MyMaster : A Multifactor Authentication Scheme for Smart Home Device

[1*]Emilli anak Lijau, [2]Shirley Sylvia Binti Sulai, [3]Nurin Syamirah Binti Tabran, [4]Nur Fathin Binti Nor Hisham, [5]Nur Fatin Shafiqah Binti Azalli, [6]Humaira Syafiqah Binti Hamdan and [7]Nur Adilya Binti Osman

Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia

email: [1*]emillilijau@gmail.com, [2]shirleysylvia17@gmail.com, [3]nurinsyamirah98@gmail.com, [4]fathinz98@gmail.com, [5]fatinshafiqah.fs.98@gmail.com, [6]humairasyafiqah98@gmail.com, [7]nuradilya12@gmail.com

Date received: 27 August 2021
Date accepted: 2 October 2021
Date published: 11 November 2021

Abstract - *Smart homes are one of the Internet of Things (IoT) applications most significant to enable people to operate intelligent devices on the Internet in their homes. However, when users can access an intelligent home system remotely, they have major privacy and confidentiality difficulties to overcome. Nothing has been done to improve the safety characteristics of an intelligent home with current research on authentication approaches. For example, to address these issues and to develop a reciprocal tracking authentication system with a critical aspect of a deal, we recommend an Internet based Smart Home System (IFTTT) model. As a controller and a safety guard, an IFTTT-Home Gateway provides a user with remote access to a Smart Home System within their company. The system is designed for mutual authentication with security features such as anonymity and full advance security by using Elliptical Curve Encryption, Nonces, XOR or cryptographic Hash functions. We also incorporate multi factor authentication (MFA) into the model to ensure more security and preventing privacy leakage.*

Keywords: Multi factor authentication (MFA), IoT, Smart home, User authentication, Smart device.

1 Introduction

In research from Khan et al. (2015), Khan et al. (2019), Khan et al. (2021), Balan et al. (2018) and Maikol et al. (2020), mutual authentication and specifically multifactor authentication mechanism is not a new research paradigm. Several researchers have proposed several methods to ensure secure authentication mechanisms in any communication protocols. With intelligent equipment and networks with high speed, the Internet of Things (IoT) gains wide awareness and acceptance. Smart Home (Baruah & Dhal, 2018) is the emerging major component of IoT. Globally, the market for the smart home is forecast to expand from 76.6 billion USD in 2018 to 12.02 percent in 2024, to USD 151.4 billion (*Smart Home Market by Product (Lighting Control, Security & Access Control, HVAC, Entertainment, Smart Speaker, Home Healthcare, Smart Kitchen, Home Appliances, and Smart Furniture), Software & Services, and Region*, n.d.).

The Smart Home IoT system offers clients connections to sensors, home appliances and smart devices, including Internet connectivity, remote monitoring, remote access and remote home control (Ali & Awad, 2018). By delivering a range of services, including energy conservation, security and health care, it delivers clients comfort and efficiency. As however, it is a huge problem for consumers to connect to smart home systems through a public route, i.e. the internet, and with resources-limited intelligent gadgets. For instance, an intelligent gadget could be utilized to determine the activity and presence of a person at a specific moment; an advertiser would be able to access the user's intelligent home monitoring system from a remote place (Barret, n.d.).

In another respect, it is a form of Internet service that IFTTT (IF This Then That) functions as a link between the phone of a person and the smart home (Baruah & Dhal, 2018; *WTF Is IFTTT?*, n.d.). IFTTT lets the user with various IFTTT recipes to remotely manipulate intelligent gadgets and set up the intelligent home. The recipes of IFTTT include phrases like 'If a member of the family comes home, move to the air conditioner.' IFTTT is an alternate technique and a promising framework for future Smart Homes (*WTF Is IFTTT?*, n.d.) to save consumers time and effort in routine, but repetitive, operation. The systems based on IFTTT are essentially a kind of third-party authentication technique. The strategy also incorporates the MFA system with three factors: user identification, password, and remote server-recognized user biometrics is a critical component of the secret process (Liu et al., 2020).

