I. J. Computer Network and Information Security, **2019, 6, 29-37**
Published Online June 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.06.04

A Privacy-Aware Dynamic Authentication Scheme for IoT Enabled Business Services

Nitin Singh Chauhan
Jawahar Lal Nehru Technological University Kakinada, 533003, India
E-mail: raju.nitin@gmail.com

Ashutosh Saxena
C.R.Rao Advanced Institute of Mathematics, Statistics and Computer Science (AIMSCS), Hyderabad, 500046, India
E-mail: asaxena@crraoaimscs.res.in

JVR Murthy
Jawahar Lal Nehru Technological University Kakinada, 533003, India
E-mail: mjonnalagedda@gmail.com

Received: 23 March 2019; Accepted: 24 April 2019; Published: 08 June 2019

***Abstract*—**Tech-savvy users are striving to bring automation and digitization in their lifestyle to make life more comfortable and efficient; Internet of Things (IoT) is an enabler in this direction. Technology advancements and new business opportunities are rapidly changing the IoT adoption landscape, and thereby security and privacy concerns have also started raising and realizing. The increasing number of IP enabled electronic devices, enormous data generation, and communication traffic have enhanced the attack surface for security and privacy violators. Many security attack scenarios are the result of poor identification and authentication mechanisms of communicating entities. In this paper, we present a secure scheme to perform a business transaction initiated by a smart device in the IoT environment. Scheme performs dynamic authentication of a business transaction while ensuring the privacy of the associated user(s). This scheme relies on Message Authentication Code (MAC) and dynamic key generation method to achieve a secure workflow. In this paper, we present a pluggable Roaming Smart Meters (RSM) concept to demonstrate the applicability of the proposed authentication scheme.

***Index Terms*—**IoT, Security, Authentication, Privacy, Smart Meter.

I. Introduction

Evolution of IPV6 has realized the opportunity of having billions of Internet Protocols (IPs). A user can have multiple IP enabled devices connected to the Internet. By 2020, installed base of the Internet of Things (IoT) devices is expected to grow to 31 billion [1]. Devices communicating with each other are forming the paradigm of Internet of Things (IoT). Electronic appliances have become smart as they are not only connected to the Internet, but also make decisions in real-time on behalf of their users. IoT brings value-add to the existing business services and evolves multiple new businesses.

While the IoT offers plenty of business opportunities, establishing trust, privacy and security present a great challenge [2,3,4]. Incidents in the past indicated that security and privacy of data are at stake in such environment. Our daily lives are now being tracked by connected devices, and attacks on car control system indicates that even lives are at stake [5]. Concerns are also increasing about data control practices and unintended use of individual's private data for the business benefits of enterprises [6]. Due to rapid advancements in the IoT as well as its increased business value, there is a need to address security and privacy concerns.

One of the key security issues in IoT environment is authentication of smart devices. This issue is even more relevant when IoT based system triggers business transaction automatically, as per pre-defined conditions/rules and the data received from these requesting devices. There is a possibility that malicious device or process triggers a transaction on behalf of the victim device. Such operations may cause user inconvenience, reputation damage of business services and financial losses to entities involved in the transactions [7]. This necessitates a simple, effective, secure and privacy-aware authentication scheme, which can authenticate business transactions initiated by identified IoT device and at the same time protect the authentication process from various attacks.

In this paper, we propose a new scheme to perform a business transaction in an IoT based system with the secure authentication process. This scheme relies on the one-time registration process for IoT devices and uses a novel approach by using Message Authentication Code (MAC) based dynamic authentication to avoid any opportunity for replay attacks. Proposed scheme also

protects the privacy of business transactions initiated by IoT devices. This scheme guarantees that only participated IoT device and business service providers are aware about the details of business orders initiated by a user's IoT device. In this paper, we also describe a pluggable roaming smart meter (RSM) use case which leverages proposed authentication scheme.

Organization of this paper is as follows: Section-2 covers related work. Section 3 discusses the proposed scheme for authentication in IoT scenario and describe the various phases involved. Section 4 presents Roaming Smart Meter use case, section 5 covers experimental setup and results. Section 6 presents security and privacy analysis of the proposed approach. We conclude the paper with section 7.

