Group Authentication for Smart Environments Using Cryptography Method of RSA And Blow Fish

Dhivya S  
M. Phil., Research Scholar,  
Department of Computer Science  
dhivyasivam27@gmail.com  
Kovai Kalaimagal College of Arts Science, Coimbatore  
Bharathiar University, Coimbatore, Tamil Nadu, India.

Jawahar S  
Assistant Professor, Department of Computer Science  
Shivamjawahar@gmail.com  
Kovai Kalaimagal College of Arts Science, Coimbatore  
Bharathiar University, Coimbatore, Tamil Nadu, India.

ABSTRACT: Smart environments aim to satisfy the experience of individuals from every environment, by replacing the hazardous work, physical and repetitive tasks with automated manner. A smart home consists of low capacity devices and wireless networks, and therefore, all working together as a secure system that needs an adequate level of security. Smart home opens up an attack surface as the SDs data collected and communicated over insecure wireless networks, leaving them vulnerable to security attacks. To obtain a satisfactory level of security, here presents a lightweight and secure session key establishment scheme using Cryptography-based Group Authentication. This scheme established a group authentication scheme also which ensures the simultaneous authentication of all the members of a group using threshold cryptography but also established a secret session key which can be used for communication that might occur in group oriented applications. To establish group authentication of devices in smart home it will provide a better security. here RSA and Blow fish algorithm were used to solve security issues.

Keywords: Smart home network, IOT, Security, Group Authentication and Cryptography Method.

I. INTRODUCTION

The smart home is an environment, where heterogeneous electronic devices and appliances are networked together to provide smart services in a ubiquitous manner to the individuals, organization and people are wide accepting and adopting the functionalities offered by the smart home applications. this can be because of the various advantages, in easing users’ everyday life and work, provided by the rising internet of Things (IoT) technologies and devices, equipped with sensors, cameras, or actuators, and able either to accumulate information from the environment or to perform proper tasks [1], the main features of smart homes embrace real-time monitoring, remote control, safety from intruders, gas/fire alarm, and so on. Since among smart homes, sensitive and personal data are managed, security and privacy solutions should be put in place, to protect users/businesses’ data against violation try still on guarantee the supply of reliable services. A smart home environment is meant to be a small physical world, consisting of different devices, including sensors, actuators, displays and computational elements interacting and exchanging information with users to provide them with automated, customized, and secured services. These types of environments are designed to make life better and secure through information processing, automation and personalized services [2]. The potential of smart home environments is huge; for example, smart homes are mainly designed for old-age people because such homes are capable of sensing, processing and relaying their important health information and communicating the data through integrated devices and networks to protectors. Fig. 1, shows a typical smart home architecture. Fundamentally, we regard a smart connected home as composed of devices,
communication, and services. The IoT smart home services are increasing day by day, digital devices can effectively communicate with each other using Internet Protocol (IP) addresses. All smart home devices are connected to the internet in a smart home environment. As the number of devices increases in the smart home environment, the chances of malicious attacks also increase. If smart home devices are operated independently the chances of malicious attacks also decreases [3].

Fig 1: Smart home Architecture

Presently smart home devices can be accessed through the internet everywhere at any time. So, it increases the chances of malicious attacks on these devices. A smart home consists of four parts: the service platform, smart devices, home gateway, and a home network. In the smart home, many devices are connected and smartly shares information using a home network. The home environments and networks are used interchangeably. Most of the devices are having resource-limitations. However, in such home networks, the Smart Devices (SDs) communicate over the wireless channels through the local home gateway. The home gateway acts as a bridge between the SDs and the users, and provides interoperability and control for the SDs, connect to the outer world via the Internet [4]. Thus, the qualities of SDs are enabling users to operate homes remotely/directly using the smart phones, tablets, or through designated web apps, anywhere and anytime [5]. The recognize that notions of privacy are situated in the everyday contexts of home routines, including the relationships between household members, and that our study captures only a snapshot of the privacy preferences and expectations of users based on their knowledge and expectations of entities not typically involved in day-to-day home life [6, 7]. Availability confirms that network services and that the resources are available and protected against malicious attacks. Especially, the Smart Home internal network is most vulnerable to direct denial of service (DOS) attacks, because of its availability to Internet. However, this paper proposes a cryptography method of security to the Smart home device with the session key management scheme. The organization of this paper is as follows. In section 1 provides the introduction about our concept, Section 2 holds a literature review section, it shows various authors approaches, in Section 3 discussed about problem statement from existing work, in Section 4 provided about our proposed approach, in Section 5 proposed work experimental result and finally Section 6 contains the a conclusion about this paper.