The proposed work can be extended to enhance end to end security mechanism in network intrusion detection system or malware detection system (Khan et al., 2020; Ahmad et al., 2021; Dildar et al., 2017; Khan et al., 2017).

2 Related works

WBAN is a wireless network of wearable devices that communicate with each other. WBANs are primarily used to collect and send patient data to a server. Security risk is a significant problem with potentially disastrous implications. Only the hash function and XOR operations are employed in this research to provide a lightweight and anonymous mutual authentication and key agreement mechanism for WBAN. The computational expenses are greatly decreased while providing maximum security by using the hash function and XOR procedures (Cui et al., 2020).

RFID (Radio Frequency Identification) is a wireless communication technology that is widely utilized in everyday life, including RFID-marked pharmacies and RFID microchips. The security challenges covered in this study include data security issues, personal privacy issues, and the illicit use of campus cards and mobile RFID, which are vulnerable to harmful assaults from the outside. Mutual authentication (bidirectional verification) and forward security are used to reduce the authentication overhead in these attacks. Several obstacles have also been uncovered throughout this research, including the phases of authentication procedure that rapidly alter to suit mobile RFID on the latest version (Xu et al., 2019).

A major Internet of Things component (IoT) collecting data from specific locations is the Wireless Sensor Network (WSN). In different communication circumstances, this hybrid approach enables mutual node-identity authentication through local blockchain, and public-blockchain authentication through the cluster-head node-identity authentication. This study essentially discusses a blockchain-based system for multi-WSN authentication of identity to address the single point failure of IoT standard authentication methods (Zheng et al., 2018).

Telecare medical information system (TMIS) delivers healthcare services to patients while also assisting health-care organizations with their demands. TMIS has a disadvantage when it comes to the privacy and integrity of patient data. As a result, several articles have presented and debated the optimal authentication techniques for dealing with the TMIS security problems (Deebak & Al-Turjman, 2021).

Smart Home is an Internet of Things (IoT)-based system that connects sensors, home appliances, and smart gadgets to allow a user to remotely track, explore, and manage a residential environment. Based on the IFTTT Smart Home device concept, a mutual authentication method and anti-tracking system was developed, in which the IFTTT home gateway authenticates distant users through an IFTTT server rather than conducting authentication or user registration as a trusted third party could. The compromise of the IFTTT server is one of the current problems for the planned solution (Lyu et al., 2019).

Vasudev et al. (2020) builds a lightweight shared authentication mechanism for an IoV situation using cryptographic procedures. IoVs communicate through an open wireless channel, which attracts attackers who can disrupt these sorts of communications.

NB-IoT is a narrowband Internet of Things, which can make mobile Internet standard popular and apply. The third-generation partnership project (3GPP) standards have been introduced to NB-IoT. The specifications of 3GPP enable hooks for non-radio access to and interaction with non-3GPP networks in the core network. However, problems with NB-IoT are still associated with the old authentication procedure of the standard user device to implement the mutual authentication between NB-IoT devices and 5G core networks, which provides plenty of communication and storage overhead. NB-current IoT's problem in the 3GPP 5G network is to be chosen as group leader in order to trust the proposed system. The future trend of NB-IoT devices is to reduce

energy consumption and cheap costs, a wide range of coverage and a great deal of capacity. The scheme offered is to make the user easier (Cao et al., 2019).

