Scientific Journal of Impact Factor (SJIF): 4.72
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406
International Journal of Advance Engineering and Research Development
Emerging Trends and Innovations in Electronics and Communication Engineering - ETIECE-2017
Volume 5, Special Issue 01, Jan.-2018 (UGC Approved)

HMACSHA256 With RSA For Ensuring Secure Communication In IoT Based Smart Home System

Idris Afzal Shah [1], Faisal Rasheed Lone [2], Syed Arshid Ahmad[3], Faizan Amin Malik[4], Hamid Hussain Haqani[5]

[1]*Department of CSE, University of Kashmir*
[2]*Department of CSE, University of Kashmir*
[3]*Programmer,NIC*
[4]*Department of Computer Science, University of Kashmir*
[5] *Department of Computer Science, University of Kashmir*

ABSTRACT- *Smart Home Systems are becoming the vogue now. It will not be an understatement/aberration to say that given the revolution internet has already brought in our lives and the impact that novel concepts and technologies like that of IoT is having in our day-to-day activities, the day is not far when virtually every real world system and for that matter be a typical home system will change in the way we interact with them. The aim of our paper is to ensure secure communication in a smart home system. We are assuming a scenario wherein the tasks performed by an end user are mostly confined to ON/OFF mechanism, so that we put no emphasis on preserving the confidentiality of message sent by the end user. However ensuring authentication and integrity of message is of prime importance. To ensure this we have used HMACSHA256 hash function at the user level. However, at the data repository/server level where all the scripts intended to perform the user operation are stored, the focus of attention is confidentiality which is ensured by using RSA. We have implemented our proposed framework using Raspberry Pi Computer.*

Keywords- *; IoT, Smart home, HMAC, SHA-256, RSA.*

I. INTRODUCTION

The “Internet of things” (IoT) has gained wide acceptance/prominence in the public and private domains in the current era of computing. It has had its impact on our lifestyle. In future, it will completely change the way we live and work. It has given a new dimension to how we interact with our day-to-day things. Any device having an on and off mechanism can be connected to the Internet and be a part of IoT. This encompasses almost everything one can think of be it Lights, Television sets, Heating/ cooling systems, coffee makers, washing machines, wearable gadgets etc. According to many industry analysts including Gartner estimate the number of IoT enabled devices could reach to 26 billion devices by 2020[1].The essence of the Internet of Things (IoT) is to make computing ubiquitous. It is because of this reason that IoT is being seen as a future prospect for both the economy as well as the individuals. Sensors and IoT enabled devices work in tandem and with the help of their networking capabilities they are able to communicate with each other as well interact with people to be accessed, monitored and managed remotely. Forerunners of this revolution are already apparent in this day and age and with each new day, the endeavour is to make more and more devices a part of the IoT [2].A “smart home” can be defined as a residence that incorporates various computing devices and sensor networks that are used to keep track of our daily appliances. All these devices are connected in a seamless fashion such that the needs of the occupants are met in a convenient manner. Any device having ON/ OFF mechanism can be connected to the Internet for remote access. So, pertaining to our Home system, there are many such devices that can be accessed and controlled using IoT. Such devices include lighting systems, heating systems, media and entertainment systems and several others[3][4].

II. HMAC

Message Authentication Codes are widely used in applications wherein the focus of attention is integrity and authenticity of a message and not confidentiality. A simple example could be uploading a video on a Video Blog where we want the content to be public but at the same time, we want to make sure no one would be able to tamper with it.
One of the most commonly used MAC is HMAC (Hashed Message Authentication Code). It is already being used in many protocols like IPSec, SSL etc. HMAC makes use of a Hash function along with a secret key. There are many Hash Functions that can be used such as MD-5, SHA-1, SHA-2 etc.Depending upon the Hash function used, the MAC produced by HMAC will vary accordingly[5].

The operation of the HMAC algorithm is shown below:

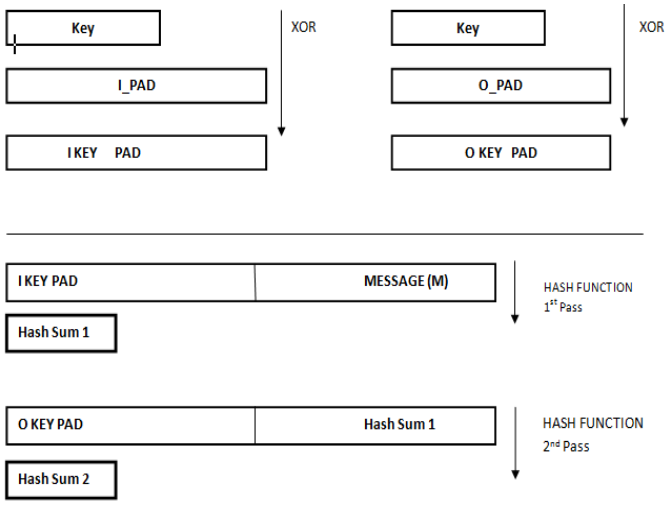


Figure 1. HMAC Algorithm

Where Key is the shared secret. (1)
I_PAD and O_PAD refer to inner and outer padding. (2)
M is the input message. (3)
The operation of HMAC is described by: $\mathrm{HMACK(M)} = \mathrm{h((K \oplus opad)||h(K \oplus ipad)||M))}$ (4)
Where h() is the iterated hash function[6][7][8].

