Iraqi Journal of Information and Communications Technology(IJICT)
Vol. 9, Issue 1, April 2026
www.ijict.edu.iq
ISSN:2222-758X
e-ISSN:2789-7362

A SECURE SMART HOME AUTHENTICATION SCHEME FOR REMOTE USERS

Ali T. Al-Hachami [1], **Mohammed F. Al-Gailani** [2]
[1] Department of Information Technology, Earthlink Telecommunications Company, Bagdad, Iraq
[2] Department of Syber Security Engineering, College of Information Engineering, Al-Nahrain University, Jadriya, Baghdad, Iraq
ali.thaer@coie-nahrain.edu.iq[1], m.falih@nahrainuniv.edu.iq[2]
Corresponding Author: **Mohammed F. Al-Gailani**
Received:26/06/2024; Revised:01/10/2024; Accepted:11/10/2024
DOI:10.31987/ijict.9.1.291

***Abstract*- Internet of things (IoT) technologies have permeated many of the devices used in daily life. Nowhere is this more evident than in smart homes, where regular home appliances are now connected to the internet to gain additional functionality, control and automation of routine tasks. However, like most technologies, convenience often comes at the price of risking user privacy. This paper aims to remedy this security risk by providing the user with a scheme to verify their identity in an anonymous manner. The solution needs to be lightweight and fast since smart home devices are resource constraint. The proposed scheme uses two stages to authenticate remote users, the first is using biometric fingerprints locally on the user's mobile device and the second relies on user identity (username and password) that are sent to the smart home gateway over a secure VPN tunnel between the mobile device and the gateway. The security of the proposed scheme is verified using the scyther tool which finds security flaws in internet protocols. The performance of the scheme is compared with similar existing schemes in terms of computational cost, and it was found that the proposed scheme achieves a computational cost of 0.02 ms and outperforms all previous schemes in those metrics.**

keywords: **Smart Homes, Authentication, VPN, Smart Home Gateway, Hash Functions, Scyther Tool.**

I. INTRODUCTION

Smart home technologies are some of the biggest growing sectors in the Internet of Things (IoT) field [1]. It provides homeowners with more control over the functions of their home appliances (smart locks, bulbs, fridges, etc.). By connecting these devices to the internet, allowing the user to monitor any activity in the home from anywhere in the world and also automate some routine household tasks such as turning the lights and locks on/off at specific time intervals, send notifications to the homeowner when someone rings the doorbell and many more applications are possible. However, this added convenience and ease of use is not without its downsides. Risks to user privacy and security have been a concern for the scientific community in the past few years [2]. Those concerns are not unfounded. The ease of use and access to these devices over the internet, coupled with the fact that many smart home devices have limited computational resources preventing the implementation of advanced security protocols, has provided malicious actors a massive attack surface to exploit. Some scenarios include theft of information, unlocking the smart locks or locking the real homeowners out of their home. The typical architecture of smart homes includes two types of entities: smart devices, which are home appliances connected to the internet, and the smart home gateway, which is used for sending control commands to the smart devices and connecting these devices to the internet [3]. A typical smart home architecture is displayed in Fig. 1. In order to secure the smart home network, the gateway needs to be able to verify the user identity when connecting to the gateway through the internet. Due to the resource constraint nature of smart home devices, the user authentication scheme is required to

ISSN:2222-758X
e-ISSN:2789-7362

be lightweight and fast, and of course, it should provide the user with adequate security against the most common attacks on smart homes. The proposed scheme is discussed in detail in the upcoming sections along with comparisons of the performance metrics with other previous schemes.

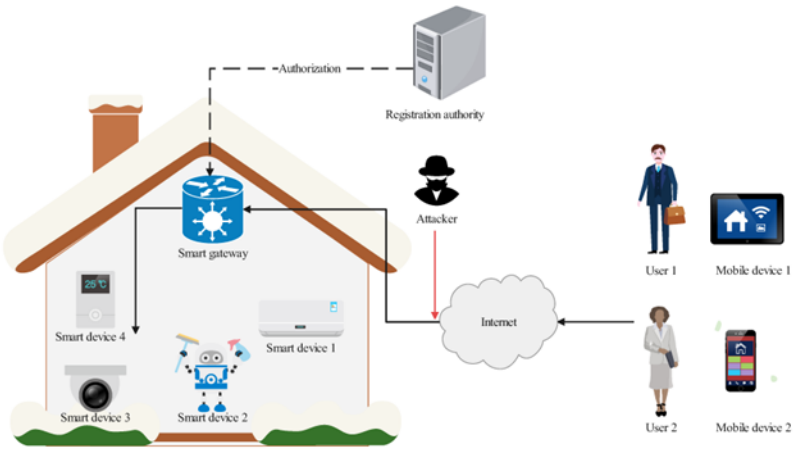

Figure 1: Typical smart home architecture.