II. Related Work

Static password-based authentication schemes are the most widely used methods for remote authentication [8]. However, such schemes are susceptible to various attacks [9]. These schemes are not viable in the IoT environment as IoT devices work with minimum human interaction and any password compromise may lead to serious attacks. Dynamic authentication is relatively considered secure and many schemes are proposed by researchers. Several such schemes use the smart card capability to achieve the dynamic behavior [10,11]. However, most of these schemes are heavily dependent on the hardware and heavy cryptographic computations [12,13]. Their verbatim applicability in the IoT environment is not effective due to their inherent limitations. Further, there are authentication schemes based on symmetric key [14] but they suffer typical complexity issues of key management and key distribution. Many frameworks are based on PKI certificate infrastructure [14,15]. Such set-up requires effective and real-time management of certificates and certificate revocation lists (CRL's), which increases the complexity of operations. Elliptic Curve Cryptography (ECC) based protocol is used to address authentication challenge, but it does not address denial of service issue [20]. In a typical business scenario, business service providers need to be one of the participating entities to perform cryptographic operations. In our proposed scheme, it does not require any cryptographic activity to be executed at the business service provider's end. We use Message Authentication Code (MAC), which is a lightweight algorithm as compared to any other cryptographic operation.

Some authentication schemes are based on signal properties [17]. However, mobility of IoT device is a constraint in such approaches. Our approach does not have such constraint. EAP (extensible authentication protocol) is a framework for Wi-Fi devices, but in a typical IoT based business scenario, it is susceptible to replay attacks [18]. Usage of one-time keys in our approach makes authentication resistant to replay attacks. Liu et al. [19] analyzes existing authentication and access control methods and presented a feasible design for IoT. Zhao et al. [20] presented a scheme which can be applied in IoT, based on the mutual authentication scheme between the platform and the terminal node.

Alcaide et al. [21] proposed a privacy-preserving decentralized anonymous authentication protocol in which the ad-hoc community of decentralized founding nodes participates. Their protocol does not rely on any central entity and performs key distribution in a (t, n) - threshold fashion. Their scheme is applicable for authentication between the user and participating IoT nodes. The scheme proposed in our paper is focused on business transaction authentication generated by identified IoT devices.

N. Mahalle et al. [22] proposed Identity Authentication and Capability Based Access Control (IACAC) mechanism which uses a secret key generation based on Elliptical Curve Cryptography-Diffie Hellman (ECCDH) algorithm. This mainly focuses on authentication of one device to another device. However, in our approach authentication is performed by a trusted third-party without compromising the privacy of business transaction. Our approach is scalable because the cloud environment is used for hosting a dedicated, trusted third- party which provides authentication services to multiple devices and business service providers.

The motivation of our work comes from the fact that the simple, effective, secure and privacy-preserving authentication scheme is required, which can authenticate business transactions initiated by identified IoT device and at the same time protects the authentication process itself from various attacks.

III. Proposed Scheme

In this section, we present a scheme for a typical business scenario where IoT device intelligently initiates a business order based on the pre-defined logic conditions. Our proposed scheme relies on a trusted third-party which has registration and authentication services. Trusted third-party registers IoT devices initially using registration service. After registration, device can perform business transactions with the service provider. On each transaction, authentication service authenticates IoT device and order using dynamic MAC. Dynamic value of MAC is not only based on the business transaction, but also owing to one-time key used in the process of generating MAC.

A. Entities and Notations

Fig.1 shows the entities involved in our approach and interaction among them

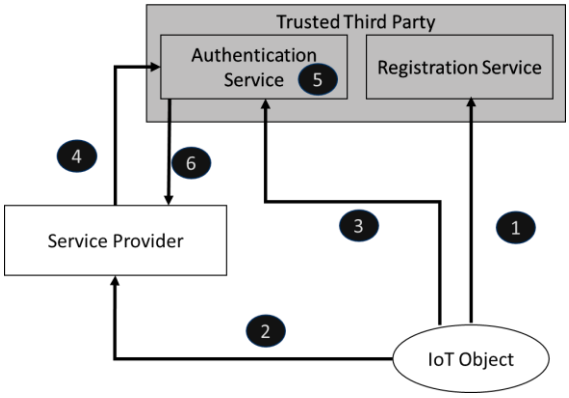

Fig.1. Involved entities and their interaction

IoT Device: It is an IP enabled device capable to sense, communicate and compute. Currently, multiple devices are available which can gather data, process them and communicate to other IP enabled device/computers. For instance, smart home appliances having sensors to monitor and capture the related home environmental data, and intelligently trigger the necessary action based on the predefined logic. IoT device could be smart refrigerators or any other container which has sensors to detect the level of availability (such as grocery, eatables, and milk) in the containers. Based on the availability and consumption pattern, the container intelligently places the order to identified grocery suppliers.