3 Proposed solution

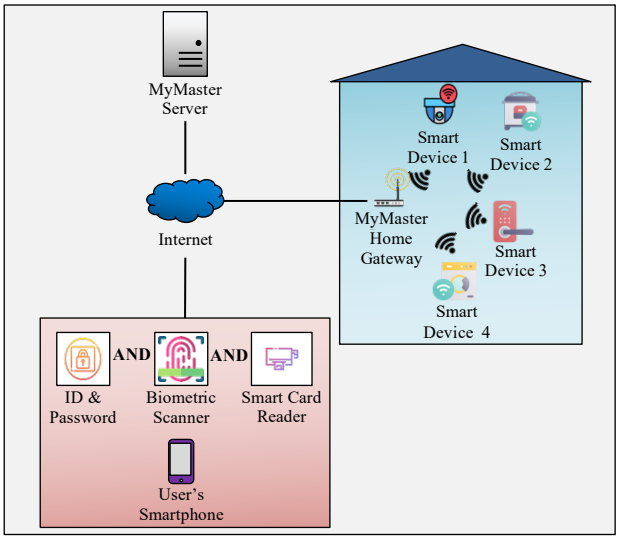

Figure 1: Proposed Smart Home System Environment

3.1 Assumptions

1) Registered users, smart phones, and the server are assumed to be trusted. After successfully registered, user will have a profile and account in the home network.

2) The home gateway will allow only the registered user and registered smart devices to communicate with the home gateway. All of the smart phones and registered smart devices must go through the registration phase in order to communicate with the home gateway.

3) A unique identification key, called private key will be assigned to each of the registered smart phones. Besides, the communication between the user's smart phone, home smart devices, and trusted server is expected to be done through a local or private channel.

3.2 Initial Registration

There will be two different registration categories:

1) *MyMaster home gateway*: MyMaster Home Gateway need to be registered after its installation. All the smart devices need to be registered with the MyMaster server. Once successfully registered, an unique identity, a secret key and a key identifier will be assigned to each registered devices. Before the registration, the registration status should appear as "Not Registered". All the registration details will be stored securely in the MyMaster server.

2) *User*: A user can register only a single account. There are three phases they need to go through. First, they need to set a password and id for their account. Second, they need to scan either their fingerprint or their facial. Lastly, they need to have a smart card that had been registered to the MyMaster server.

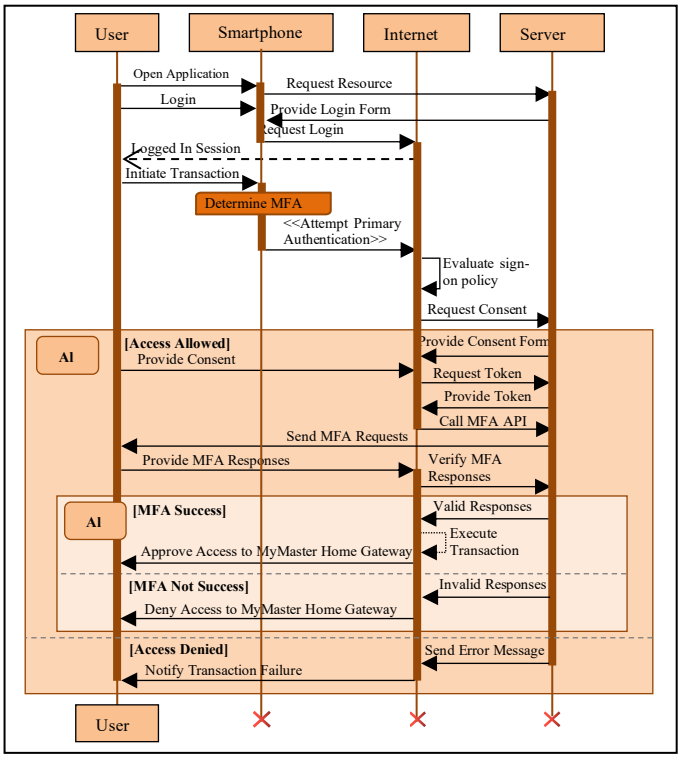

Figure 2: Proposed Authentication Scheme Flow

3.3 Step-by-Step

Step 1: To begin the process user will first open the application before the authentication process begins. The application will send resource request to the server. The user will then login into the application to begin the process.

Step 2: To use the smart device user will initiate a transaction to authenticate themselves before they can use the smart device. The user will first attempt primary authentication and evaluate sign-on policy, this process will be a one-time process only which is when the user first uses the application. This is to make sure if the user agrees to give consent for their information to be store on the server. The consent form will be sent to the user once the primary authentication process is initiated.