The rest of paper is organized as follows. Section II presents a common related works. Section III addresses the problem statement. The proposed scheme introduced in Section IV. The formal security analysis of the scheme presented in Section V. A performance comparison was mad in Section VI. Finally, the conclusion is presented in Section VII.

II. RELATED WORKS

Authentication schemes have been following similar trends in the past few years. A secure authentication scheme based on Elliptic Curve Cryptography (ECC) is in [4]. The scheme proves to be secure against the most common passive and active attacks on smart homes. Additionally, no verification table is kept in order to maintain user authentication. However, elliptic curves suffer from slow performance. Additionally, if not implemented properly, ECC may suffer from mathematical weaknesses.

Another ECC-based scheme is proposed in [5]. In this scheme, the process of computing the session keys is offloaded to a home gateway known as Home Energy Manager (HEM), this HEM would then distribute the session keys to both the user and the requested smart device. Before the key distribution, the user needs to authenticate himself on a smart phone app using a username and password, the IP of the HEM, and the device serial number, which can all be obtained by an attacker for an impersonation attack.

In [6] proposed an authentication scheme that relies on blockchain technology for user authentication in smart homes. The system provides mutual authentication and key agreement for both the user and gateway using group signatures. However, blockchain technology is too computationally intensive to be used in the lightweight smart home environment. Additionally, users can be traced and identified by the system group manager, which could compromise the system if the group manager is compromised.

ISSN:2222-758X
e-ISSN:2789-7362

In [7] proposed a three factor authentication scheme to lower the communication cost from the previous schemes. The scheme also relies on ECC for authentication and key agreement. However, using three factors for authentication requires high computational power.

In [8] proposed a new smart home authentication scheme that improves upon the previous scheme proposed by in [4]. Where the user utilizes two factor authentication by using elliptic curve cryptography and user credentials (username and password). The improved scheme manages to enhance the security features in [4] but does not improve the performance of the scheme in terms of computational cost.

Other schemes have been developed to run on newer network protocols such as IPv6. For instance, in [9] developed a smart home authentication scheme for IPv6 enabled smart homes by creating an Authenticated Key Exchange (AKE) to establish a secure connection with the gateway using the user starts by registering with a registration authority and using the AKE protocol to establish a session key. Despite providing adequate security, the scheme has a high computational cost compared to other lightweight schemes.

In [10] proposed a scheme that authenticates users based on the concept of Photo Response Non-Uniformity (PRNU). In this scheme, the user sends a face image to the home gateway where the gateway will test the image freshness (if the image is new or not) and recognize the face of the user. If both are valid, the user is authenticated. While this scheme is secure, it does not maintain user anonymity.

III. PROBLEM STATEMENT

In recent years, research related to authenticating smart home users remotely has relied on using the gateway to authenticate smart home users, offloading the computational cost to the gateway since smart device have limited processing power. While this solution works well, leaving the home gateway open to the internet is generally very dangerous. An attacker gaining access to the smart home gateway means gaining access to the entire smart home network. In order to truly secure a smart home, this communication channel must be secured so that it cannot be accessed by an attacker. Narrowing down the attack surface that might compromise the gateway.

The aim of this paper is to establish an authentication scheme that can reliably verify a user's identity without making the smart home network accessible to the public internet. This is achieved by creating a secure communications channel between the user's mobile device and the smart home gateway. This is achieved by creating a VPN tunnel where the user can send authentication information to the gateway [11]. The scheme must also be secure against the most common attacks on smart homes in order to be useful in real-world scenarios.

IV. THE PROPOSED SCHEME

There are three entities involved in the scheme: remote user, home gateway, smart device. The authentication process starts locally at the mobile device, where the user authenticates himself using his biometric fingerprint [12][13]. After that, the user connects over an encrypted VPN tunnel to his private home network, where the user enters his unique identity and password. Finally, the user becomes fully authenticated and is granted access to the smart home devices according to his user privileges. Fig. 2 demonstrates a flowchart of the proposed scheme.