Business Service Provider (CSP): This is an entity which receives the request for the business service and performs the necessary action based on business request. Grocery supplier is a BSP in this business case. Supplier receives the request for business service and perform the necessary action (e.g. delivering the grocery to the user) based on the request.

Registration Service Module: Our approach uses the concept of a trusted third-party which has registration service module to perform registration of each device. Registration is a one-time activity for a defined period.

Authentication Service Module: Authentication Service is another module of a trusted third-party. This module performs the authentication for every business service request received by BSP from IoT device.

Registration Service and Authentication Service modules can be hosted by a single trusted authentication service or can be part of separate services. For scalability purpose, we propose a cloud environment for hosting such services.

Notations used in this paper are mentioned in Table 1.

Table 1. Notations used in the paper

Notation	Description
U	the user
O_n	is n^{th} IoT device/appliance
Bo_i	i^{th} business order placed by O_n
RS	Registration Service Module
AS	Authentication Service Module
BSP	Business Service Provider
bsp_i	j^{th} business service provider's identity
ak_n	Registration acknowledgement for n^{th} device.
oh_i	Hash of the i^{th} business order
$h(M)$	Function to perform hash on message M
c_i	Counter value of i^{th} business order
s_n	Seed value for object O_n
I_n	Identity information of O_n
k_i	Key value for i^{th} business order
$g(oh_i, c_i, k_i)$	g is a function to generate the MAC using the message oh_i, counter c_i and key k_i
m_i	a Message Authentication Code i^{th} business order
$f(s_n, c_i, I_n)$	f is a function to generate key k_i using input parameters s_n, c_i, I_n
ar_i	Authentication response of i^{th} business order.
$A \rightarrow B :< a,b,c >$	A sends message to B containing information a, b and c over open channel
$A \Rightarrow B :< a,b,c >$	A sends message to B containing information a, b and c over secure channel

B. Activity Flow

Without losing generality, Fig.1 can be upscaled to *n* IoT devices and *j* number of BSP's. We now explain the flow of activity in brief for a typical business transaction in the proposed scheme.

1. User registers the IoT object/smart device to the registration service of trusted third-party. This is a one-time process and performed over the secure channel.
2. Whenever there is a need for an object to initiate the message transaction with the SP, it performs necessary cryptographic operation to generate the MAC of transaction message. It sends the message and identity information to the service provider.
3. Object sends the hash value of the message and identity information to the Authentication server as well.
4. SP requests the authentication server for authentication of that object.
5. AS retrieves information received from IoT Object, SP and RS, performs operations to calculate MAC and validate the authenticity of transaction message and object.
6. AS sends the authentication validation result to SP.

C. Transaction Process

This process has five phases. The registration phase is performed only once for a particular device. Other phases are executed every time the IoT device places a request for a business transaction.

1) Registration Phase

It is assumed that every IoT device/Sensor O_n has a unique identity I_n. To register, the device first generates a random seed s_n , initial counter c_0 and communicate the s_n, c_o and I_n to the registration service. As this is a one-time activity we prefer to perform communication over secure channel to protect the seed value, which is used later to generate the one-time keys.

This phase is invoked whenever a user U registers the IoT device O_n to the registration service *RS*.

Step 1. O_n Generates a random seed s_n and initial counter c_0. For first counter c_i=c_0;

Step 2. $O_n \Rightarrow RS :< I_n, s_n, c_i >$ Registrations service securely store the I_n, s_n, c_i

Step 3. RS sends an acknowledgement of registration to O_n

$$RS \Rightarrow O_n :< ak_n >$$

2) Transaction Initiation Phase

In this phase the IoT device generates a business order Bo_i and sends it to the configured BSP .

$$k_i : for \forall i, \ э$$

Step 1. O_n generates a key $k_i : for \forall i, \ э$ 12

$$k_i = f\left(s_n, c_i, I_n\right) \quad (1)$$

Step 2. O_n calculates the hash of the message

$$oh_i = h\left(Bo_i\right) \quad (2)$$

Step 3. MAC is calculated by O_n using one-time key k_i

$$m_i = g\left(oh_i, c_i, k_i\right) \quad (3)$$

Step 4. O_n send the business order to BSP along with m_i and I_n

$$O_n \rightarrow BSP :< m_i, I_n, Bo_i >$$

Counter value can be set to a fixed number and can be increased on every event of key generation and order placement. This process always generates a new key because every key generation event uses a new incremented count value.

