
International Conference On
GREEN ENERGY, COMPUTING AND SUSTAINABLE TECHNOLOGY (GECOST) 2022
Green Sustainable Technologies for Creating a Better World
GECOST 2022
GECOST 2022 is a virtual conference organised to discuss and present the latest developments and applications related to the challenges of securing green and clean energy sources for the 21st century to protect the environment.
26 - 28 OCTOBER 2022
MIRI SARAWAK MALAYSIA | VIRTUAL CONFERENCE
Organised by
Curtin University Malaysia
Supported by
IEEE
ComSoc VTS
SDEC Digitalising Sarawak
In Collaboration with
UNIVERSITY OF Southampton MALAYSIA
IST Indore Institute of Science and Technology
UNTAR Universitas Tarumanagara

A Lightweight Multifactor Authentication Scheme for Wireless Sensor Networks in the Internet of Things

Izzatul Nabila Sarbini
Faculty of Computer Science and Information Technology
Universiti Malaysia Sarawak
Sarawak, Malaysia
sinabila@unimas.my

Adnan Shahid Khan
Faculty of Computer Science and Information Technology
Universiti Malaysia Sarawak
Sarawak, Malaysia
skadnan@unimas.my

Nurul Zawiyah Mohamad
Faculty of Computer Science and Information Technology
Universiti Malaysia Sarawak
Sarawak, Malaysia
mnzawiyah@unimas.my

Norfadzlan Yusup
Faculty of Computer Science and Information Technology
Universiti Malaysia Sarawak
Sarawak, Malaysia
ynorfadzlan@unimas.my

***Abstract*—Internet of Things (IoT) has become an information bridge between societies. Wireless sensor networks (WSNs) are one of the emergent technologies that work as the main force in IoT. Applications based on WSN include environment monitoring, smart healthcare, user legitimacy authentication, and data security. Recently, many multifactor user authentication schemes for WSNs have been proposed using smart cards, passwords, as well as biometric features. Unfortunately, these schemes are shown to be susceptible towards several attacks and these includes password guessing attack, impersonation attack, and Man-in-the-middle (MITM) attack due to non-uniform security evaluation criteria. In this paper, we propose a lightweight multifactor authentication scheme using only hash function of the timestamp (TS) and One Time Password (OTP). Furthermore, public key and private key is incorporated to secure the communication channel. The security analysis shows that the proposed scheme satisfies all the security requirement and insusceptible towards some well-known attack (password guessing attack, impersonation attack and MITM).**

Keywords—Multifactor Authentication, Wireless Sensor Networks, Internet of Things

I. INTRODUCTION

The IoT is made up of a network of physical sensors and controllers that serve a variety of purposes. Through the network, these devices are connected to one another to provide a range of services, including real-time monitoring, data collecting, and data analysis [1]. The increase in the number of smart devices has simultaneously increase the number of IoT applications which includes smart home, smart health, and industrial IoT. In these applications, physical objects are embedded with sensors and terminal devices which are constantly connected to IoT to exchange information. In WSNs, tens of thousands of different sensors are deployed everywhere (e.g., architectures, bridges, and intelligent terminals). Real-time data are gathered from the immediate environment or the target objects, and they are then sent to the nearby gateway nodes for additional processing. Through the network, the application systems can access the data [2]. Due to this characteristic of heterogeneous WSNs, the existence of any insecure terminal nodes can threaten the whole network's security as the flexible access mode; potential vulnerabilities continually come forth due to the complexity of heterogeneous networks. It is known that the sensor nodes are resource-constrained in some aspects such as low energy, insufficient computing capabilities, and lack of memory space, many expensive cryptographic primitives are not suitable [2]. Thus, there is a need to design an authentication protocol proposal for WSNs that satisfy in both security and efficiency. As a result, this study suggests a simple multifactor authentication system that incorporates both public and private keys during encryption. The suggested technique focuses on using the TS hash function and implementing OTP. As a result, the computational process is sped up without sacrificing security in any way. The goal of this study is to provide an effective and safe multifactor authentication system for communication between users (Ui), gateway networks (GWN), and sensor devices (SDj). Therefore, this study will offer a safe authentication method that is portable and usable by all resource-constrained sensors and terminal devices. The contribution of this study is listed as follows:

1) We introduced a lightweight multifactor authentication scheme by reducing the computational cost in the existing scheme. Our scheme only focuses on the hash function of the *TS*, which is suitable for resource-constrained sensing devices.
2) We also implement the use of public and private keys in the scheme to secure communication between the User, *Ui*, GWN, and the *SDj*.
3) The proposed scheme uses the secret-sharing technology and Chinese Remainder Theorem (CRT) in the offline sensing device registration phase.

