Ilkogretim Online - Elementary Education Online, Year; Vol 20 (Issue 4): pp. 2401-2406
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.04.275

DESIGN A NOVEL APPROACH FOR TOKEN BASED AUTHENTICATION IN IOT NETWORKS

B. Bamleshwar Rao, Research Scholar ,AKSU, Satna(M.P.)
Dr. Akhilesh A. Waoo, Associate Professor,AKSU, Satna(M.P.)

Abstract : Raising incidents of security threats among active sessions is an increasing concern in IoT environment. Continuous authentication was introducing to be superior to traditional authentication schemes by constantly verify users' identities on an ongoing basis and spot the moment at which an illicit attacker seizes control of the session. However, several challenges remain unsolved. . In this paper, we propose a decentralized token-based authentication based on fog computing and blockchain. The protocol provides a secure authentication protocol using access token, ECC cryptography, and also blockchain as decentralized identity storage. The blockchain uses cryptographic identifiers, records immutability, and provenance, which allows the implementation of a decentralized authentication protocol.

Keywords : blockchain, IoT environment, Token ,Authentication

I. INTRODUCTION

Internet of Things (IoT) environment merges the digital and physical universes and enabling them to communicate real-time data, this makes security and privacy concern critical aspects that cannot be neglected. To illustrate, smartphone store a significant amount of personal data and it could be pair with a smartwatch to exchange data between them, these sensitive data should be accessed only by legitimate users, a vulnerability in one of them can directly affect the connected device. Consequently, the IoT device needs a unique identity that can reliably identify the legitimate user, thus authenticating the legitimacy of the access request. Besides, it would prevent malicious usage if the IoT device is robbed. It is crucial to constantly ensure that, the user is not impersonated which brings a particular type of authentication known as continuous authentication. The traditional authentication scheme authenticates the legitimacy of an entity statistically at the beginning of the communication session and decides either it is authenticated or not. Therefore, they are vulnerable to security threats such as hijacking attacks, which take control of the active sessions. Accordingly, there is an urgent need to tackle this weakness by continuously authenticate the identity of the connected nodes during the whole session. It must be considered that the continuous authentication scheme proposed to complement and reinforce static scheme not to replace it, and it has two types of communication models namely: device-to-device model and user-to-device model. In the IoT ecosystem, the user-to-device communication model identified several opportunities and challenges regarding the authentication process as opposed to the device-to-device model. Several schemes aim to authenticate users continuously in real-time with the help of IoT devices to prevent impersonation attacks or illegal access to the IoT environment from both anonymous and known users.

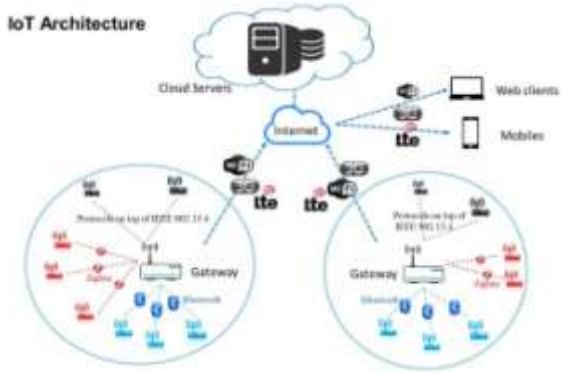

Figure 1: The generic architecture of the Internet of Things. Chuang et al[13]

The proposed IoT-based user-to-device continuous authentication solutions are largely focused on the performance of the authentication decision. More specifically, the reviewed literatures evaluate the performance either on a fixed number of user actions, or over a chunk of test dataset, and others evaluate the results in terms of Equal Error Rate (EER), False Acceptance Rate (FAR), and False Rejection Rate (FRR) over the test data set which consequently allows an imposter to carry out a variety of unauthorized actions before the system recognize his/her identity for the first time, this considered as a parodic authentication rather than CA procedure. Accordingly, there is a lack of detecting unauthorized access as short a few times as possible continuously in real-time.

II. RELATED WORK

Improving IoT identity and authentication has been an active research field for years, many identity/ authentication already proposed, there are some of these different studies.
A. Corici, et al[1]This article introduces a solution for enabling dynamic security domains in which devices join in a trustful way via an authentication framework. In the present paper we document the addressed use cases and requirements, the background technology evolution from 4G to 5G core network, together with the proposed solution and its results using a laboratory testbed.