3) Authentication Phase

Step 1. Device sends the authentication request to AS

$$O_n \rightarrow AS :< m_i, I_n, c_i, oh_i, bsp_j >$$

One can omit c_i in the above tuple if O_n is conducting the business with only one BSP.

Step 2. AS already possess the s_n generated during the initial registration and current c_i. AS calculates the one-time key again by using the s_n, c_i, I_n received from device.

$$k_a = f\left(s_n, c_i, I_n\right) \quad (4)$$

Step 3. AS also re-generates the MAC

$$m_a = g\left(oh_i, c_i, k_a\right) \quad (5)$$

Step 4. P sends the m_i, I_n, bsp_j to AS

$$BSP \rightarrow AS :< m_i, I_n, bsp_j >$$

Step 5. If $m_i = m_a$, it proves that m_i is an authentic business order from device registered with RS. As keys used for producing the MAC are independently generated at device and AS sides.

Step 6. With successful validation, AS marks the received m_i as valid and communicate the success message $ar_i = "TRUE"$ to *BSP* along with I_n, m_i. In case if $m_i \neq m_a$, AS returns the $ar_i = "FLASE"$ as unsuccessful authentication.

$$AS \rightarrow BSP :< I_n, m_i, ar_i >$$

Here we use secure channel to communicate the authentication response to BSP as using the open channel may lead to the man-in-the-middle attack. However, in case of open channel, we suggest that the AS should put verifiable timestamp/signature in the authentication response.

4) Service Delivery Phase

Once BSP validates the authenticity of MAC through AS, it executes the business transaction and deliver the requested service to the user of the requesting device.

5) Renew or revoke phase

Renew phase deals with the registration renewal. This phase is applicable, if the device registration with the RS module is for a time period or based on the defined usage limit. After a pre-defined time period or the number of authentication events, new seed value is used. Changing the secret value of seed at regular interval is a good practice from a security point of view. Further, such policy provides flexibility for authentication service to control usage of its service. For example, if authentication service sets the policy of providing its service to the device for 100 times, an initial counter can be set to 200 and with every successful authentication request, the counter can be decremented by 2. Authentication service stops its service to request iff $c_i = 0$. Counter gets reset to a new number as per pre-defined policy after renewal.

Device revocation takes place when device is deactivated or destroyed for any reason. In such cases, the AS service removes the entry for the device from its database and flag the device as "*invalid*". AS checks for "*invalid*" flagged ID list before authenticating any request. Once this check is successful only then it further authenticates the business transaction.

IV. Use Case-Roaming Smart Meter

Smart meters are usually fixed to home/industry premises. We propose a roaming smart meter (RSM) system that is based on the proposed authentication scheme. In such system, a roaming user consumes the energy at any power outlet and system ensures that proper billing settlements take place at the end of the power consumption between the user (energy consumer) and energy provider (power outlet from which energy is being consumed). Nicanfar et. al [23] presented privacy preserving authentication scheme for communication between electric vehicle as energy storage and power station. However, the concept of secure roaming smart meter and associated charging infrastructure network system for roaming Internet enabled devices is not available in the present literature or practice. Fig. 2 shows key components of proposed the RSM system. System includes RSM device and other associated service module hosted in RSM service provider environment. It is assumed that components presented in the left side of the dashed line are already available as part of the power supply infrastructure.

Registration Module: Registration module registers the user device to the RSM. By registering, the user can control the number and type of devices to be used for roaming smart meter services.

Authentication Service Module: Authentication Module performs authentication of roaming IoT devices which need to authenticate at the time of electricity charging/consumption. For authentication purpose, we propose an authentication server hosted as part of RSM service in RSM service provider environment. Authentication server uses the protocol mentioned in our scheme to authenticate the IoT devices.

