UDC 621.391.3

SECURE IOT DEVICE AUTHENTICATION

Minochkin D., Sushyn I.
National Technical University of Ukraine
“ Igor Sikorsky Kyiv Polytechnic Institute”
E-mail: dmytro.minochkin@gmail.com, rubin26898@ukr.net

БЕЗПЕЧНА АУТЕНТИФІКАЦІЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

У статті наводиться опис способу аутентифікації пристроїв інтернету речей та користувацьких пристроїв за допомогою хмарної технології з використанням цифрових сертифікатів. Наведено структуру мережі на основі інфраструктури відкритого ключа.

The growth of number of intelligent devices will create a network rich with information that allows supply chains to assemble and communicate in new ways. The technology research company “Statista” predicts that there will be above 74 billion installed units on the Internet of Things (IoT) by 2025 [1].

The Internet of Things (IoT) provides the ubiquitous connection between devices with sensitive and communication capabilities. IoT programs include healthcare, smart cities, smart grid, automotive, industrial applications, etc. [2], [3], [4]. IoT provides a large-scale deployment of communication between the device and machine to machine. The low complexity and low energy requirements for these devices pose security problems [5].

IoT device authentication is a vital step in key validation and key sharing, otherwise systems are open to attacks such as man-in-the-middle. In various studies and literature reviews security issues have been discussed, however, due to the lack of emphasis on a more structured and robust security architecture, security and privacy issues still remain. Thus, IoT authentication, access control, and intrusion attacks are major security issues you may encounter when implementing an IoT system.

In the proposed platform we focused on these security issues and offered a secure platform that allows user and IoT device to log on to a cloud server using a digital certificate. Once the registration process is completed, only the actually registered user can access the IoT device available on the network.

The platform (shown in Figure 1) is based on the Public Key Infrastructure

(PKI) system that manages certificates, systems, and applications to uniquely identify users, services and devices used on the network. An effective PKI should be transparent and comply with security principles, especially authentication and data integrity. This platform consists of IoT devices, users, cloud, certification authority (CA) and registration center (RA). Before connecting, IoT users and devices must be registered in the cloud with their verified digital certificate.