As potential network vulnerabilities grow over time, future research should be considered to constantly raise the authentication scheme's security level. Any IoT authentication strategy should priorities minimizing computing cost and maximizing security.

The paper is organized as follows: Section 2 extensively discusses related works to this research, Section 3 elaborates the proposed scheme, Section 4 illustrates the security analysis, followed by Section 5, which is the conclusion.

978-1-6654-8663-7/22/$31.00 ©2022 IEEE

II. Related Works

Since this is not a new research area, so many authors have already contributed to this domain, for instance, [2] highlights the importance of the balance between security and efficiency of an authentication scheme for WSNs, later he proposed new lightweight three-factor authentication and key agreement scheme for multi-gateway WSNs. They found out that their new scheme performed better than other relevant schemes for maintaining efficient performance, meanwhile satisfying the security criteria. Similarly, [3] is concerned about a high security level that normally imposes a greater degree of overhead costs of any IoT authentication solution. As a result, they suggested a framework for multi-factor, multi-level, and interaction-based (M2I) authentication. The framework uses interaction-based and LoA connected authentication. Peer-to-peer (P2P) and one-to-many (O2M) interaction modes are examined through the design of two related protocols. The findings demonstrate that adoption of the O2M interaction mode for authentication in the relevant use-case situations can dramatically reduce communication costs. Additionally, [4] emphasizes the significance of security in the management of patient data for the healthcare industry and data for smart homes. They therefore suggested a safe remote multi-factor authentication system that has three components: User identification, password, and user biometrics are all components of the secret key and take part in the key agreement procedure after being verified by the remote server. They used the chaotic map because it has a smaller key size and less computational overhead, and they skillfully combined it with zero-knowledge technology and fuzzy extractor technology to achieve distant multi-factor authentication and key agreement. They discovered that the system is more secure and robust because the user is not disclosing any critical information, and even if the adversary obtains the server's master key, he is unable to impersonate any user. The relevance of the suggested scheme is that it is ideal for smart devices with limited power as well as the environment for fifth-generation (5G) communications. Furthermore, [5] proposed a lightweight and secure user authentication protocol based on the Rabin cryptosystem. They are using ProVerif in the security analysis and it show that that their protocol is secure against all the possible attacks. Furthermore, [6] addressed a comparable issue with WSN-aided IoT connectivity. By utilising improved Rabin assisted elliptic curve encryption, biometric characteristics, and time stamping techniques, they introduce a multifactor authentication and key management mechanism. The analysis shows that the suggested protocol may guarantee maximum QoS levels while preventing security vulnerabilities by providing higher packet delivery and low latency. Meanwhile, both [7] and [8] discussed on the multifactor authentication key agreement for Industrial IoT (IIoT). Author [7] focused on the security of data transmission between authorize machines. Hence, they proposed a new multifactor authenticated key exchange protocol to achieve the human involved “machine-to-machine” secure communication in IIoT. A secure multifactor authenticated key agreement approach for IIoT is proposed in [8] to support authorised users who want to access sensing devices from a distance. The system makes use of smart cards, biometrics, and passwords to identify users in IIoT environments. Since the proposed approach only makes use of symmetric cryptography, bitwise XOR operations, and hash functions, it is appropriate for the resource-constrained IIoT. Their performance research shows that, in comparison to existing correlative schemes, their proposed scheme has lower communication and computing costs. In order to lower the computational cost, we simply use the timestamp hash function in our newly proposed method, which improves the existing scheme [7]. We consequently use this novel lightweight authentication method in IoT WSNs.

