received the bachelor's degree in electronic information science and technology and the M.S. degree in physics electronics from Central South University, in 2004 and 2007, respectively, and the Ph.D. degree in testing technology and automation from Tongji University, in 2017. She is currently an Experimental Teacher with the College of Engineering Science and Technology, Shanghai Ocean University. Her main research interests include network security and authentication protocol.



HE XIN received the bachelor's degree in mechanical engineering from Anhui Polytechnic University, in 2018. He is currently pursuing the degree with the College of Engineering Science and Technology, Shanghai Ocean University. His main research interest includes the Internet-of-Things technology.

JI ZHIYONG received the bachelor's degree from the Nanjing University of Aeronautics and Astronautics, in 2012, and the M.S. degree from Jiangsu University, in 2017. He is currently the Master's Supervisor of mechanical engineering with Shanghai Ocean University. He is also the Medical Equipment Senior Engineer and the Deputy Director of Shanghai Sixth People's Hospital East. His research interests include the development and application of wearable medical devices based on the Internet of things and the information security of the medical Internet of things.