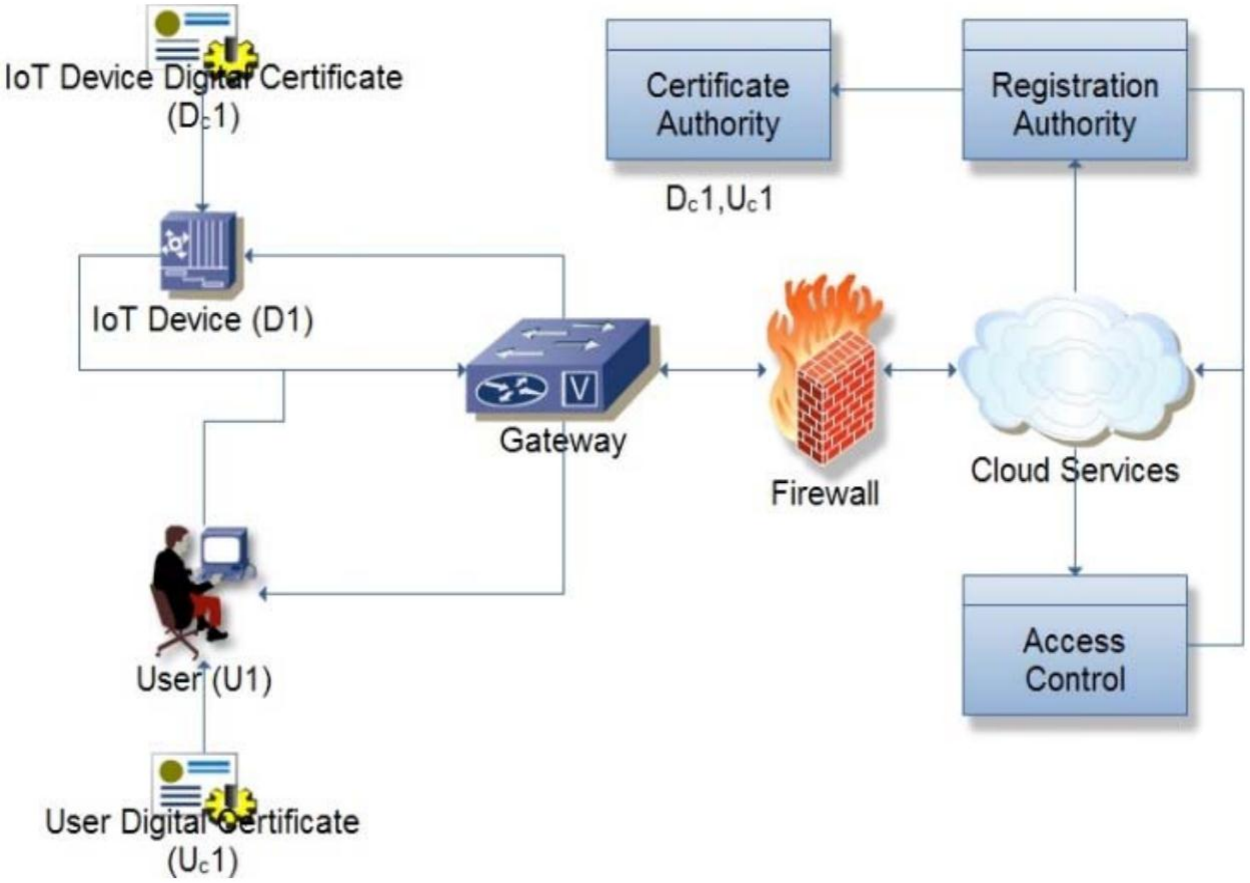

Fig. 1. Security platform for Cloud based IoT Network.

These certificates can be obtained from the RA. Here, the cloud application authenticates itself through PKI, but then issues certificates to the devices and users. Therefore, the cloud application also issues a separate certificate for the device, and for users these certificates are displayed as Dc1 and Uc1. The third and most important element in this platform is the centralized cloud, in which all devices, users and certificates with the corresponding keys Dc1, Uc1, ... are stored and indexed in their central repository. The registering authority provides the PKI binding, which is additionally linked to the CA certificate.

When a user registers, the cloud application checks the user’s identity (for example, using the second factor, such as a voice call or SMS) before generating a certificate for storage in the central cloud and issuing the certificate to the user application through a properly protected TLS channel. The device also has a unique certificate issued by the vendor. The device certificate and a unique device ID (included with the certificate) can be set before sending. When the user wants to use the device, the cloud app checks the user's certificate from the cloud index and access control defined in the management system.

Available Public key certificates require the following services: certificate storage; creation and revocation of certificates; key story management. The management system contains backup/restore keys; non-repudiation of digital signature systems; automatic update of key pairs and certificates. These digital certificates contain information such as the public key, name and expiration date of the certificate. The Certification authority is an integral part of PKI, as it is a source of trust and provides services to ensure an individual level of authentication of business units in the information exchange.

Conclusion. The proposed security structure based on PKI and implemented on IoT network is expected to be robust and very secure as it covers the major gap that exists in the application layer of the IoT infrastructure. In particular the work is focused on the systems authentication: device-to-cloud, user-to-cloud and user-to-device. It will also reduce the costs associated with the loss and allow new services to be introduced.

References

1. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 // - Access mode: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
2. L. Atzori, A. Iera, and G. Morabito, The Internet of Things: A survey.: Computer Networks, 2010, vol. 54, no. 15, pp. 2787–2805.
3. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of Things: A survey on enabling technologies, protocols, and applications.: IEEE Commun. Surveys Tuts., Fourth Quarter 2015, vol. 17, no. 4, pp. 2347–2376.
4. S. Mumtaz, A. Bo, al-Dulaimi and K.Tsang. Guest Editorial 5G and Beyond Mobile Technologies and applications for Industrial IoT.: IEEE Transactions on Industrial Informatics, June 2108, vol 14, no. 6, pp. 2588-2591.
5. J. Zhang, Trung Q. Duong, R. Woods, A. Marshall. Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview: ResearchGate, 2017.