A Survey on Authentication Approaches to Secure Smart Home Networks

Ta Quang Tung (104222196), *Fellow, IEEE*

***Abstract*—Internet of Things (IoT) is a field that has gathered much interest and has found applications in many areas. Smart home is one application of IoT in which the home is equipped with various smart appliances that communicate over a wireless network. While these devices can enhance users' lives, they are open to security risks that leave the home vulnerable to attacks. Securing the smart home network is a crucial step in ensuring safety for residents. Authentication, a process that verifies the identities of the devices and users in the network, is one means of achieving security. This paper surveys five influential authentication approaches, details their methodologies, strengths, and weaknesses, and discusses possible further improvements.**

***Index Terms*—Internet of Things, IoT, smart home, security, authentication**

I. INTRODUCTION

THE Internet of Things (abbreviated IoT) is a network of interconnected devices such as lights, cameras, cars, sensors, etc [1]. In recent years, the field has garnered considerable interest in the research community and has found applications in many areas. Among these, smart home is an area that has seen much development thanks to how closely it is related to people's everyday lives. A smart home is a home fitted with appliances that can be controlled remotely by the user via the Internet [2]. Currently, a multitude of smart home devices exist on the market: from smart lights and smart air-conditioning systems to smart cameras and sensors. These devices are manufactured by different companies and do not follow the same standards. However, two characteristics these devices share are their limited computing power and their ability to transmit and receive information across a wireless channel. Many smart home devices are capable of communicating with wireless protocols such as WiFi, Bluetooth, and ZigBee [3]. Their wireless support allows smart devices to be installed conveniently in any part of the house but leaves them open to security risks. Operating in a wireless environment means that the messages they transmit can be eavesdropped on by malicious attackers, who will then gain access to the home's private information such as camera recordings. From this information, attackers could spy on residents' routines, leaving them at serious risk. To demonstrate the frailty of smart devices, in January 2014, it was found that more than 750,000 consumer devices had been compromised to become phishing and SPAM bots [4]. To provide consumers with a safer smart home environment, security measures must be put in place to safeguard devices from external tampering. One approach to securing smart devices is authentication, a process where users and devices have to verify their identities before being able to participate in the system [5]. Over the years, various authentication schemes have been proposed for smart home networks, each having certain strengths and weaknesses. This paper will survey some of these approaches and give suggestions where appropriate. More specifically, the contributions of this paper are as follows:

- First, the author selects five papers describing the implementations of a smart home authentication system for discussion and analysis. These papers are chosen based on their high impact (more than 80 citations) and recency (published in 2013 or later).
- Second, the author describes the network setup of these schemes in detail. In addition, their methodologies, security analyses, performances, strengths, and weaknesses are also compared and discussed.
- Third, the author makes suggestions on where these schemes can be improved for future development and adoption.

II. CURRENT STATE OF THE ART

A. Paper selection

For discussion and analysis, the following papers have been chosen:

- [3] describes a simple authentication scheme using the public key mutual authentication protocol and Elliptic Curve Cryptography.
- [6] describes an authentication framework that can achieve device anonymity and unlinkability in the network.
- [7] describes a lightweight authentication scheme that establishes a secure session key between the IoT device and the home gateway.
- [8] describes an advanced authentication scheme that supports two-factor authentication (password and biometrics) and many end users.
- [9] describes a lightweight authentication scheme that incorporates biometrics for two-factor authentication.

Ta Quang Tung is a currently a second-year Software Development student at Swinburne University Vietnam (email: 104222196@student.swin.edu.au).