III. Proposed Scheme

A. Offline Sensing Devices

In this phase, GWN will register the sensing devices in offline using secret-sharing technology and Chinese remainder theorem (CRT). GWN picks a unique identity ID_{SDj} for each sensing device S_{Dj}, where $j = 1, 2,..., n$. GWN then choose two n-dimensional vector $Vector_1$, $Vector_2$ and a secret value S which is utilized to act as the secret (It is assumed that $S = Vector_1 \cdot x_0$ and $S_2 = Vector_2 \cdot x_0$, where $x_0 = \phi(D)$, $x_i = \phi(Pi)(1 \leq i \leq n)$). GWN calculates $s_j = Vector_1 \cdot x_j$, $f_j = Vector_2 \cdot x_j$. GWN selects pairwise relative positive numbers $k_1,..., k_n$ for each sensing devices S_{Dj}, j = 1,..., n, respectively. GWN calculates $Mul = \prod_{j=1}^{n} k_j$ and $Mul_j = Mul/k_j$. Then, GWN generates a random nonce $Nonce_j$ which satisfies $Mul_j \times Nonce_j \equiv 1 \mod k_j$. GWN calculates $\gamma = \sum_{j=1}^{n} Var_j = \sum_{j=1}^{n} Mul_j \times Nonce_j$ and stores γ. Finally, GWN securely sends <ID_{SJi}, s_j, f_j, k_j> to each sensing device, respectively.

B. User Registration

To access sensing devices securely, U_i must first register with *GWN*. Fig.1 shows an illustration of registration phase. The following steps shows the detailed process of the registration.

Step 1: First, U_i chooses a unique identity ID_i and high-entropy password, PW_i. U_i then imprints the biometrics B_i and computes $B_k{*}= Gen(B_i)$ by the generation algorithm in fuzzy extractor to obtain biometric key B_{Ki}. U_i randomly generates a 128-bit nonce a and calculates $TPW = h(IDi|| PWi||B_K{*}) \oplus a$. Finally, U_i transmits a message ID_i, TPW_i to *GWN* securely.

Step 2: After receiving message ID_i, TPW_i, *GWN* randomly generates a 1024-bit secret key KEY_{GWN} and computes $KEY_{GWN-Ui} = h(ID_I||KEY_{GWN})$. Then, GWN calculates $A_i = KEY_{GWN\text{-}ui} \oplus TPWi$, $C_i = ID_{GWN} \oplus TPWi$. In addition, GWN generates a 128- bit temporary identity TIDi for each user Ui. Finally, GWN generates the smart card SC_i which stores { TID_i, A_i, C_i, $h(\cdot)$} for each U_i and sends SC_i to U_i securely.

Step 3: When receiving SC_i, U_i computes $RPW = h(ID_i || PW_i ||BK_i)$, $A_i' = A_i \oplus TPW_i \oplus RPW_i$ to protect A_i. Then, U_i calculates $D_i = a \oplus h(ID_i||BK_i)$, $C_i' = C_i \oplus TPW_i \oplus h(ID_i||BK_i)$. To help validate the identity of U_i locally, U_i computes $V_i = h(RPWi||Ai||a||h(IDi||BKi)) \mod \omega$, ω is the medium integer and the capacity to defeat an online guessing attack employing a fuzzy verifier is determined by the medium integer [8], [9]. The adoption of a fuzzy verifier can effectively stop an attacker from guessing an opponent's password, biometric key, or user identity [10, 11]. Finally, U_i stores {TID_i, A_i', C_i', D_i, V_i, Gen (·), Rep (·), h (·), τ_i, ω } into the memory and deletes other information.

User (U_i)		**Gateway Node (GWN)**
Input ID_i, PW_i, B_i Compute $B_k{*}= Gen (B_i)$ $TPW = h(IDi\|\| PWi\|\|B_K{*})\oplus a$		
	<$IDi.\ TPW_i$> → Secure channel	Generate 1024-bit secret key KEY_{GWN} Calculate $KEY_{GWN\text{-}ui} = h(ID_I\|\|KEY_{GWN})$ $A_i = KEY_{GWN\text{-}ui} \oplus TPW$ $C_i = ID_{GWN} \oplus TPW$ Store <TID_i, A_i, C_i, $h(\cdot)$> into smart card, SC_i
Compute $RPW = h(ID_i \|\| PW_i \|\|BK_i)$ $A_i' = A_i \oplus TPW_i \oplus RPW_i$ $D_i = a \oplus h(ID_i\|\|BK_i)$ $C_i' = C_i \oplus TPW_i \oplus h(ID_i\|\|BK_i)$ $V_i = h(RPWi\|\|Ai\|\|a\|\|h(IDi\|\|BKi))$mod ω Store <TID_i, A_i',C_i',D_i, V_i, Gen (·), Rep (·), h (·), τ_i, ω >	SC_i ←	