T. Claeys, et al[2] propose an alternate key establishment scheme for use cases where devices cannot directly communicate. We test our proposal by implementing the critical aspects on a STM32L4 microcontroller. The results indicate that our framework guarantees a strong level of security for IoT devices with basic asymmetric cryptography capabilities.

S. Kinikar et al[3] Fire alarm system is built by integrating IoT technology with temperature detecting sensors. In order to use Gmail and twitter our device need to authenticate on behalf of the user. For this we use OAuth protocol for delegated access to applications like Gmail and twitter. Conventional end-to-end encryption based techniques are not accurate to ensure better quality of security because of exceeding slow response time of the smart devices, and has extremely low processing clock speed.

L. Zhou, et a;[4] we investigate the feasibility of extracting long-term memory ability from users' brainwaves. Third, we conduct the bio-features identified in the brainwaves of users as authentication tokens in the proposed authentication system which transparently performs continuous (or real-time) entity verification in the background without the need for direct input from the user. Experiment results demonstrate the efficacy of the proposed authentication system in achieving high verification accuracy.

H. Luo, et al[5] implement a prototype to further evaluate the performance of G2F. Based on our realization on the commercial IoT server, i.e. Alibaba Cloud, G2F demonstrates the ability to protect against malicious attacks with high authentication efficiency.

M. Naveed Aman et al[6] Energy-quality scaling is introduced at several levels of abstraction, from the individual components in the security subsystem to the network protocol level. The analysis on an MICA 2 mote platform shows that the proposed scheme is robust against different types of attacks and reduces the energy consumption of IoT devices by up to 69% for authentication and authorization, and up to 45% during data transfer, compared to a conventional IoT device with fixed key size.

J. Khan et al., [7] proposed an authentication scheme based on the OAuth 2.0 protocol to secure access loT network by providing authentication service. An OAuth 2.0 protocol is used to propose authentication mechanism to allow only authorized and authentic users by comparing user information and access tokens in the security manager local database and denies the access to the loT network. It also keeps safe loT network from different types of attacks like impersonation and replays attacks etc.

III. PROPOSED METHODOLOGY

The authors in [9] discuss access control's importance in distributing trusts among entities in the IoT environment. They propose using a hybrid architecture called Auth, locally centralized yet globally distributed architecture. With this approach, an IoT gateway governs IoT devices in the domain centrally, while the system manages accesses to different domains distributedly. A similar design pattern also appears in LSB [10]. The authors take the same hybrid architecture idea to the blockchain realm. Specifically, they suggest using two blockchain networks. A local blockchain network exists on each of the

IoT domains, with the IoT gateway serves as a central authority that mines the blockchain solely. Meanwhile, an overlay blockchain network oversees the governance among multiple domains in a decentralized manner. Similar to previously mentioned proposals, we also employ a gateway-based architecture in this paper. In particular, the gateways manage the domain centrally while the blockchain maintains inter-domain communications governance.

propose a decentralized authentication system that provides excellent key management features such as online and offline secret key, public keys binding to domains, public key lookups, key recovery, and key revocation. Moreover, this study also presents several strategies to cut down blockchain's storage requirements using accumulators and Distributed Hash Table. Together with SCPKI [12], these two papers can serve as extensions to our protocol. We can use them for our key and certificate management, which we do not discuss in this paper. Another study uses blockchain to provide an out-of-band authentication [13]. Before getting access to IoT resources, IoT devices need the help of a nearby already-authenticated device to provide proof for their authentications. For example, the IoT server instructs a light bulb to perform a secret sequence that the target device has to decode and present back to the server through blockchain. In other words, the system resembles a two-factor authentication mechanism. Therefore, this study can serve as an alternative method for authentication between IoT devices and vendors in our protocol. Bubbles of Trust (BoT) [14] propose an IoT authentication mechanism using virtual domains, called a bubble. A Master exists in their architecture to create bubbles in the blockchain and distribute tickets to the Follower. The Follower has to sign those tickets and deliver them to the blockchain for authentication to join a bubble. At the n-th transaction, when the Follower wants to transmit messages to other entities in the same bubble, he sends a transaction to the blockchain by attaching his previous tickets as proof for authentication.