B. Network setup

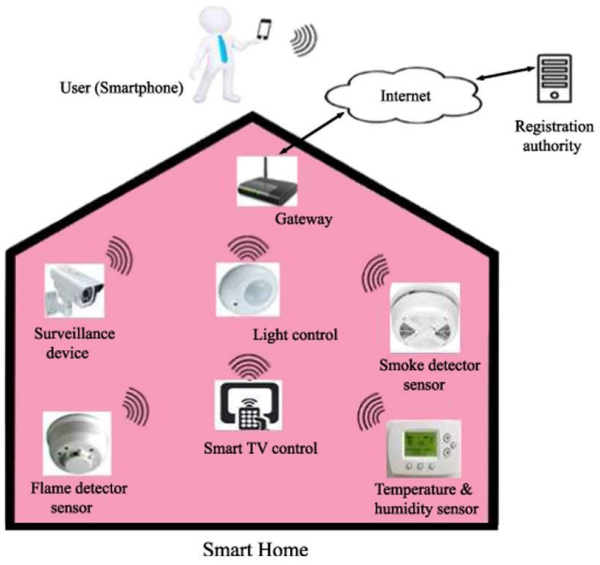

Fig. 1. The network model [8] used by the selected papers.

Nearly all five selected papers use the network model described in **Fig. 1**. The only exceptions are papers [3] and [9], which do not require the Registration Authority. The major components of the network are:

- The Home Gateway (HG), which is responsible for collecting and routing the network data, ensuring interoperability across smart home devices, and securing access to the home. It is connected to the Internet and can contact the outside world.
- The smart home devices, which are varied in type and standard. These devices can emit data and receive instructions (such as turn on or off). In addition, they have very limited computing power.
- The user, which can be inside the home or outside operating the devices remotely. The user typically interacts with the smart home devices through their mobile phones or personal computers.
- The Registration Authority (also called Security Service Provider by papers [6] and [7]), which is where the Home Gateway, smart home devices, and (optionally) users are registered and configured with initial secret values that are used for authentication. This entity is assumed to be trusted and tamper-proof.

C. Description of different approaches

Santoso and Vun [1ˢ] propose an authentication scheme that uses the public key mutual authentication protocol and Elliptic Curve Cryptography (ECC). Using ECC yields secure keys that are smaller in size than other approaches, which is ideal as smart devices generally have low computing and storage capabilities. Their authentication scheme takes place over WiFi using IPv6 and consists of two steps. The first step mutually authenticates the user's mobile phone (or a personal computer) with a smart device. The user first enters the smart device's identity and pre-shared secret key into their phone, then turns on the smart device, which boots up in WiFi access point mode, allowing it to be connected to the mobile phone. The phone then provides the smart device with the home network credentials and gateway location for it to connect to the gateway. The second step authenticates the smart device with the gateway. The gateway first receives the identity and pre-shared secret of the smart device through the user's mobile phone. It then authenticates the smart device and generates a shared key through the Elliptic Curve Diffie-Hellman (ECDH) algorithm. This shared key is used by both the gateway and smart device for communication. The benefit of this approach is that each smart device only needs to store one key for communication.

Kumar et al. [6] propose an authentication framework that ensures device anonymity and unlinkability. These properties prevent attackers from knowing the devices' identities and relationships. Their approach involves the Security Service Provider (SP), which is assumed to be trusted and tamper-proof. Authentication is split into three stages. In the first stage (system setup), the gateway is configured at the SP with a unique identity and various secret values. In the next stage (new device installation), the smart device is registered at the SP and provided with various secret credentials calculated by the SP. It is worth noting that this configuration is inextricably tied to the home gateway that the user wants to attach the device to, and any future changes to the home gateway require re-registering at the SP. The secrets stored in the smart device are used during the key agreement process and can only be computed by the legitimate gateway. In the final stage (key establishment), the smart device and the gateway are mutually authenticated. First, the smart device computes several values based on a random number, its current timestamp, and its secrets. It then sends all this information to the gateway. Next, the gateway checks the timestamp for any potential replay attacks, checks the identity of the smart device, and generates a shared symmetric key for future communication. It then sends the smart device the means to generate this key. When the smart device receives a response from the gateway, it checks for replay attacks, verifies the identity of the gateway, and generates the symmetric key. To close the authentication process, the smart device sends a confirmation to the gateway about the shared key. Security analysis shows that this approach is secured against various types of attacks such as replay, man-in-the-middle, and impersonation. Even when a smart device is compromised, the scheme will still protect the rest of the network, effectively localizing the impact of the attack. Performance analysis shows that this approach is only marginally faster than [7] but incurs approximately 53% of the communication overhead of [7].