Fig. 1. User Registration Process

User (U_i)	Gateway Node (GWN)	**Sensor Device (SD_j)**
Input SC_i Input ID_i, PW_i, B_i Compute $BK_i{*} = Rep(B_i{*}, \tau)$ $RPW_i{*} = h(ID_i\|\|PW_i\|\|BK_i{*})$ $a{*} = D_i \oplus h(ID_i\|\|BK_i{*})$, $A_i{*}=A_i{*}\oplus a{*}$ $V_i{*}=h(RPW{*}\|\|A_i{*}\|\|a{*}\|\|h(ID_i\|\|BK_i{*}))$mod ω Check if $V_i=V_i{*}$, If yes, Generate timestamp, TS_1 and One Time Password (OTP) Choose Private Key, K_{priv} and Public Key, K_{pub} Store K_{priv} M1 = $[(h(TS_1)_{kpriv}]_{kpub}$	Check if $\|TS_1\text{-}TS_1'\|\leq \Delta\ TS$ Insert OTP and check if similar If yes, extract ID_i Compute $M_2 = h(M_1)$ Check if $M_2 = M_1$? If yes, Generate timestamp TS_2 and OTP $M_3 = [(h(TS_2)_{kpriv}]_{kpub}$	
<IDi, M_1, TS_1, OTP> → Secure channel	<IDi, ID_{GWN} M_3, TS_2, OTP> → Secure channel	Check if $\|TS_2\text{-}TS_2'\|\leq \Delta\ TS$ Insert OTP and check if similar If yes, extract ID_{SDj} Compute $M_4 = h(M_3)$ Check if $M_3 = M_4$? If yes, Generate timestamp TS_3 and OTP $M_5 = [(h(TS_3)_{kpriv}]_{kpub}$

Fig. 2. Login and Authentication Process

C. Login and Authentication Phase

This section will describe the login and the authentication process. Fig. 2 shows the process of login and authentication process of a lightweight multifactor authentication in IoT. The detailed of login (LP) and authentication (AP) process is shown below:

Step LP1: U_i inputs a unique identity, ID_i and password, PW_i, and imprints the biometrics $B_i{*}$ to the card reader. The SC_i reconstructs the biometric key $BK_i{*} = Rep(B_i{*}, \tau)$. Then, SC_i computes $RPW_i{*} = h(ID_i\|\|PW_i\|\|BK_i{*})$, $a{*} = D_i\oplus$

$h(ID_i\|\|BK_i{*})$ and $A_i{*}=A_i{*}\oplus a{*}$ by the U_i's credentials and the information stored in the SC_i. SC_i then computes $V_i{*}=h(RPW{*}\|\|A_i{*}\|\|a{*}\|\|h(ID_i\|\|BK_i{*}))$ mod ω and checks whether $V_i=V_i{*}$, to validate the identity of the user U_i.

Step LP2: If the authenticity of U_i is successful, SC_i generates a timestamp, TS_1 and One Time Password (OTP). Then, SCi choose a private key, K_{priv}, and public key, K_{Pub}. SC_i then store the K_{priv}. Then SC_i calculates, M1 = $[(h(TS_1)_{kpriv}]_{kpub}$. To securely transfer the message, it is encrypted using K_{priv} and K_{pub}. Finally, SC_i sends the message {IDi, M1, TS1, OTP} to GWN via a secure channel.

Step AP1: After receiving the message {IDi, M1, TS1, OTP} from U_i, GWN first checks the freshness of login request by verifying whether $|TS_1\text{-}TS_1'|\leq \Delta\, TS$. If it is true, GWN will insert the OTP received from SC_i. Then GWN will proceed to retrieves the database to obtain IDi,. GWN will compute $M_2 = h(M_1)$ and checks whether M_2 is equal to M_1 to authenticate the authenticity of U_i. If it holds, GWN then generates a timestamp, TS_2 and One Time Password (OTP). GWN then calculates $M_3 = [(h(TS_2)_{kpriv}]_{kpub}$. To securely transfer the message, it is encrypted using K_{priv} and K_{pub}. Then GWN sends the message {IDi, ID_{GWN} M_3, TS_2, OTP}to sensing devise via a secure channel.