II. LITERATURE REVIEW

Rishi Sairam et al [8] dissect the period of smart gadgets or things which are energizing the development of Internet of Things (IoT). It is affecting each circle around us, making our life reliant on this mechanical accomplishment. It is of high worry that these smart things are being focused by digital lawbreakers exploiting heterogeneity, minute security highlights, and vulnerabilities inside these gadgets. Regular concentrated IT security measures have constraints as far as adaptability and cost. Thusly, these smart gadgets are required to be checked nearer to their area in a perfect world at the edge of IoT systems. In this paper, we investigate how some security highlights can be executed at the system edge to verify these smart gadgets in a smart home/endeavor condition. We clarify the significance of system work virtualization (NFV) so as to send security capacities at the system edge. To accomplish this objective, we present NETRA-a novel lightweight docker-based engineering for virtualizing system capacities to give IoT security. Additionally, we feature the upsides of the proposed design over the institutionalized NFV engineering as far as capacity, memory use, dormancy, throughput, load normal, and adaptability and clarify why the institutionalized design isn't reasonable for IoT. We study the exhibition of proposed NFV-based edge examination for IoT security and demonstrate that assaults can be recognized with over 95% exactness in under a second.

Rixin Xu ; Qiang Zeng ; et al [9] Analyze the mix of smart home stages and mechanization applications acquaint numerous accommodations with smart home users. Notwithstanding, this likewise brings the capability of
protection spillage. On the off chance that a smart home stage is allowed to gather every one of the occasions of a user day and night, at that point the stage will gain proficiency with the personal conduct standards of this user after a short time. In this paper, we examine how IFTTT, one of the most well known smart home stages, has the capacity of checking the day by day life of a user in an assortment of ways that are not really observable. Also, we propose numerous thoughts for moderating protection spillages, which all together structure a "Channel and Fuzz" (F&F) process: first, it sift through occasions unneeded by the IFTTT stage. At that point, it fuzzifies the qualities and frequencies of the rest of the occasions. We assess the F&F procedure and the outcomes demonstrate that the proposed arrangement makes the IFTTT incapable to perceive any of the user's personal conduct standards.

Waqar Ali et al [10] explore security assaults in smart home and assess their effect on the general framework security. Internet of Thing (IoT) is going to make such a reality where physical things (smart home machines, and smart watches and so forth.) changed the information systems and administrations giving frameworks which give inventive and smart administrations to human. With smart home innovation, our living region is winding up increasingly agreeable and helpful. Smart home innovation gives robotized, savvy, smart, creative and universal administrations to private users through Information Communication Technology (ICT). Because of internet-connected, dynamic and heterogeneous nature of smart home condition makes new security, validation and protection challenges. Creator distinguished security prerequisites and arrangements in the smart home condition. In light of a few situations, we propose to set security objectives for the smart home condition. In light of verifiable data, we conjecture security assaults (like malware, infection and so forth.) and assessed that what number of assaults are required to be propelled in coming years.

Shafiq ur Rehman; Volker Gruhn et al [11] propose a protected design for smart homes. Smart homes likewise help older individuals; they can deal with the home with effortlessness from their remote or smart gadget which is connected up to focal gadget that is connected with home mechanization. Security is the fundamental concern while keeps up the smart homes, these days programmers don’t have to make a trip to focused homes, they can approach for all intents and purposes to assault smart homes effectively. We included a sicher firewall framework between a focal center (LAN) that are connected to the internet and opposite end that is connected with home machines. Along these lines security dangers become down and out and assailants can't arrive at home mechanization frameworks. A sicher firewall additionally shields framework from internet dangers. It creates an admonition and shield framework from outer dangers. Applying a sicher firewall, it implements security framework and increment security and covering to smart homes. This experience will upgrade user reliability for utilizing smart homes innovation.