Kumar et al. [7] propose a system that is in many ways similar to [6]. Their authentication scheme is split into two steps. The first step is a combination of the first two steps of [6]. Here, the user registers the home gateway and every smart device they want to attach to the network at the SP. Unlike [6], the gateway is now also configured with the secrets of every smart device. The second step is to authenticate the devices and establish a session key. The gateway first sends the smart device its current timestamp and a message authentication

code (MAC) computed from the secrets it knows of the smart device. On receipt, the smart device checks for any replay attacks, computes its own version of the MAC, and checks it against the MAC sent by the gateway. If it matches, the device computes an encrypted value N_A (which can be decrypted by the gateway) and a hashed MAC called tag then sends it to the gateway. The gateway can decrypt N_A to verify the identity of the device and calculate its own version of the tag. If this new tag matches the one sent by the device, the gateway generates the session key and sends an encrypted version of it to the device. The device, after verifying the payload, can obtain the session key that will be used for future communication. Security analysis shows that the scheme is safe against the Dolev-Yao attack model and various attacks such as masquerade, message forgery, replay, known key, and denial-of-service. It also offers protection when a smart device is compromised, similar to [6]. Performance analysis shows that its computation and communication costs are generally lower than other proposed systems.

Wazid et al. [8] propose an authentication system that supports multiple users and two-factor authentication using biometrics. Their scheme, while being much more intricate in design, has the overall structure of [6] and [7]. In this scheme, the SP is called the Registration Authority (RA) and the new users must also register here. Authentication is split into four steps. In the first step (offline smart device and gateway registration), the smart devices and home gateway are configured with initial secrets. The gateway is also configured with the identity of all users. In the second step (user registration), each user provides their identity, password, and biometrics to the RA. The RA then generates a secret key corresponding to the gateway and the user, plus a temporary identity. This identity and a hashed version of the key are sent to the user, who then computes and stores in memory various parameters that are used in later steps. In the third step (login), the user provides their identity, password, and biometrics on their phone. If all is correct, the phone sends a login request to the gateway. In the final step (authentication and key agreement), the gateway checks for any replay attacks and verifies the information received from the user. It then sends a request to the smart device, which in turn verifies the request using its calculations. If the request is correct, the device generates a session key for that user and sends it to the gateway. After another round of checks, the gateway forwards the reply to the user. The user's phone can now compute and validate the session key, which will be used for future communication. This scheme also enables the user to update their password and biometrics. To do this, the user first supplies their old password and biometrics. If the system finds this information correct, it will prompt the user to supply their new credentials and save them in memory. Security analysis shows that this scheme is protected from many forms of attacks and offers anonymity and unlinkability similar to [6]. Performance analysis shows that it incurs more communication and computational costs (2x the communication cost and 4x the computational cost of [7]).

Dhillon and Kalra [9] propose a lightweight scheme that supports biometric authentication. Similar to [3], their approach does not involve the external SP. The process comprises three steps: registration, login, and authentication. In the first step, the user registers with the home gateway with their ID, password, and biometrics, while the smart devices register with a shared secret of the gateway. In the second step, the user accesses an IoT service app and provides their ID, password, and biometrics to begin authentication. If the details provided are correct, the user's device sends a request directly to the smart device. In the third step, the smart device checks for any replay attacks and sends a message to the gateway to authenticate both itself and the user. The gateway authenticates the smart device first, then the user. After receiving a successful authentication response from the gateway, the smart device sends the user one final message to confirm the identities of itself and the gateway. If the user can verify the information, it generates the session key to be used for communication. This approach also allows password changes similar to [8]. Security analysis shows that this scheme is protected against many forms of attacks and offers user anonymity and mutual authentication. As a trade-off, it is more computationally expensive than other methods.