Step AP2: After receiving the message from GWN, GWN first checks the freshness of login request by verifying whether $|TS_2\text{-}TS_2'|\leq \Delta\, TS$. If is satisfied, SDj will insert the OTP received from GWN. Then SDj will proceed to retrieves the database to obtain ID_{SDj},. SDj will compute $M_4 = h(M_3)$ and checks whether M_4 is equal to M_3 to authenticate the authenticity of U_i. If it holds, SDj then generates a timestamp, TS_3 and One Time Password (OTP). GWN then calculates $M_5 = [(h(TS_3)_{kpriv}]_{kpub}$.

IV. SECURITY ANALYSIS

In order to have a secure communications system between the U_i, GWN and SD_j, some of the security requirements must be fulfilled. Hence, in this section we discuss how the proposed scheme fulfilled this security requirements and how it can resists against some well-known attacks.

A. Data Confidentiality

To verify the data confidentiality of the proposed scheme, we need to check on the privacy of the data sent by the sender and the receiver. The data transmitted by the sender must not be able to be retrieved by anyone other than the receiver. This confidentiality is achieved by using the public key and private key. We can refer to Fig. 2 where we can observe that all the messages from U_i to GWN to SD_j are encrypted with K_{priv} and K_{pub}. Thus, this shows that the data is confidential and can only be read by the receiving devices.

B. Data Integrity

To verify the data or message integrity of the proposed scheme, we need to verify whether the data sent is received as it was sent or can be modified. To achieve data integrity requirement, the timestamps of each message must be hashed. In addition, the actual timestamp also needs to be sent to the receiver along with the hashed timestamp. Whenever the message is received, the receiving party need to ensure that the message have not been modified by matching the value of hash sent with the value of hash received, if the hash value is different, then we have a modification issue in the message. Thus, in our scheme, the messages sent are fully secure against any integrity lost as any modification will be detected.

C. Non-Repudiation

To ensure the reliability of information transmitted, any parties that communicating with each other must agree at some point that either one of them is an originator of a particular message. At these states, the sender should not deny that one had not sent a message. Thus, digital signature is utilized. In the proposed system, the hash value of timestamp is digitally signed with the sender's private key which is only known by the sender. Consequently, the sender cannot deny that the message is sent by one. Hence, non-repudiation is achieved.

D. User Privacy

To verify the privacy of the proposed scheme, there is a need to ensure whether the real identity of the user can be revealed or not. In cell-free communication, knowing the real identities of all users can cause various privacy issues as well as real security threats such as identity reveal attack and location visibility attack. Thus, the real identities must be kept private by assigning pseudo identity of the participant. Secondly, participating device cannot know who is communicating to whom. These identities are only known to SDj since SDji the one who needs to manage the authorization of GWN and Ui.

E. Traceability

To verify the traceability of the proposed scheme, we need to verify whether the sender can deny that the was the sender of the message. For this, all hashed timestamp is encrypted with the private key of the sender as shown in Figure 2. Also, the returning hash is signed by the receiving party to make sure the reception and message generator. Consequently, this also method also can mitigate man-in-the-middle attack.

F. Mutual Authentication

To ensure that impersonation attack cannot be performed, all users are registered with the network and their public key also gets registered at registration authority. In the proposed scheme, SDj are registered within GWN using secret-sharing Technology and Chinese Remainder Theorem. GWN picks a unique identity ID_{SDj} for each sensing device $S_{Dj.}$ Also, to ensure mutual authentication, the sender sends OTP in each stage of the communication that is only known by the receiver. Receiver needs to verify the OTP in each step. Thus, the validation trust and authorization keys are already established. Impersonation attack cannot be made on the proposed scheme as the OTP is only known to the receiver.

V. CONCLUSION

In this paper, we have addressed the importance of security and efficiency of WSNs by considering its low computing capabilities and lack of memory space at the sensor nodes. Hence, we have introduced a lightweight multifactor authentication scheme for WSNs that overcomes the security vulnerabilities of WSNs towards password guessing attack, impersonation attack, and MITM attack. Through the analysis, we have found that the proposed scheme satisfies all the security criteria. This research can be improved by considering other well-known attack and reducing its computational cost without compromising the security level of the authentication scheme.

ACKNOWLEDGMENT

This research work is fully funded by Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak.