ISSN:2222-758X
e-ISSN:2789-7362

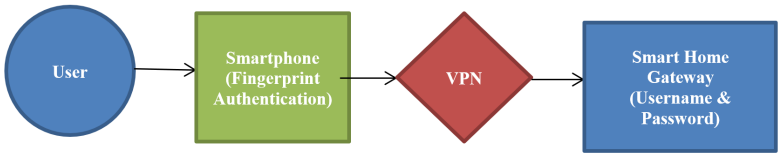

Figure 2: Flowchart of the proposed scheme.

A. *System Initialization Phase*

The Home Gateway (HG) is booted up and connected to the Internet. Both the user U_i and HG exchange key materials to generate a session key using the Diffie-Hellman key exchange [14], where both parties agree on global variables g and n. Both variables are prime numbers and $g < n$. Additionally, each party generates a private key, where x is the private key for U_i and y is the private key for HG. Each party computes a public key as $PU_u = g^x \bmod n$ for the user and also $PU_{gwn} = g^y \bmod n$ for the gateway. The two communicating parties then exchange those public keys and compute a common secret (session key) using their respective private key as $K_s = (g^x)^y \bmod n$ for both U_i and HG. This session key will be used to encrypt the VPN connection between U_i and HG [15].

B. *System Registration Phase*

The user U_i registers an account on the HG and creates an identity UID and a password P_i. The account credentials will be stored on the HG, where the password P_i will be hashed using SHA-256 and stored on the HG [16], in order to prevent an attacker from gaining full account information in the case the HG is breached.

C. *System Authentication Phase*

If U_i wants to connect to the smart home network, first, the user authenticates himself on the local user smartphone US_i with the biometric fingerprint. Then, U_i connects to the smart home network using the encrypted VPN tunnel. Once in the network, U_i enters $E_k(UID, P_i, N_i, T_i, C)$, which is an encrypted message containing the username, password, nonce, timestamp, and checksum. The HG computes $H(P_i)$ using SHA-256, and the hash values are compared; if $H(P_i) = H(P_{gwn})$, then U_i is verified and can access the smart home devices on the private home network [17].

V. FORMAL SECURITY ANALYSIS

The formal security analysis of the scheme involves using automated software for testing the protocols used to exchange keys and authenticate users. The scyther tool [18] is an open source python tool that is employed to test the steps of the proposed scheme for any potential vulnerabilities in the system. The Fig. 3 demonstrates the results of the test run on the proposed scheme and it shows that both the key material and the authentication of the remote user are not vulnerable to attacks.

ISSN:2222-758X
e-ISSN:2789-7362

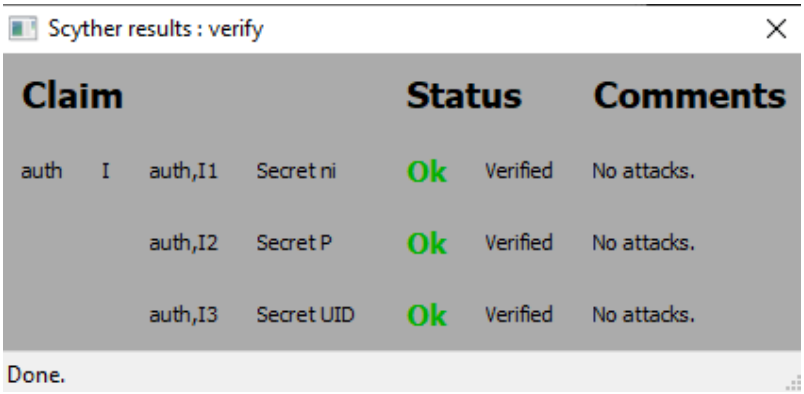

Figure 3: Scyther tool verifying the proposed scheme.

VI. PERFORMANCE COMPARISON

In this section, the computational cost of the proposed scheme is measured and compared to previous smart home authentication schemes, this helps evaluate the performance and speed along with comparing the resistance of the schemes to known attacks. The proposed scheme is compared to the following schemes: Shuai et. al. [4], Sadhukhan et. al. [7], Kaur & Kumar [8], tanveer et. al. [9] and Nimmy et. al. [10]. The hardware used includes: a huawei y9 prime for mobile users, which has an octa-core processor, 4 GB of RAM and a fingerprint sensor. For smart home gateway, a raspberry pi 3B+ is used, which has a Broadcom BCM2837B0 1.4 GHz processor and 1 GB of RAM.