Step 3: After the consent is provided by the user, internet will then send a token request for service identification. A timestamp will be appended to the token to prevent replay attack. The server will then provide a token. Next, multifactor (MFA) API will be called, and the server will send an MFA request to the user.

Step 4: To provide an MFA response user will first need to enter their ID and password. Once successful, the user will need to either scan their fingerprint or face for the biometric phase. The third phase will be authentication by smart card which is a sim card, user will need to enter the OTP or one-time password provided for verification purposes. The MFA response will then be verified by the server.

Step 5: The response will be considered valid if all three phases are successful. Once the response is valid the access to the home gateway will be approved. If the server sends an invalid response request the access to the home gateway will be denied. The server will send an error message and notify user of transaction failure.

4 Security analysis

Our proposed scheme shows that we can avoid from the attack happen.

1) *User Impersonation Attack*: From our purposed scheme it shows that we have used tighten multi-factor authentication in order to avoid from user impersonation. We had chosen to use ID and password, biometric scanner and also smart scan for the system authentication. This authentication occurs when user want to login the system. The multi-factor authentication protocol will help legitimate user to access the system securely by

enter all the authentication correctly. This process will only allow the legitimate user to access and use the system. So, this proposed scheme will be opposed user impersonation attack.

2) *Home Gateway Impersonation Attack*: In our proposed scheme, authentication for home gateway required for the security of network. This authentication help to avoid adversary from try connecting the network by impersonate home gateway. Home gateway only allow legitimate users and registered devices connect to the system. After the devices and user have been verified, they will be allowed to access the system. If the other devices that doesn't registered yet and want to access to the system, the system will deny the connection. Hence, it will be impossible for adversary to attack the system. Consequently, the proposed scheme resists home gateway attack.

3) *Network Attack*: Our proposed scheme can resist network confidential attack by assigned private key for each device that have been registered. This is to ensure network cannot be access by the adversary. Other than that, we choose to use local or private network that only can be access by registered devices. So that attacker cannot cause the server crash and non-legitimate users cannot access the system without the permission. The network can be reduced from exposed to the attack when the network not sharing with another network. Therefore, the proposed scheme is secure from network attack (Coppolino et al., 2015).

5 Complexity analysis

Computation and communication costs will be used to measure the performance of the schemes. The computation cost is the time it takes to execute the needed operations, while the communication cost is the number of bits sent across the communication channel. In this section, we compare the computation and communication costs of the proposed scheme with schemes from our related works, such as the schemes of Lyu et al. (2019), Vasudev et al. (2020), and Zheng et al. (2018) in the authentication phase.

The computational cost is calculated based on the time it takes by the IFTTT server to complete certain tasks. We use the work of Oh et al. (2021) to compare. The proposed scheme has a greater computational cost than the schemes established by Vasudev et al. (2020) and Zheng et al. (2018) because the proposed scheme uses extra devices and we introduce the login using ID and password, biometrics scanner, and smart card to enhance security which significantly increases the computational cost. It can still be considered as our scheme provides more security and privacy. Furthermore, the proposed scheme's computational cost is lower than that of Lyu et al. (2019). This is because Lyu et al. (2019) applies the elliptic curves' cryptography (ECC) algorithm which has a higher level of computational complexity to ensure a more private and secure scheme.

Communication overhead is the portion of time spent to communicate with team members rather than completing productive work. Communication is needed, but as team grows, so does the overhead communication (Kaufman, 2005). Dr Michael Sutcliffe from University of Cambridge has proposed "8 Symptoms of Bureaucratic Damage" that appear in teams suffering from Communication Overhead includes Nothing New-There are no radical ideas, inventions or lateral thinking-a general lack of initiative and Pseudo-Problems-Minor issues become magnified out of all proportion which can be found in Lyu et al. (2019) and Oh et al. (2021).