oT AUTHORIZATION FairAccess [16] proposes the use of blockchain to store access token for IoT authorization. The resource owner sends an access token to the requester by creating a transaction and lock script in the blockchain. The requester then generates an unlocking script for the access token and then sends a reply transaction back to the blockchain. At this moment, the authorization is complete. Other parties can conduct verification by checking that the script from the requester can unlock the token. Because this study is one of the first blockchain-based IoT authorization schemes, the authors employ the scripting model of the Bitcoin with limited functions. However, our proposal makes use of a more modern approach by leveraging the smart contract. Like the previous research, IoTChain [17] also stores proofs of access control in the blockchain. However, this study's distinguishable feature is the introduction of the Key Server, which serves as a proxy for the client and server to communicate securely. By default, IoT services encrypt all the IoT resources using a secret key. IoT users then have to get the key from the Key Server to decrypt the resource. However, the key server will check the proof in the blockchain before he distributes the keys to the users. Unlike this approach, clients and servers can build a secure channel without any proxy or centralized third party in our proposal

IoT Hub security tokens

IoT Hub uses security tokens to authenticate devices and services to avoid sending keys on the network. Additionally, security tokens are limited in time validity and scope. Azure IoT SDKs automatically generate tokens without requiring any special configuration. Some scenarios, however, require the user to generate and use security tokens directly. These scenarios include the direct use of the MQTT, AMQP, or HTTP surfaces, or the implementation of the token service pattern.

More details on the structure of the security token and its usage can be found in the following articles:

Security token structure

Using SAS tokens as a device

Each IoT Hub has an identity registry that can be used to create per-device resources in the service, such as a queue that contains in-flight cloud-to-device messages, and to allow access to the device-facing endpoints. The IoT Hub identity registry provides secure storage of device identities and security keys for a solution. Individual or groups of device identities can be added to an allow list, or a block list, enabling complete control over device access. The following articles provide more details on the structure of the identity registry and supported operations.

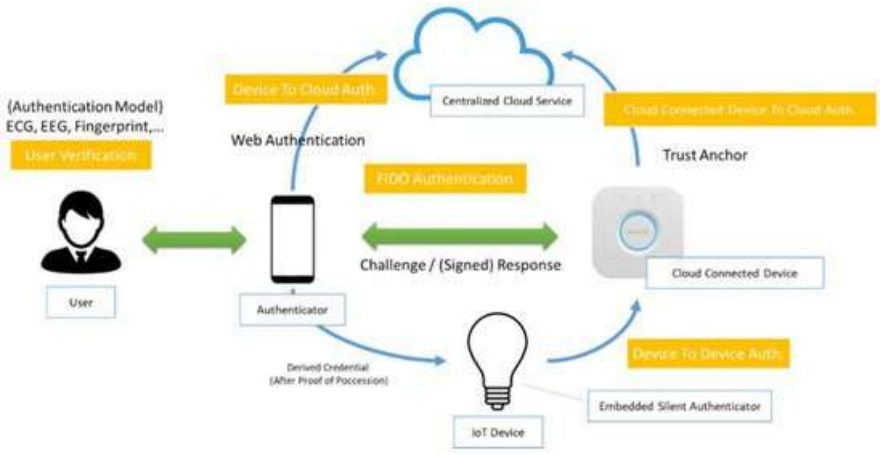

Figure 2: Iot Device Communication (Chiu et al[16])

IoT Hub supports protocols such as MQTT, AMQP, and HTTP. Each of these protocols uses security tokens from the IoT device to IoT Hub differently:

AMQP: SASL PLAIN and AMQP Claims-based security ({policyName}@sas.root.{iothubName} with IoT hub-level tokens; {deviceId} with device-scoped tokens).

MQTT: CONNECT packet uses {deviceId} as the {ClientId}, {IoThubhostname}/{deviceId} in the Username field and an SAS token in the Password field.

HTTP: Valid token is in the authorization request header.

IoT Hub identity registry can be used to configure per-device security credentials and access control. However, if an IoT solution already has a significant investment in a custom device identity registry and/or authentication scheme, it can be integrated into an existing infrastructure with IoT Hub by creating a token service.

Secure device provisioning and authentication

The IoT solution accelerators secure IoT devices using the following two methods:

By providing a unique identity key (security tokens) for each device, which can be used by the device to communicate with the IoT Hub.

By using an on-device X.509 certificate and private key as a means to authenticate the device to the IoT Hub. This authentication method ensures that the private key on the device is not known outside the device at any time, providing a higher level of security.