Arunmozhi Manimuthu; Ramadoss Ramesh et al [12] fundamentally explores the verified data stream in HAN and guarantees data security of users during basic and crisis tasks. Data are made accessible progressively with least travel time delay. Gadgets are ceaselessly checked for indispensable and crisis administrations. This paper centers around machine to machine data stream and bundle conveyance utilizing IoT. It helps in making user's capacity utilization data accessible over the cloud and furthermore in redefined electronic gadgets progressively. This examination work exhibits the necessities for building up a savvy IoT-HAN connected with smart lattice for vitality mindful directing. The propelled structure plan places sensors, and control door in a well-characterized limit, devouring less vitality for data move and data handling. Data stream example and bundle conveyance rate is tried utilizing both recreated and genuine data from sensors and concentrators. The got outcomes and stream example is assessed utilizing MATLAB and system test system. The created IoT-HAN arrangement is ideally useful in verified data trade among various connected gadgets inside HAN.

III. PROBLEM DEFINITION

In existing work considers a lightweight and secure session key foundation scheme for smart home systems and fuses the Diffie-Hellman (DH) key trade as an elective technique. Availability confirms that system services and that the assets are accessible and secured against malignant attacks. Particularly, the Smart Home inward system is most defenceless against direct denial of service (DOS) attacks, due to its accessibility to Internet. In any case, one issue here is that each time another device should be introduced it must be enrolled offline with the service supplier, to have the security parameters put away, which might be troublesome. Offline communication with the service is troublesome [13]. Classification is security instrument that verifies the system by keeping unapproved parties from getting to the data created in smart home Environment. Less Authentication in service identified with affirming genuine character of an individual dependent on a secret phrase or mystery key shared between the communication parties.
IV. PROPOSED WORK

A smart home opens up an attack surface as the Smart Devices (SDs) data collected and communicated over insecure wireless networks, leaving them vulnerable to security attacks. To obtain a satisfactory level of security, here presents a lightweight and secure session key establishment scheme. It allows each entity should be performed a light-weight mutual authentication prior participation in the home network and establish a session key in a secure manner. This scheme uses the symmetric key cryptography and a hash function to compliment other techniques in order to provide more security in the smart homes [14]. In addition, a new device can be easily entered arbitrarily and securely into the scheme to extend the smart home services.

This proposed scheme gives significant security properties including avoidance of different well-known attacks, for example, disavowal of-service and listening stealthily attack. Notwithstanding this security attacks group authentication can likewise centre in this proposed work. A smart home can fill in as a group that speaks with a service supplier (which updates that group), or with a neighbouring group, or a solitary user-device group, in a WBAN environments. In any case, if the quantity of devices in a group increments, or when numerous devices must convey all the while, authentication of all devices is required during every session to guarantee that communication is secure [15]. Profoundly productive group authentication innovation is in this way required. Here, we build up a group authentication and key trade scheme that works effectively in lightweight devices inside a group-based IoT smart metering environment. As the quantity of devices in the group expands, the quantity of communications in the group chief generally turns out to be exceptionally enormous. In this manner, we structure our scheme to guarantee that the group head connects with an authentication server to guarantee key understanding. Additionally, we build up a key trade procedure creating and appropriating group keys after group authentication, by means of an edge mystery sharing scheme; this diminishes the group communication overhead.

This proposed scheme gives significant security properties including avoidance of different well-known attacks, for example, disavowal of-service and listening stealthily attack. Notwithstanding this security attacks group authentication can likewise centre in this proposed work. A smart home can fill in as a group that speaks with a service supplier (which updates that group), or with a neighbouring group, or a solitary user-device group, in a WBAN environments. In any case, if the quantity of devices in a group increments, or when numerous devices must convey all the while, authentication of all devices is required during every session to guarantee that communication is secure [15]. Profoundly productive group authentication innovation is in this way required. Here, we build up a group authentication and key trade scheme that works effectively in lightweight devices inside a group-based IoT smart metering environment. As the quantity of devices in the group expands, the quantity of communications in the group chief generally turns out to be exceptionally enormous. In this manner, we structure our scheme to guarantee that the group head connects with an authentication server to guarantee key understanding. Additionally, we build up a key trade procedure creating and appropriating group keys after group authentication, by means of an edge mystery sharing scheme; this diminishes the group communication overhead.

Fig 2: Proposed Architecture overview

a. AUTHENTICATION PROCESS

Authentication module plays out the module authentication process. The authentication module in the system confirms all modules when a smart device is controlled on. The authentication procedure is matching procedure. In the system, basic data are transmitted after authentication between devices. End-user’s security administrator gives security provisioning and support service for devices. A session is set up between the utilizations of devices for data transmission. Authentication is performed with the utilization of a group key and a testament. Confirmed devices transmit the messages encoded with a given strategy. It utilizes the authentication procedure of smart devices and lightweight grid based homomorphic cryptosystem to encode a message. It is partitioned into the introduction stage and perusing total stage [16]. Since the scheme makes it conceivable to screen authentication between smart devices, control focus, smart meter, and communication between APs, the control focus can unscramble a scrambled message to improve classification and protection of devices. To verify smartphones and send messages securely in a smart home environment.