III. SHA256

SHA stands for secure hash algorithm. SHA256 is one of the functions of SHA2 family. SHA-256 is a cryptographic hash function with digest length of 256 bits. It is used to verify the integrity of the message. The SHA-256 algorithm makes use of eight 32-bit sub-blocks. The input message (M) is padded, and divided into several blocks each 512-bits[9]. The following diagram depicts SHA256 compression function.

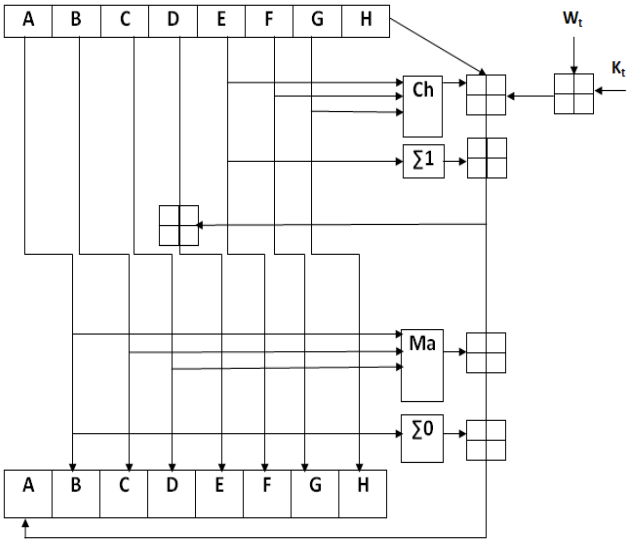


Figure 2. SHA256

The various functions performed by various components are as follows:

$$\mathrm{Ch(E,F,G)} = (\mathrm{E} \wedge \mathrm{F}) \oplus (\sim \mathrm{E} \wedge \mathrm{G}) \quad (5)$$

$$\mathrm{Ma(A,B,C)} = (\mathrm{A} \wedge \mathrm{B}) \oplus (\mathrm{A} \wedge \mathrm{C}) \oplus (\mathrm{B} \wedge \mathrm{C}) \quad (6)$$

$$\sum_0(\mathrm{A}) = (\mathrm{A} \gg 2) \oplus (\mathrm{A} \gg 13) \oplus (\mathrm{A} \gg 22) \quad (7)$$

$$\sum_1(\mathrm{E}) = (\mathrm{E} \gg 6) \oplus (\mathrm{E} \gg 11) \oplus (\mathrm{E} \gg 25) \quad (8)$$

The ⊞ is addition modulo 2^{32}.

IV. RSA

RSA is primarily an asymmetric encryption /decryption Algorithm proposed by Rivest, Shamir, and Adleman. It is called asymmetric because the public key (used to encrypt the message) and the private key (used for decryption) is kept secret and is not shared to public. The RSA cryptosystem is believed to be the most widely-used public key cryptography algorithm in the world[10]. RSA algorithm is used for public key encryption and also digital signatures. The main security aspect of this algorithm is based on the difficulty of factoring large integers. User 1 can send a message in an encrypted format to User 2 without any prior knowledge of secret keys. User 1 simply uses User 2's public key to encrypt the message and User 2 decrypts it using the private key, which is only known to the later.
RSA can also be used to sign a message, so User 1 can sign a message using its private key and User 2 after receiving the message can verify it using the public key of User1.
RSA Algorithm

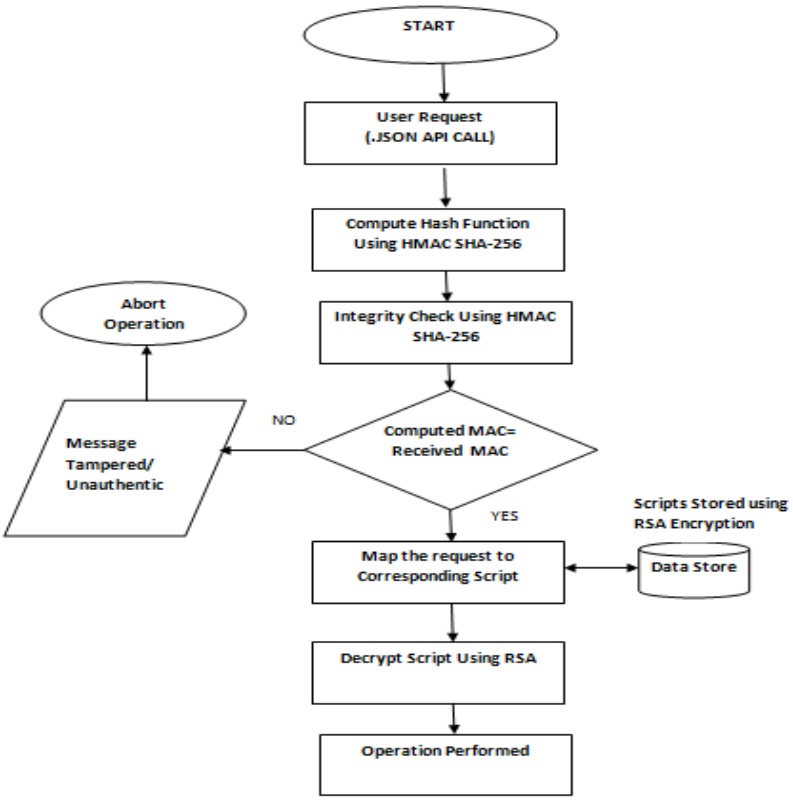
Generate two large distinct prime numbers, p and q. (9)
Compute modulus n = pq. (10)
Compute totient $\varphi(n)=(p-1)(q-1)$ (11)
Choose an integer e, $1 < e < \varphi(n)$, such that e and n are coprime. (12)
Compute the secret exponent d,where $1 < d < \varphi(n)$ such that $(d*e)\% \varphi(n)=1$. (13)
The public key is (e,n) and the private key is (d,n). (14)
Ciphertext is given by $C=M^e \bmod n$. *(15)*
Plaintext is $M=C^d \bmod n$ (16)