The communication cost is evaluated based on the number of bits sent across the communication channel. We use the work by Oh et al. (2021) to compare. Table 2 contains the result of the communication costs comparison. To conclude, the comparison shows that our scheme is comparatively more cost-efficient than the other schemes in terms of the total number of bits transmitted. Our scheme requires 2080 amount of bits for effective mutual authentication while being the most secured scheme compared to Lyu et al. (2019), Vasudev et al. (2020), and Zheng et al. (2018).

With the increasingly growing application of intelligent terminals, servers will be more powerful, these costs do not have a great effect on the performance. Overall, the proposed scheme is more secure and private than existing schemes, and it is a viable option for protecting smart home environments.

Table 1: Computational cost comparison in ms

Authentication scheme	Computational cost (ms)
Lyu et al.	77.540
Vasudev and Das	0.0340
Xu et al.	0.0624
Proposed scheme	0.168

Table 2 : Computational cost comparison in bits

Authentication scheme	Computational cost (bits)
Lyu et al.	2816
Vasudev and Das	2496
Xu et al.	3904
Proposed scheme	2080

6 Conclusions

Most of the previous work mention involved in proposed model in mutual authentication. Since there are no works on multi factor authentication (MFA), we proposed Smart Home System Environment. Moreover, due to the multi-factor authentication, the proposed scheme can resist several attacks such as user impersonation, home gateway attack, and by assigning a private key to each device that has been registered, our proposed scheme can withstand network confidential attack. This is to guarantee that the attacker cannot gain access to the network. The proposed model includes extra devices and have the login utilizing ID and password, biometrics scanner, and smart card to strengthen security, which considerably raises the computational cost. Overall, the proposed scheme is more secure and private than existing schemes, and it might be a feasible option for protecting smart home environments.

Acknowledgements

The authors would like to thank Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak to support this research work. This work is carried out as a short-term research-based project.

References

Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2020). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), e4150. https://doi.org/10.1002/ett.4150

Ali, B., & Awad, A. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. Sensors, 18(3). https://doi.org/10.3390/s18030817

Balan, K., Khan, A. S., Julaihi, A. A., Tarmizi, S., & Pillay, K. S. (2018). RSSI and Public Key Infrastructure based Secure Communication in Autonomous Vehicular Networks. International Journal of Advanced Computer Science and Applications, 9(12), 298–304. https://doi.org/10.14569/ijacsa.2018.091243

Barret, B. Hack Brief: Hacker Strikes Kids, Gadget Maker VTech to Steal 5 Million Accounts. WIRED. Accessed: Sep. 25, 2018. [Online]. Available: https://www.wired.com/2015/11/vtech-childrens-gadget-maker-hack-5- million-accounts/

Baruah, B., & Dhal, S. (2018). A two-factor authentication scheme against FDM attack in IFTTT based Smart Home System. Computers & Security, 77, 21–35. https://doi.org/10.1016/j.cose.2018.03.004

Cao, J., Yu, P., Ma, M., & Gao, W. (2019). Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network. IEEE Internet of Things Journal, 6(2), 1561–1575. https://doi.org/10.1109/jiot.2018.2846803

Coppolino, L., D'Alessandro, V., D'Antonio, S., Levy, L., & Romano, L. (2015). My Smart Home is Under Attack. 2015 IEEE 18th International Conference on Computational Science and Engineering, 145–151. https://doi.org/10.1109/cse.2015.28

Cui, Z., Xue, F., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN. IEEE Transactions on Services Computing, 13(2), 241–251. https://doi.org/10.1109/tsc.2020.2964537

Deebak, B. D., & Al-Turjman, F. (2021). Smart Mutual Authentication Protocol for Cloud Based Medical Healthcare Systems Using Internet of Medical Things. IEEE Journal on Selected Areas in Communications, 39(2), 346–360. https://doi.org/10.1109/jsac.2020.3020599

Dildar, M. S., Khan, N., Abdullah, J. B., & Khan, A. S. (2017). Effective way to defend the hypervisor attacks in cloud computing. 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), 154–159. https://doi.org/10.1109/anti-cybercrime.2017.7905282