A. Computational Cost Comparison

Calculating the computational cost of the scheme requires measuring the amount of time needed to execute each algorithm used in the proposed scheme. This is achieved by measuring the CPU time (in milliseconds) for each cryptographic operation used. It should be noted that the cost of the key exchange protocol will not be measured, since it is performed only once to exchange the session keys or when the key needs to be updated for transporting data through the VPN, so the cost is negligible. Instead, the cost will focus on the algorithms involved in the authentication process every time the user logs in to the smart home. The cost of the scheme involves TLS 1.3, which is a cryptographic suite of algorithms used to send encrypted data over the Internet. TLS 1.3 uses authenticated encryption, namely: TLS_AES_128_GCM_SHA256, which uses AES with a 128-bit key for encryption and SHA-256 as a cryptographic checksum. The execution time of the hash function (SHA-256), encryption/decryption, and the checksum are denoted as T_h, T_{ed}, and T_{mac} respectively. The result of benchmarking every cryptographic algorithm on a Raspberry Pi 3B+ is listed in Table I. These results are obtained using the CRYPTO++ library, which is a C++ library for running performance tests on cryptographic algorithms. These benchmarks give us the average time needed for executing each individual algorithm in the scheme, which in turn helps to calculate the total computational cost.

The cost of sending three encrypted authentication messages between the user mobile device and the home gateway, denoted by $6T_{ed} + 6T_{mac}$, takes approximately $0.018\,\text{ms}$. The password will be hashed with SHA-256 and compared to

TABLE I
Execution Time for Different Cryptographic Operations

Notation	Cryptographic Operation	Execution Time (ms)
T_h	Hash Function (SHA-256)	0.002
T_{ed}	Encryption/Decryption (AES-128 bit GCM)	0.001
T_{mac}	HMAC (SHA-256)	0.002

the stored hash, which takes 0.002 ms. Thus, the total computational cost is 0.02 ms. Table II shows the comparison of the computational cost with other related schemes and demonstrates that the proposed scheme achieves a lower computational cost than all related schemes when compared to Shuai et al. [4], Sadhukhan et al. [7], Kaur & Kumar [8], Tanveer et al. [9], and Nimmy et. al. [10]. Thus, the scheme manages to perform a secure authentication process at a lower cost to both the user side and the gateway side without requiring additional help from a trusted third party such as a registration authority or an external server.

TABLE II
Comparison of Computational Cost

Scheme	Total Time (ms)
Shuai et al. [4]	1.366
Sadhukhan et al. [7]	80.6
Kaur and Kumar [8]	1.366
Tanveer et al. [9]	7.6
Nimmy et al. [10]	1.28
Proposed Scheme	**0.02**

VII. CONCLUSION

This paper addresses the problem of identity authentication of smart home users. The limitation of processing power of smart devices poses a unique challenge to security researchers. Finding a delicate balance between security, speed and resource consumption is required. The proposed solution was lightweight and secure, and when compared to previous schemes, manages to outperform them in terms of computational cost, where the closest performing scheme in [10] achieves a cost of 1.28 ms while the proposed scheme achieves a cost of 0.02 ms which is significantly lower than the previous works. This is achieved by avoiding the use of computationally expensive cryptographic algorithms, offloading the processing of cryptographic algorithms to the home gateway and using the gateway as a proxy to interface with smart devices over home Wi-Fi. One potential avenue of future work includes making the authentication process more seamless for the user by creating a one-time token stored on the user's smartphone that can authenticate the user without having to type any passwords manually, and automatically regenerate the token on every new session.

FUNDING

None.

ACKNOWLEDGEMENT

The author would like to thank the reviewers for their valuable contribution in the publication of this paper.