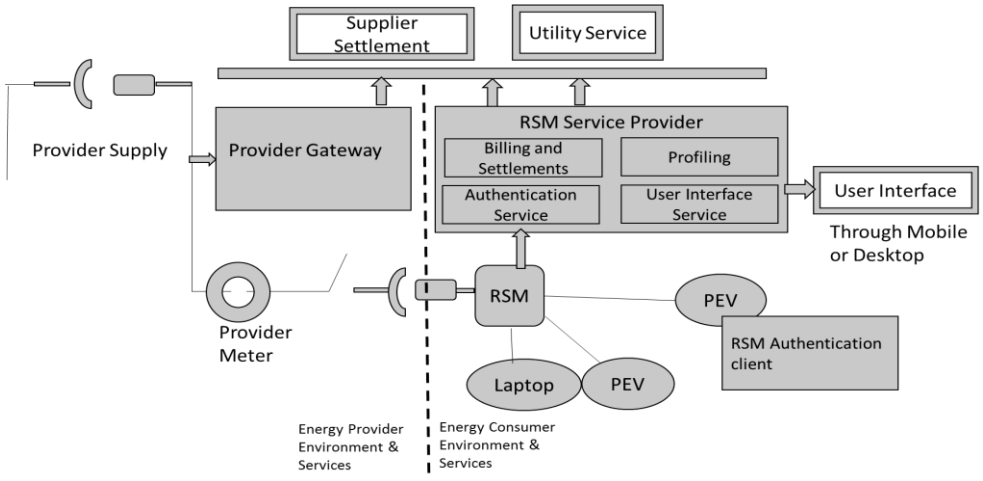

Fig.2. Key components of RSM system

It maintains device ID and an associated authentication seed value. This value is used to generate the MAC. Seed value/Counter will be incremented after each authentication request from the device.

RSM Authentication Client: RSM authentication client is installed at roaming IoT device at the time of the device registration. The unique and random seed value is stored in the device. Seed value can be protected with any PIN/password mechanism used in the roaming device. The client application uses the seed to generate key and MAC for authentication during every charging request. Authentication module of RSM Service provider generates similar key and MAC as proposed in our scheme.

There are additional module components from the proposed scheme in Fig. 2 to complete the business flow of Roaming Smart Meter.

Profiling Module: This module allows the user to configure the devices, priorities, and quota of electricity consumption at the remote power outlet. Once RSM records the threshold consumption limit, it initiates the power disconnect signal for electricity consuming device.

User Interface: User interfacing application provides access to mobile or desktop and manages registration of identified devices, establish secure key management, monitor the electricity consumption and generate reports which are useful for the user to control and manage the electricity consumption by individual devices.

Billing and Settlement: RSM records energy consumption by consumer device at provider power outlet and reports it to the settlement service. Settlement service communicates the information to the provider's energy supplier who can claim the charges from consumer's energy supplier. User intern receives the bill for consumed energy from his (consumer's) supplier. Fig. 3 represents the sequence of activities performed during a typical electricity consumption event.

V. Experimental Setup and Results

To demonstrate the proposed authentication scheme as a proof of concept, a working prototype was built as a limited experimental set up using Arduino Uno microcontroller. The scope of the experiment was confined to validate the dynamic key generation on a microcontroller and performing authentication using MAC. Below is a brief description of the hardware used in this setup.

Arduino Uno: Arduino is an open-source microcontroller build around ATmega 328P. Arduino can interface with ESP8266 WiFi module and provides the option to perform required cryptographic operations. We developed the code to generate the dynamic key for MAC calculation and executed it on Arduino uno. We selected the Arduino uno as it provides host of features apart from the supporting hash function SHA256 in HMAC mode for generating the message authentication code, which is a crucial requirement in our protocol.

ESP8266 Wifi Module: ESP8266 is a WiFi chip. ESP 8266 provided interface for Arduino board and Android application.

Android Mobile: We used Android mobile to host the authentication module and registration module applications for IoT Devices.

Results of Experimental Setup: On invoking the MAC generation application on Ardunio, device sent the authentication request to the authentication module hosted on android mobile device. The android device application also calculated the dynamic one-time key and generated MAC. While conducting the experiment we observe that both MAC values were the same, and therefore we could able to prove the successful working of the proposed authentication scheme. Also, we noticed that for each authentication cycle, MAC values were different. This clearly establishes dynamic behaviour of our authentication scheme.