The security token method provides authentication for each call made by the device to IoT Hub by associating the symmetric key to each call. X.509-based authentication allows authentication of an IoT device at the physical layer as part of the TLS connection establishment. The security-token-based method can be used without the X.509 authentication, which is a less secure pattern. The choice between the two methods is primarily dictated by how secure the device authentication needs to be, and availability of secure storage on the device (to store the private key securely).

. Protocol Evaluation It contains the most recent research and categorizes it from multiple perspectives. It shows how context-awareness extends security and what approaches exist to incorporate context-awareness into IoT security. It shows how existing and current, widely adopted technologies are adapted for the IoT and surveys new security proposals designed specifically for that environment. We discussed whether security solutions for centralized or distributed architectures are favored and analyzed whether machine-to-machine or user-to-machine security is more prevalent in the current research. To our best knowledge there is no similar study or survey of IoT security or any other study containing the latest IoT security research. We believe that this overview will help readers gain an overall picture about the state

of IoT security research, allowing them to reapply existing knowledge and deal with the security issues that are preventing IoT popularity and adoption from increasing among end users. The proposed protocol is tested using AVISPA/ HLPSL by simulating the intruder behavior, searching for any insecure channel, encryption efficiency, or weak authentication. This analysis, has the following assumptions: intruder knowledge includes all the public keys, and also intruder is aware of all roles but not the private keys nor device IDs. The main attacks that considered by this analysis are masquerade, manin-the-middle, and replay attacks. The outcome result from the AVISPA analysis is a safe protocol or not a safe protocol based on the secrecy and weak authentication criteria. This test includes three different steps. In each step, there are specific roles, session knowledge, initial state, and transactions. This protocol has the following steps: (step 1) Gateway registration, (step 2) Device registration, and (step 3) device authentication. In (step 1) there are two roles Gateway and Controller. The predefined goals for this step are the secrecy of (IDg||T) and the strong authentication between the Gateway and Controller. The gateway ID is used as a challenge to authenticate the connection between controller and gateway. In (step 2) there are three roles Device, Gateway, and Controller. Analysis goals are defined to be the secrecy of (IDd||N1) and the strong authentication between Device and Gateway. In (step 3), there are two roles Device and Gateway. Goals are defined to be the secrecy of (T), and also strong authentication between device the controller Connection. This paper selected the ECC cryptography to reduce the overhead in our schema as the key size fits the IoT limited storage and processing capacity. IoT devices should store its identity, private and public keys and also gateway public key (Kud||Krd||IDd||Kug). The device should create a nonce as a challenge to authenticate the gateway. In (step 3) when the device receives the access token (T), the device should check the received nonce. The result of the AVISPA for the above three steps shows that the proposed protocol is safe, the secrecy and strong authentication criteria are met.

IV. CONCLUSION

This article provides overview of implementation level details for designing and deploying an IoT infrastructure using Azure IoT. Configuring each component to be secure is key in securing the overall IoT infrastructure. The design choices available in Azure IoT provide some level of flexibility and choice; however, each choice may have security implications. It is recommended that each of these choices be evaluated through a risk/cost assessment.

REFERENCE

[1]. A. Corici, Y. Shashi, M. Corici, R. Shrestha and D. Guzman, "Enabling Dynamic IoT Security Domains : Cellular Core Network and Device Management Meet Authentication Framework," 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 2019, pp. 1-6, doi: 10.1109/GIOTS.2019.8766390.

[2]. T. Claeys, F. Rousseau and B. Tourancheau, "Securing Complex IoT Platforms with Token Based Access Control and Authenticated Key Establishment," 2017 International Workshop on Secure Internet of Things (SIoT), Oslo, Norway, 2017, pp. 1-9, doi: 10.1109/SIoT.2017.00006.

[3]. S. Kinikar and S. Terdal, "Implementation of open authentication protocol for IoT based application," 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2016, pp. 1-4, doi: 10.1109/INVENTIVE.2016.7823267.

[4]. L. Zhou, C. Su, W. Chiu and K. -H. Yeh, "You Think, Therefore You Are: Transparent Authentication System with Brainwave-Oriented Bio-Features for IoT Networks," in IEEE Transactions on Emerging Topics in Computing, vol. 8, no. 2, pp. 303-312, 1 April-June 2020, doi: 10.1109/TETC.2017.2759306.