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] A. A Laghari, R. A. Laghari. K. Wu, M. Ali, A. A. Khan. A Review and State of Art of Internet of Things (IoT) . Arch Computat Methods Eng Vol. 29 PP. 1395–1413 (2022). https://doi.org/10.1007/s11831-021-09622-6
[2] Y. Meng, W. Zhang, H. Zhu and X. S. Shen, "Securing Consumer IoT in the Smart Home: Architecture, Challenges, and Countermeasures," in IEEE Wireless Communications, vol. 25, no. 6, pp. 53-59, December 2018, doi: 10.1109/MWC.2017.1800100.
[3] R. Yu, X. Zhang and M. Zhang, "Smart Home Security Analysis System Based on The Internet of Things," IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), Nanchang, China, , pp. 596-599, (2021) doi: 10.1109/ICBAIE52039.2021.9389849.
[4] M. Shuai, N. Yu, H.Wang, L. Xiong, Anonymous authentication scheme for smart home environment with provable security, Computers Security, Vo. 86, PP 132-146, ISSN 0167-4048, (2019). https://doi.org/10.1016/j.cose.2019.06.002
[5] S. Naoui, M. E. Elhdhili, L. A. Saidane. Lightweight and Secure Password Based Smart Home Authentication Protocol: LSP-SHAP. J Netw Syst Manage, Vol. 27, PP. 1020–1042 (2019). https://doi.org/10.1007/s10922-019-09496-x
[6] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar and K. -K. R. Choo, "HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes," in IEEE Internet of Things Journal, vol. 7, no. 2, pp. 818-829, Feb. 2020, doi: 10.1109/JIOT.2019.2944400.
[7] D. Sadhukhan, S. Ray, G. P. Biswas, M. K. Khan, M. Dasgupta. "A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography. J Supercomput Vol. 77, PP. 1114–1151 (2021). https://doi.org/10.1007/s11227-020-03318-7
[8] D. Kaur, D. Kumar, "Cryptanalysis and improvement of a two-factor user authentication scheme for smart home", Journal of Information Security and Applications, Volume 58, 2021, 102787, ISSN 2214-2126. https://doi.org/10.1016/j.jisa.2021.102787
[9] M. Tanveer, G. Abbas, Z. H. Abbas, M. Bilal, A. Mukherjee and K. S. Kwak, "LAKE-6SH: Lightweight User Authenticated Key Exchange for 6LoWPAN-Based Smart Homes," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2578-2591, 15 Feb.15, 2022, doi: 10.1109/JIOT.2021.3085595.
[10] K. Nimmy, S. Sankaran, K. Achuthan and P. Calyam, "Lightweight and Privacy-Preserving Remote User Authentication for Smart Homes," in IEEE Access, vol. 10, pp. 176-190, 2022, doi: 10.1109/ACCESS.2021.3137175.
[11] J. Bugeja, A. Jacobsson and P. Davidsson, "On Privacy and Security Challenges in Smart Connected Homes," 2016 European Intelligence and Security Informatics Conference (EISIC), Uppsala, Sweden, pp. 172-175, 2016 doi: 10.1109/EISIC.2016.044.
[12] S. Dargan, M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities", Expert Systems with Applications, Vol. 143, 2020, 113114, ISSN 0957-4174. https://doi.org/10.1016/j.eswa.2019.113114
[13] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Ch.2 in Handbook of Fingerprint Recognition 2nd edition, London, U.K.:Springer-Verlag, 2009.
[14] N. Mäurer, T. Gräupl, C. Gentsch and C. Schmitt, "Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS," 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC), San Antonio, TX, USA, pp. 1-10, 2020 doi: 10.1109/DASC50938.2020.9256746.
[15] R. O. Andrade, I. Ortiz-Garcés and M. Cazares, "Cybersecurity Attacks on Smart Home During Covid-19 Pandemic," 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, pp. 398-404, 2020, doi: 10.1109/WorldS450073.2020.9210363.
[16] National Technical Information Service. FIPS 180-2 – secure hash standard, U.S. Department of Commerce/NIST, Springfield, VA; 2002. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf
[17] S. Chethana, S. S. Charan, V. Srihitha, D. Radha and C. R. Kavitha, "Comparative Analysis of Password Storage Security using Double Secure Hash Algorithm," 2022 IEEE North Karnataka Subsection Flagship International Conference (NKCon), Vijaypur, India, pp. 1-5, 2022, doi: 10.1109/NKCon56289.2022.10127057.
[18] C. Cremers, "The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols", in Proc. CAV-20th International Conference on Computer Aided Verification, Berlin, 2008.