V. PROBLEM DOMAIN

A typical smart home system is comprised of many components linked together in a network that is connected to Internet for remote access and monitoring. Therefore, such systems can be exposed to many security threats. The operations generated by the end user can be prone to attacks. A malicious attacker can intercept the messages (operations) generated by the end user and tamper it in such a way such that it can sabotage the whole system. This can really prove hazardous in a smart home system as there are many appliances with a high degree of risk factor.
Tampering with the message generated by the end user by just changing its device ID number can really prove catastrophic in a smart home system. The attacker may tamper with the message in a way such that he can invoke the operation intended by the user on a different device. This can really pose a serious concern. Imagine an end user invoking an operation to turn on a light and in turn a heating system is switched on.
Moreover, a malicious attacker can hack into the Home controller system where all the scripts intended to perform the user operations are stored and compromise the integrity of the data stored. It may result in serious consequences as many operations in a smart home system have stringent time constraints. Hence, ensuring a secure communication in an IoT based smart home system is critical.

VI. PROPOSED METHODOLOGY

The aim of this paper is to ensure secure communication in a smart home system. We have already given a brief description of the concepts namely HMAC, SHA-256 and RSA that will be used in our proposed framework. As already stated above, we are assuming that the operations invoked by the end user is confined to an on/ off mechanism such that we lay no emphasis on preserving the confidentiality of the message however we want to ensure the authenticity and integrity of the message. To achieve this goal, we have used HMAC with Hash function SHA-256. On the other hand, the confidentiality of the scripts stored on the server is pivotal. We have encrypted the scripts using RSA algorithm.
We have implemented the proposed methodology using Raspberry-pi computer that acts as the Main home controller to handle all the operations across the devices and stores the scripts for various operations in an encrypted form using RSA. A user connects to the Home controller from the Internet to invoke operations on various devices. The User to device communication is accomplished using API calls with the help of .JSON files. Hash-based Message Authentication Codes (HMAC) using the SHA256 hash function are computed on the API calls generated by the user from the end device before being transmitted to the home controller. The home controller will check the authenticity and integrity of the message based on HMAC SHA-256. Then the script to be invoked for the requested operation is decrypted using RSA Algorithm and then invoked. After successful operation, the user is notified accordingly.



.

Figure 3. Proposed Algorithm

VII. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a framework for secure communication in IoT based smart home systems. At the user end, our focus of attention has been ensuring message authentication and integrity. Also, at the server end, we have ensured that an intruder is not able to compromise our scripts by storing them in an encrypted form. We have put forward a robust scheme that combines the advantages of HMAC, SHA-256 and RSA Algorithm to ensure a secure environment in smart home systems.

REFERENCES

[1]http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#53541a366828
[2] Weiser M.: The Computer for the 21st Century. Scientific American 265(9):66–75 (1991)
[3] J. A. Stankovic "Research directions for the Internet of Things "IEEE Internet Things J., vol. 1, no. 1, pp. 3-9,*Feb., 2014*
[4] J. Holler, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand and D. Boyle From Machine-to-Machine to the Internet of Things:
Introduction to a New Age of Intelligence*2014*, Elsevier.
[5] James M.Turner,Deparity Director.National Institute of Standard and Technology.The Keyed-Hash Message Authentication Code(HMAC),March,2008;
[6] ISO/IEC 9797-1 Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a
block cipher, 1999.
[7] ISO/IEC 9797-2 Information technology - Security techniques - Message Authentication Codes (MACs) - Part 2: Mechanisms using a
hash- function, 2000.
[8] ISO/IEC 9798-1 Information technology - Security techniques - Entity authentication mechanisms - Part 1: General, 1997.
[9] Federal Information Processing Standards Publication 180-3, "SECURE HASH STANDARD", October 2008
[10] R.L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM, Feb. 1978, 21(2): 120-126.