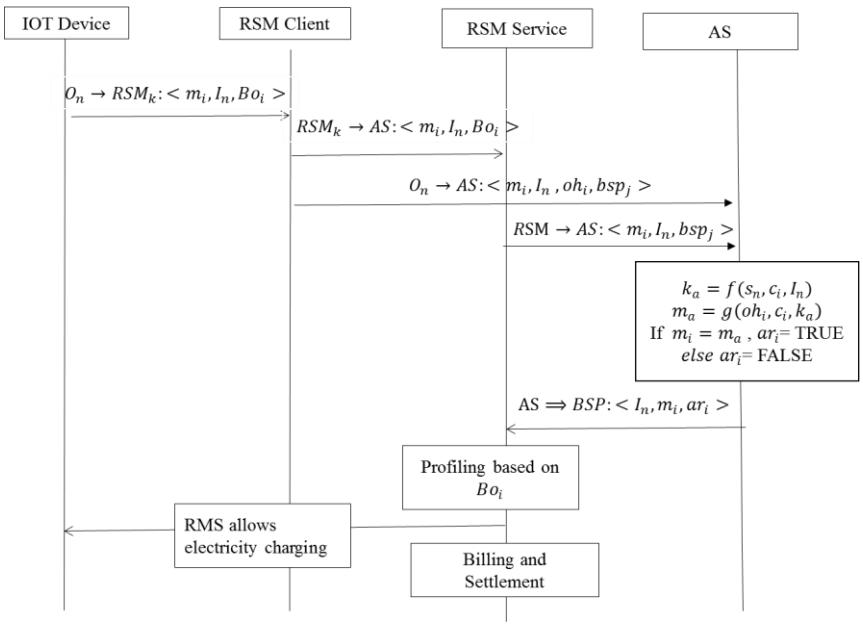

Fig.3. Authentication and profiling activity sequence for IoT devices through RMS

VI. Security and Privacy Analysis

In this section, we analyze the security and privacy of our scheme. We evaluate the scheme by reviewing the adversary models to attack the system.

A. Adversary Models

In the model, the adversary is capable of recording and replaying the messages. For the sake of simplicity, we consider two adversary models based on the adversary situations, both from the security and privacy point of view. In the first one, we assume the adversary is a party out of the introduced parties (e.g. Untrusted IoT Object) and in the second model, we assume that adversary is the service provider or authentication service.

Scenario 1: Replay Attack

Objective: The adversary wants to gain access to replay the business order using the intercepted communication channel.

Capabilities: The adversary knows the ID of the victim IoT Device O_n, and can intercept the communication channel between IoT Object and RSM SP. Also, the adversary knows in detail the design of our mechanism. If the adversary creates a malicious business order, he will be able to place the unauthorized business orders on behalf of the victim.

Analysis: A replay attack, replaying the business order using the intercepted authentication key cannot work because a new key is being used during every business transaction in the authentication phase. To create a new key adversary, need to have initial seed and counter. It is assumed that AS module of trusted third-party has secure process of storing key generation parameters (s_n, c_i, I_n).

$$k_{i'} = f\left(s_n, c_{i'}, I_n\right) \tag{6}$$

n such case, if adversary wants to repeat the same order as Bo_i

$$O_n' \; such\; that \;\; I_n = I_n', Bo_i = Bo_i$$

However, adversary does not have the capability to generate the appropriate $k_{i'}$ *and* m_i in the absence of s_n *and* $c_{i'}$.

Therefore, adversary will end up sending the message where $m_{i'} = m_i$

$$O_n' \rightarrow BSP :< m_{i'}, I_n', Bo_{i'} >$$

At the server end, during authentication, a new $m_{a'}$ is generated as

$$m_{a'} = g\left(oh_{i'}, c_{i'}, k_a\right) \tag{7}$$

in case $m_i != m_{a'}$, then ar_i is FALSE indicating that the authentication is failed.

Even if adversary changes the Bo_i authentication gets failed as m_a is also dependent on Bo_i, Another opportunity for the adversary is to get access to the seed and counter during communication between device and RA. However, we consider a secure channel, or one can use the public key of trusted authentication service to encrypt the communication for initial registration so that only the authentication service can get access to parameters. Predefined function at device and AS generate synchronized counter value dynamically after every transaction. Thus, the adversary cannot forge the identity of the device and generate a business transaction on behalf of genuine device.

Our approach uses key based hash functions for authentication purpose. The security of such mechanisms depends on the strength of hash functions used in the process. We claim that our scheme is secure enough and subject to the strength of the hash function used. Formal proof and security evaluation of such functions is available in existing literature [24, 25].

Scenario 2: Privacy Attack

Objective: The adversary is AS and wants to gain access to business order transactions performed by the IoT device of a user.

Capability: If AS gets the details about Bo_i, then there is a privacy compromise.