[5]. H. Luo, C. Wang, H. Luo, F. Zhang, F. Lin and G. Xu, "G2F: A Secure User Authentication for Rapid Smart Home IoT Management," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3050710.

[6]. M. Naveed Aman, S. Taneja, B. Sikdar, K. C. Chua and M. Alioto, "Token-Based Security for the Internet of Things With Dynamic Energy-Quality Tradeoff," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2843-2859, April 2019, doi: 10.1109/JIOT.2018.2875472.

[7]. J. Khan et al., "An Authentication Technique Based on Oauth 2.0 Protocol for Internet of Things (IoT) Network," 2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 2018, pp. 160-165, doi: 10.1109/ICCWAMTIP.2018.8632587.

[8]. F. Wang, Y. Xu, L. Zhu, X. Du and M. Guizani, "LAMANCO: A Lightweight Anonymous Mutual Authentication Scheme for N -Times Computing Offloading in IoT," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4462-4471, June 2019, doi: 10.1109/JIOT.2018.2888636.
[9]. Rajawat A.S., Upadhyay P., Upadhyay A. (2021) Novel Deep Learning Model for Uncertainty Prediction in Mobile Computing. In: Arai K., Kapoor S., Bhatia R. (eds) Intelligent Systems and Applications. IntelliSys 2020. Advances in Intelligent Systems and Computing, vol 1250. Springer, Cham. https://doi.org/10.1007/978-3-030-55180-3_49
[10]. M. Mumtaz, J. Akram and L. Ping, "An RSA Based Authentication System for Smart IoT Environment," 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Zhangjiajie, China, 2019, pp. 758-765, doi: 10.1109/HPCC/SmartCity/DSS.2019.00112.
[11]. X. Zheng, Y. Sun, Z. Lin and J. Min, "A Secure Dynamic Authorization Model Based on Improved CapBAC," 2019 International Conference on Information Technology and Computer Application (ITCA), Guangzhou, China, 2019, pp. 114-117, doi: 10.1109/ITCA49981.2019.00033.
[12]. Ö. Yerlikaya and G. Dalkılıç, "Authentication and Authorization Mechanism on Message Queue Telemetry Transport Protocol," 2018 3rd International Conference on Computer Science and Engineering (UBMK), Sarajevo, Bosnia and Herzegovina, 2018, pp. 145-150, doi: 10.1109/UBMK.2018.8566599.
[13]. Chuang, Y. H., Lo, N. W., Yang, C. Y., & Tang, S. W. (2018). A Lightweight Continuous Authentication Protocol for the Internet of Things. Sensors (Basel, Switzerland), 18(4), 1104. https://doi.org/10.3390/s18041104
[14]. Anand Singh Rajawat, Dr. Akhilesh R. Upadhya, "Big Web Data Mining for Predicting Usage Behaviour Using Fusion Map Reduce Model ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 3, Issue 1, pp.1641-1647, January-February-2018
[15]. K. Yeh, C. Su, W. Chiu and L. Zhou, "I Walk, Therefore I Am: Continuous User Authentication with Plantar Biometrics," in IEEE Communications Magazine, vol. 56, no. 2, pp. 150-157, Feb. 2018, doi: 10.1109/MCOM.2018.1700339.
[16]. Chiu, Wayne; Su, Chunhua; Fan, Chuan-Yen; Chen, Chien-Ming; Yeh, Kuo-Hui. 2018. "Authentication with What You See and Remember in the Internet of Things" *Symmetry* 10, no. 11: 537. https://doi.org/10.3390/sym10110537
[17]. K. Barhanpurkar, A. S. Rajawat, P. Bedi and O. Mohammed, "Detection of Sleep Apnea & Cancer Mutual Symptoms Using Deep Learning Techniques," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 821-828, doi: 10.1109/I-SMAC49090.2020.9243488.
[18]. Pinto, A., & Costa, R. (2016). Hash-chain-based authentication for IoT. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, 5(4), 43-57. https://doi.org/10.14201/ADCAIJ201654435
[19]. T. L. N. Dang and M. S. Nguyen, "An Approach to Data Privacy in Smart Home using Blockchain Technology," 2018 International Conference on Advanced Computing and Applications (ACOMP), Ho Chi Minh City, Vietnam, 2018, pp. 58-64, doi: 10.1109/ACOMP.2018.00017.