Authentication procedure requires the capacity of some public key, in the device. The key must be permanent – it must not be workable for an attacker to change the key, or cause the device to utilize another key. This key is alluded to as the ‘foundation of trust’ for the particular key progressive system. Some of the time it is expected to join the public key of a device/user, with other information to recognize the device. The procedure are

1. Sending API, a request to create a gateway
2. Adding a new user who has access to the gateway to the system
3. The user connects to the gateway locally followed by the user’s authentication
4. The gateway was properly authenticated—i.e., test with the password and the user id to get authenticate.

The first functionality, particularly important from the perspective of the entire system, is authentication and authorization of the user in the system. After registering, the user is asked to provide its login and password.

b. AUTHENTICATION USING RSA

RSA is an application of a public key crypto system to allow authentication and integrity detection of messages from the smart home user. It always related to both communicating parties showing proof that they have or know a particular secret. RSA can be used for more than just encrypting data [17]. Its properties also make it a useful system for confirming that a message has been sent by the user who has sent it, as well as proving that a message hasn’t been altered or tampered with. This consists of three steps

a) Key Generation:
   • Select p, q, … p and q both are the prime numbers, p ≠ q.
   • Calculate n = pq
   • Calculate φ(n) = (p-1) (q-1)
   • Select integer g(d ( (n), e)) = 1 & 1 < e < (n)
   • Calculate d; d= e\−1 modulo (n)
   • Public Key, PU = {e, n}
   • Private Key, PR = {d, n}

b) Encryption:
   • Plaintext: m < n < p
   • Ciphertext: C

c) Decryption:
   • Ciphertext: C
   • Plaintext: M = Cd mod n
   • Note 1: (n) -> Euler’s totient function
   • Note 2: Relationship between C and d is expressed as:
     \[ ed \mod (n) = 1 \]

   \[ d = e^{-1} \mod (n) \]

At the point when somebody needs to demonstrate the genuineness of their message, they can figure a hash of the plaintext, at that point sign it with their private key. They sign the hash by applying a similar recipe that is utilized in decoding.

\[ (m = cd \mod n) \]

When the message has been marked, they send this message to the user with the message. On the off chance that a beneficiary gets a message with a computerized mark, they can utilize the mark to check whether the message was genuinely marked by the private key of the individual who professes to have sent it. They can likewise observe whether the message has been changed by attackers after it was sent.

c. GROUP AUTHENTICATION USING BLOWFISH

The group leader must authenticate many devices and engage in secure communication only after key exchange. In a scheme without an authentication server, a group leader is generally identified; this leader monitors when devices join and leave the group [18]. Earlier group authentication schemes (GASs) were based on a “threshold secret sharing” technique. Group authentication not only manages group participants, but also performs hierarchical group-based authentication using a group key. The process are

1. The encrypted key of blowfish (C-Blow-K) must be decrypted using RSA algorithm with the help of private key RSA-Pri-Cloud. Blow-K = Dec RSA-Pri-Cloud (C-Blow-K)
2. CPL has to be input to HMAC to produce M1, if M1=M then the message is authenticated, otherwise it will be discarding and send request message to sender to resend the message. M1 = HMAC Blow-K (CPL)
3. If the value of M1 is equal to receive M, then go to step number 4. Otherwise the cloud must send message to sender to inform him to resend the message again.
4. Original message can be obtained by applying Blowfish algorithm with its decrypted secret key (Blow-K) on cipher text (CPL). PL = Dec-Blowfish (Blow-K, CPL).

The F-Function of BA is likely the most mind boggling some portion of the algorithm since it is the main part that uses the Sboxes. It acknowledges a 32-piece stream of data and parts the data into four equivalent parts. Every
8-piece subdivision is changed into a 32-piece data stream utilizing the comparing of every subdivision S-box. The 32-piece data that is gotten is XOR-ed or consolidated to give a last 32-piece an incentive for changes of the Blowfish.