Analysis: Scheme protects the user's privacy, as even trusted authentication service also does not get details of business transactions performed by IoT device of the user. The device creates the hash of order oh_i and performs MAC on a new message that includes oh_i and c_i. At the AS side during MAC authentication only hash value of business order is received instead of the complete message.

Further, our scheme does not reveal any information related to keys to any business service provider. Therefore, any dishonest BSP cannot reproduce fake business transactions. AS authenticates entries of all business transactions and therefore correctness of transactions is verifiable at any point to time. The scheme provides an optional feature of using one PKI certificate for AS to prove its authenticity. This is minimum PKI related overhead as only during registration activity the public key of AS is used to receive the encrypted registration request. This mechanism protects authentication and registration activities from the possibility of impersonated AS and secure channel protects the data from the man-in-the-middle attack.

Thus, the proposed scheme can resist replay attacks, forgery attacks, and stolen verifier attacks. The scheme also protects any privacy violation of the user's business transactions.

VII. Conclusion

The IoT is increasing the connectivity of people and devices at an unimaginable scale. The proliferation of IoT promises a smoother life, such as the ability for consumers to keep track of their groceries, health, and energy data etc., on their smart gadgets. However, the constant connectivity and data sharing in the IoT environment also create new opportunities for security attacks that have not been seen in the past. In this paper, we presented a secure scheme to authenticate IoT devices. The scheme also protects the privacy of the user by not disclosing the business transaction to unintended entities. Our approach considers a secure channel between device and registration service for one-time registration activity. PKI can also be considered as one option for a secure channel. Our future work focuses on achieving the minimum computation overhead for secure channel and explores the possibility of completely removing the need for secure channel by providing offline device personalization mechanism. Though we have considered a scenario of placing business orders, our scheme is generic and applicable to various business scenarios and industries where privacy protected authentication is the need.

Disclaimer

The views expressed here are the authors' personal opinions; they might not represent the view of associated organization.

References

[1] L. Columbus, "2017 Roundup Of Internet Of Things Forecasts," *Forbes*, 11-Dec-2017. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/. [Accessed: 22-Mar-2019].

[2] A. Radovici, C. Rusu, and R. Serban, "A Survey of IoT Security Threats and Solutions," *2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, 2018.

[3] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2018.

[4] M. T. Banday, "Security in Context of the Internet of Things," *Cryptographic Security Solutions for the Internet of Things Advances in Information Security, Privacy, and Ethics*, pp. 1–40, 2019.

[5] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway-With Me in It," *Wired*, 20-Nov-2018. [Online]. Available: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Accessed: 22-Mar-2019].

[6] P. Leskin, "The 21 biggest data breaches of 2018," *Business Insider*, 11-Dec-2018. [Online]. Available: https://www.businessinsider.in/The-21-biggest-data-breaches-of-2018/articleshow/67045497.cms. [Accessed: 22-Mar-2019].

[7] R. Nukala, A. Shields, U. McCarthy, S. Ward, "An IoT based approach towards Global Food Safety and Security", *IT&T*, pp. 10, 2015.

[8] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol.24, no.11, pp.770-772, 1981.

[9] Tsai, Chwei-Shyong, Cheng-Chi Lee, and Min-Shiang Hwang, "Password Authentication Schemes: Current Status and Key Issues," *IJ Network Security*, vol.3, no. 2 (2006): 101-115.

[10] M.L. Das, A. Saxena, and V.P. Gulati, "A Dynamic ID-based Remote User Authentication Scheme", *IEEE Transactions on Consumer Electronics*, vol. 50, No. 2, 2004.

[11] K. Awasthi, and S. Lal, "A remote user authentication scheme using smart cards with Forward Secrecy," *IEEE Transactions on Consumer Electronics*, vol.49, no.4, pp.1246-1248, Nov. 2003.

[12] M. S. Hwang, C. C. Chang, and K. F. Hwang, "An E1Gamal-like cryptosystem for enciphering large messages," *IEEE Trans. on Knowledge and Data Engineering*, vol.14, no.2, pp.445-446, 2002.

[13] C. C. Lee, L. H. Li, and M. S. Hwang, "A remote user authentication scheme using hash functions," *ACM Operating Systems Review*, vol.36, no.4, pp.23-29, 2002.