REFERENCES

[1] F. Balali, J. Nouri, A. Nasiri, and T. Zhao, ''IoT platform: Smart devices, gateways, and communication networks,'' in Data Intensive Industrial Asset Management. Cham, Switzerland: Springer, 2020, pp. 67–77.

[2] L. Xue, Q. Huang, S. Zhang , H. Huang , and W. Wang, "A Lightweight Three-Factor Authentication and Key Agreement Scheme for Multigateway WSNs in IoT" in Security and Communication Networks Volume 2021, Article ID 3300769, 15 pages https://doi.org/10.1155/2021/3300769I.

[3] S. AlJanah, N. Zhang and S. W. Tay, "A Multifactor Multilevel and Interaction Based (M2I) Authentication Framework for Internet of Things (IoT) Applications," in IEEE Access, vol. 10, pp. 47965-47996, 2022, doi: 10.1109/ACCESS.2022.3170844.

[4] W. Liu, X. Wang and W. Peng, "Secure Remote Multi-Factor Authentication Scheme Based on Chaotic Map Zero-Knowledge Proof for Crowdsourcing Internet of Things," in IEEE Access, vol. 8, pp. 8754-8767, 2020, doi: 10.1109/ACCESS.2019.2962912.

[5] Q. Jiang, S. Zeadally, J. Ma and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," in IEEE Access, vol. 5, pp. 3376-3392, 2017, doi: 10.1109/ACCESS.2017.2673239.

[6] Ara, T., & Prabhakar, M. (2019). Multifactor authentication and key management protocol for WSN-assisted IoT communication. *Journal of Telecommunications and Information Technology,* (3), 17-26. doi:10.26636/jtit.2019.134019

[7] Z. Li, Z. Yang, P. Szalachowski and J. Zhou, "Building Low-Interactivity Multifactor Authenticated Key Exchange for Industrial Internet of Things," in IEEE Internet of Things Journal, vol. 8, no. 2, pp. 844-859, 15 Jan.15, 2021, doi: 10.1109/JIOT.2020.3008773.

[8] R. Vinoth, L. J. Deborah, P. Vijayakumar and N. Kumar, "Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3801-3811, 1 March1, 2021, doi: 10.1109/JIOT.2020.3024703.

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

[10] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," IEEE Trans. Depend. Secure Comput., vol. 15, no. 4, pp. 708–722, Jul./Aug. 2018.

[11] D. Wang and P. Wang, "On the anonymity of two-factor authentication schemes for wireless sensor networks," Comput. Netw., vol. 73, pp. 41–57, Nov. 2014. [Online]. Available: https://doi.org/10.1016 /j.comnet.2014.07.010

[12] C. G. Ma, D. Wang, and S. D. Zhao, "Security flaws in two improved remote user authentication schemes using smart cards," Int. J. Commun. Syst., vol. 27, no. 10, pp. 2215–2227, 2014.

[13] B. Chatterjee, D. Das, S. Maity and S. Sen, "RF-PUF: Enhancing IoT Security Through Authentication of Wireless Nodes Using In-Situ Machine Learning," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 388-398, Feb. 2019, doi: 10.1109/JIOT.2018.2849324.

[14] Kebande, V. R., Awaysheh, F. M., Ikuesan, R. A., Alawadi, S. A., & Alshehri, M. D. (2021). A blockchain-based multi-factor authentication model for a cloud-enabled internet of vehicles. Sensors, 21(18) doi:10.3390/s21186018

[15] Khalid, H., Hashim, S. J., Ahmad, S. M. S., Hashim, F., & Chaudhary, M. A. (2021). A new hybrid online and offline multi-factor cross-domain authentication method for iot applications in the automotive industry. Energies, 14(21) doi:10.3390/en14217437

[16] Abuarqoub, A. (2020). D-FAP: Dual-factor authentication protocol for mobile cloud connected devices. Journal of Sensor and Actuator Networks, 9(1) doi:10.3390/jsan9010001

[17] Alshahrani, M. M. (2021). Secure multifactor remote access user authentication framework for iot networks. Computers, Materials and Continua, 68(3), 3235-3254. doi:10.32604/cmc.2021.015310

[18] S. Atiewi et al., "Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography," in IEEE Access, vol. 8, pp. 113498-113511, 2020, doi: 10.1109/ACCESS.2020.3002815.