**Key distribution algorithm**

Input: GA---Key distribution, NewMem--- New Member, GJoin--- Group member want to join

Step 1: Start

Step 2: IF (REQUEST==WANT JOINT

Step 3: IF(grouplist(Gjoin) && Pswd==Gjoin.Password)

Step 4: UPDATE Memberlist(IP[NewMem])

Step 5: UPDATEThreshold(n)

Step 6: keys[] = KeyGeneration. Threshold(128, n, threshold)

Step 7: FOR (k: GJoin.Groupmembers)

Step 8: ADD (Groupmember.GJoin.i)

Step 9: END

Therefore, a robust authentication method needs to be enforced in all those points. IOT technology is installed in multifaceted authentication to assemble a solid user authentication instrument. A session key might be gotten from a hash esteem, utilizing the CryptDeriveKey work (this technique is known as a session-key deduction scheme). All through every session, the key is transmitted alongside each message and is scrambled with the beneficiary's public key. Since a lot of their security depends upon the curtness of their utilization, session keys are changed much of the time. An alternate session key might be utilized for each message.

**V. EXPERIMENTAL RESULT**

A light weight and secure session key can be establishing for the smart home environment for authenticating the outside devices. This can be making secure against denial-of-service and eavesdropping attacks. Also here make group authentication of the devices in the smart home environment. For this group authentication threshold cryptography-based group authentication is used. The implementation was done using NS2 environment by using day to day accessing dataset.

By GA of the group, who creates the group, is responsible for generating a public key KPu (G) and multiple private keys KPr1 (G).....KPrn(G) are then distributed by the GA among all the members of the group.

During this test a new gateway was configured in the system. The following steps were undertaken:

1. Sending API, a request to create a gateway
2. Adding a new user who has access to the gateway to the system
3. The user connects to the gateway locally followed by the user’s authentication
4. The gateway was properly authenticated—i.e., the result of the test resulted positive.

The average time it takes a data bundle to arrive at the goal. This incorporates every single imaginable postponement brought about by buffering during course disclosure idleness, lining at the interface line. This measurement is determined by subtracting time at which first parcel was transmitted by source from time at which first data bundle landed to goal. Numerically, it very well may be characterized as: Avg. EED=S/N Where S is the entirety of the time spent to convey bundles for every goal, and N is the quantity of parcels gotten by the all goal hubs.

**Chart 1: Encryption and Decryption time comparison**

The use of encryption and secure communication requiring a high degree of computing power and provide more security. From chart 1 our method provides a high security system to the smart home environments. The comparison was shown in that chart.
Here RSA and Blowfish algorithm is used to obtain a satisfactory level of security. Security is an important factor in the IOT based smart home. By applying this we reach high level of security when compared to existing work that was shown in chart 3. The combination of Blowfish algorithm and RSA algorithm yields the high security to the IOT.

VI. CONCLUSION

A smart home comprises of low limit devices and remote systems, and along these lines, all cooperating as a protected framework that needs a satisfactory degree of security. Numerous works are actualized to unravel this security issue. Here for security reason session key with group authentication technique was proposed. This proposed scheme gives significant security qualities including avoidance of different mainstream attacks, for example, disavowal of-service and listening stealthily attack. A smart home can fill in as a group that speaks with a service supplier (which updates that group), or with a neighboring group, or a single user-device group, in an IOT environments. Cryptography method is used to solve this issue by applying the RSA and Blowfish algorithm it provides more security to the data for the smart home devices. It allows each entity should be performed a lightweight mutual authentication prior participation in the home network and establish a session key in a secure manner. This scheme uses the symmetric key cryptography and a hash function to compliment other techniques in order to provide more security in the smart homes.

REFERENCES

International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST) (pp. 451-454), IEEE.


[6]. Vishakha D. Vaidya ; et al, “A Comparative Analysis on Smart Home System to Control, Monitor and Secure Home, based on technologies like GSM, IOT, Bluetooth and PIC Microcontroller with ZigBee Modulation”, IEEE Xplore, November 2018


[12]. Arummozhi Manimuthu ; Ramadoss Ramesh et al, “Privacy and data security for grid-connected home area network using Internet of Things”, IEEE, November 2018.

[13]. Shreya Dey et al, “Session-Key Establishment and Authentication in a Smart Home Network using "Public Key Cryptography", IEEE, 2019


[18]. G. Sathish Kumar, K. Premalatha, “Secured Cryptosystem using Blowfish and RSA Algorithm for The Data in Public Cloud”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7 Issue-4S, November 2018