Kaufman, J. (2005). Communication Overhead - The Personal MBA. The Personal MBA. https://personalmba.com/communication-overhead/#:%7E:text=Communication%20Overhead%20is%20the%20proportion,increases%2C%20so%20does%20Communication%20Overhead

Khan, A. S., Ahmad, Z., Abdullah, J., & Ahmad, F. (2021). A Spectrogram Image-Based Network Anomaly Detection System Using Deep Convolutional Neural Network. IEEE Access, 9, 87079–87093. https://doi.org/10.1109/access.2021.3088149

Khan, A. S., Balan, K., Javed, Y., Tarmizi, S., & Abdullah, J. (2019). Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. Sensors, 19(22), 1. https://doi.org/10.3390/s19224954

Khan, A. S., Javed, Y., Abdullah, J., & Zen, K. (2021). Trust-based lightweight security protocol for device to device multihop cellular communication (TLwS). Journal of Ambient Intelligence and Humanized Computing. Published. https://doi.org/10.1007/s12652-021-02968-6

Khan, A. S., Lenando, H., Abdullah, J., & Fisal, N. (2015). Secure Authentication and Key Management Protocols for Mobile Multihop WiMAX Networks. Jurnal Teknologi, 73(1), 75–81. https://doi.org/10.11113/jt.v73.3258

Khan, N., Abdullah, J., & Khan, A. S. (2017). Defending Malicious Script Attacks Using Machine Learning Classifiers. Wireless Communications and Mobile Computing. Published. https://doi.org/10.1155/2017/5360472

Liu, W., Wang, X., & Peng, W. (2020). Secure Remote Multi-Factor Authentication Scheme Based on Chaotic Map Zero-Knowledge Proof for Crowdsourcing Internet of Things. IEEE Access, 8, 8754–8767. https://doi.org/10.1109/access.2019.2962912

Lyu, Q., Zheng, N., Liu, H., Gao, C., Chen, S., & Liu, J. (2019). Remotely Access "My" Smart Home in Private: An Anti-Tracking Authentication and Key Agreement Scheme. IEEE Access, 7, 41835–41851. https://doi.org/10.1109/access.2019.2907602

Maikol, S. O., Khan, A. S., Javed, Y., Bunsu, A. L. A., & Petrus, C. (2020). A novel authentication and key agreement scheme for countering MITM and impersonation attack in medical facilities. International Journal of Integrated Engineering, 13(2), 127–135.

Oh, J., Yu, S., Lee, J., Son, S., Kim, M., & Park, Y. (2021). A Secure and Lightweight Authentication Protocol for IoT-Based Smart Homes. Sensors, 21(4), 1488. https://doi.org/10.3390/s21041488

Smart Home Market by Product (Lighting Control, Security & Access Control, HVAC, Entertainment, Smart Speaker, Home Healthcare, Smart Kitchen, Home Appliances, and Smart Furniture), Software & Services, and Region. (n.d.). Global Forecast to 2024. https://www.marketsandmarkets.com/Market-Reports/smarthomes-and-assisted-living-advanced-technologie-and-global-market121.html

Vasudev, H., Deshpande, V., Das, D., & Das, S. K. (2020). A Lightweight Mutual Authentication Protocol for V2V Communication in Internet of Vehicles. IEEE Transactions on Vehicular Technology, 69(6), 6709–6717. https://doi.org/10.1109/tvt.2020.2986585

WTF is IFTTT? (n.d.). IFTTT. https://ifttt.com/explore/new_to_ifttt

Xu, Z., Xu, C., Liang, W., Xu, J., & Chen, H. (2019). A Lightweight Mutual Authentication and Key Agreement Scheme for Medical Internet of Things. IEEE Access, 7, 53922–53931. https://doi.org/10.1109/access.2019.2912870

Zheng, L., Song, C., Cao, N., Li, Z., Zhou, W., Chen, J., & Meng, L. (2018). A New Mutual Authentication Protocol in Mobile RFID for Smart Campus. IEEE Access, 6, 60996–61005. https://doi.org/10.1109/access.2018.2875973