[14] H. Wang, B. Sheng, C. C. Tan, and Q. Li, "Comparing Symmetric-key and Public-key Based Security Schemes in Sensor Networks: A Case Study of User Access Control," *2008 The 28th International Conference on Distributed Computing Systems*, 2008.

[15] C. Adams, M. Just, *PKI: Ten Years Later. PKI R&D Workshop*, 2004.

[16] M. Braun, E. Hess, B. Meyer, "Using Elliptic Curves on RFID Tags", *IJCSNS International Journal of Computer Science and Network Security*, vol. 8, no. 2, Feb 2008.

[17] T. Suen and A. Yasinsac, "Ad hoc network security: peer identification and authentication using signal properties," *Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005.*

[18] A. M. El-Nagar, A. A. A. El-Hafez, and A. Elhnawy, "A novel EAP-moderate weight Extensible Authentication Protocol," *2011 seventh International Computer Engineering Conference (ICENCO2011)*, 2011.

[19] J. Liu, Y. Xiao, and C. P. Chen, "Authentication and Access Control in the Internet of Things," *2012 32nd International Conference on Distributed Computing Systems Workshops*, 2012.

[20] G. Zhao, X. Si, J. Wang, X. Long, and T. Hu, "A novel mutual authentication scheme for Internet of Things," *Proceedings of 2011 International Conference on Modelling, Identification and Control*, 2011.

[21] A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, "Anonymous authentication for privacy-preserving IoT target-driven applications," *Computers & Security*, vol. 37, pp. 111–123, 2013.

[22] P. N. Mahalle, B. Anggorojati, N. R. Prasad, R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things", *Journal of Cyber Security and Mobility*, vol. 1, no. 4, pp. 309-348, 2013.

[23] H. Nicanfar, S. Hosseininezhad, P. Talebifard, and V. C. M. Leung, "Robust privacy-preserving authentication scheme for communication between Electric Vehicle as Power Energy Storage and power stations," *2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2013. pp. 55-60.

[24] I. B. Damgård, "A Design Principle for Hash Functions," *Advances in Cryptology — CRYPTO' 89 Proceedings Lecture Notes in Computer Science*, pp. 416–427.

[25] B. Preneel, “Analysis and design of cryptographic hash functions,” thesis.

Authors’ Profiles

Nitin Singh Chauhan obtained Master’s degree in computer application from Jai Narain Vyas University, Jodhpur, India in 2000. He started his professional career as Project Executive with Institute for Development and Research in Banking Technology IDRBT (Established by Reserve Bank of India) Hyderabad India (2001-2005). He worked for AppLabs (2005-2006) as a Security Lead and at Genpact (2006-2008) as an Assistant Manager- Information Security. He was Senior Technology Architect at Infosys Limited (2008-2016). He is a Research Scholar at Jawahar Lal Nehru University, Kakinada. His research interest includes cloud security, strong authentication, information security, and sustainable IT. He has 4 granted patents and around 10 published research papers to his credit. Nitin holds multiple security certifications including Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA).

Ashutosh Saxena M.Sc. (1990), M.Tech. (1992) and Ph.D. in Computer Science (1999). An industry expert and academician with over two decades of experience, 90+international publications, 26 granted patents, and a book on PKI: Concept, Design and Deployment (Tata McGraw Hill 2004) to his credit. Research interest: information security and privacy. Began career as a lecturer and computer engineer in the university and IUC-DAE facilities at Indore. Associate Professor at IDRBT (established by RBI), from 1998-2006. Worked at Infosys Ltd. (2006-16) as Principal Research Scientist & AVP. Member of the review board for many international journals, conferences and committees. Served as Adjunct Faculty at NIT Warangal & Professor and Dean R&D at CMR Technical Campus. Currently Professor (CS) at CRRAO-AIMSCS, UoH Campus, Hyderabad.

Dr. J.V.R.Murthy is Professor in the Department of Computer Science and Engineering, JawaharLal Nehru Technology University College of Engineering, Kakinada, India. He also holds position of Director, In-charge of Incubation Center JNTU Kakinada. He has 26 years of Teaching, Research and Industrial experience in the field of Computer Science with specialization in data warehousing and mining. He has multiple publications in national and international journals.

How to cite this paper: Nitin Singh Chauhan, Ashutosh Saxena, JVR Murthy, "A Privacy-Aware Dynamic Authentication Scheme for IoT Enabled Business Services", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.6, pp.29-37, 2019.DOI: 10.5815/ijcnis.2019.06.04