D. Key limitations, challenges, and author's opinions

While the approaches above can enhance the security of smart home networks, they are not without challenges. The scheme by [3] has several drawbacks. First, the authors have not analyzed its performance and security, making its effectiveness hard to assess. Second, this approach uses IPv6, which is not yet universally adopted. Therefore, the user might encounter issues integrating it into an existing network. Further development is necessary to ensure these devices are compatible with non-IPv6 networks. Third, this approach assumes the existence of a pre-shared secret key that comes with the smart device. A question worth asking is what party generates this key, and how it can be protected if it comes unencrypted with the device. In its current state, a malicious insider who seizes the device can easily use this information to illegitimately authenticate with the home gateway and leak information. The approach by [6] has two main drawbacks. First, it is predicated on the assumption that the gateway shares the same symmetric cryptographic systems as the smart devices, which is unlikely given that these devices are produced by different companies and follow different standards. Second, if the smart device were to be moved to another network or if the gateway were to change, it would have to be registered at the SP again. A possible improvement is to provide online device registration so that users can more conveniently register devices, although this may entail additional security risks that warrant further research. The drawbacks of [7] and [8] are similar to [6]. However, this time, when a new device is added, the home gateway must also be updated by the SP, which can be quite cumbersome. While [9] does not suffer from the inconvenience of [6], [7], and [8] by eliminating the SP, it forces the user to be near the

smart device during the authentication process, limiting the distance from which the user can access the system.

III. Conclusion

Smart home is a field that has great potential to enhance people's lives by allowing home appliances to operate more intelligently and be controlled more easily from afar. However, in many current implementations, smart home devices operate in a wireless environment, leaving them vulnerable to malicious attackers who can invade residents' privacy, spy on their routines, and obtain private information. Securing the smart home network with a robust system is paramount; however, it can be quite challenging due to the limited computing power and heterogeneity of smart devices. One security approach is to use authentication to verify the identities of the devices and users in the network. In this paper, the author has surveyed five influential authentication schemes by other researchers in the field. Their approaches vary in complexity, computational and communicative performance, and security level. All methods, despite certain advantages, are not without drawbacks. Some approaches offer more advanced security features, including biometrics verification, but incur a performance trade-off. Some require the involvement of a third-party security service provider, which adds additional complexity while installing a new device or adding a new user. Some are robust in theory but operate on the assumption that the devices on the network share the same cryptographic processes to be used during authentication, which is unlikely due to the heterogeneity of smart devices. More research and development are needed to ensure interoperability between devices, seamless integration with existing networks, and ease of installation for users.

References

[1] "What is IoT? - Internet of Things Explained - AWS." Accessed: Jun. 09, 2024. [Online]. Available: https://aws.amazon.com/what-is/iot/

[2] "Smart Home: Definition, How They Work, Pros and Cons," Investopedia. Accessed: Jun. 09, 2024. [Online]. Available: https://www.investopedia.com/terms/s/smart-home.asp

[3] F. K. Santoso and N. C. H. Vun, "Securing IoT for smart home system," in *2015 International Symposium on Consumer Electronics (ISCE)*, Jun. 2015, pp. 1–2. doi: 10.1109/ISCE.2015.7177843.

[4] B.-C. Choi, S.-H. Lee, J.-C. Na, and J.-H. Lee, "Secure firmware validation and update for consumer devices in home networking," *IEEE Trans. Consum. Electron.*, vol. 62, no. 1, pp. 39–44, Feb. 2016, doi: 10.1109/TCE.2016.7448561.

[5] "What is authentication?" Accessed: Jun. 09, 2024. [Online]. Available: https://www.cloudflare.com/learning/access-management/what-is-authentication/

[6] P. Kumar, A. Braeken, A. Gurtov, J. Iinatti, and P. H. Ha, "Anonymous Secure Framework in Connected Smart Home Environments," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 4, pp. 968–979, Apr. 2017, doi: 10.1109/TIFS.2016.2647225.

[7] P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila, and M. Sain, "Lightweight and Secure Session-Key Establishment Scheme in Smart Home Environments," *IEEE Sens. J.*, vol. 16, no. 1, pp. 254–264, Jan. 2016, doi: 10.1109/JSEN.2015.2475298.

[8] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 2, pp. 391–406, Mar. 2020, doi: 10.1109/TDSC.2017.2764083.

[9] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services," *J. Inf. Secur. Appl.*, vol. 34, pp. 255–270, Jun. 2017, doi: 10.1016/j.jisa.2017.01.003.