The Seybold Report

ISSN 1533-9211

DOI 10.5281/zenodo.6997861

DEVELOPMENT OF IOT SECURITY STRATEGY WITH MQTT PROTOCOL ENABLED CRYPTOGRAPHIC SMART CARD SECURITY

SHAMITA SHIVASHANKAR HIREMATH

Research scholar, Shri JJT University, Jhunjhunu, Rajasthan, India. Email: shamitha.hm@gmail.com

ABSTRACT

Internet of Things is a most promising domain where the confidentiality and integrity of data is a key to maintain the application security. Cryptographic smart card security is very crucial element in almost all financial, healthcare organizations. Though the chips security is the element of embedded systems, the IoT enabled an interdisciplinary research where IoT protocols play an important role to secure the chip. Hence, this paper presents the device to device communication strategy where every smart card and card reader supports MQTT protocol. This proved to be a more efficient strategy over the existing research.

KEYWORDS: Internet of Things, CoAP, MQTT, Smart Card Security

1. INTRODUCTION

The Message Queuing Telemetry Transport (MQTT) [1, 2] protocol is one of the most extended protocols on the Internet of Things (IoT). However, this protocol does not implement a strong security scheme by default, which does not allow a secure authentication mechanism between participants in the communication. Furthermore, we cannot trust the confidentiality and integrity of data. Lightweight IoT devices send more and more sensible data in areas of Smart Card, Smart House, Health Care, Industrial IoT (IIoT), etc. This makes the security challenges in the protocols used in the IoT particularly important [3].

Author(s) proposed the smart card authentication method that has four phases, as user registration phase, login phase, mutual authentication phase, and password update phase. Initially, the user accesses the real-time information from the sensing node by registering at the gateway node. During the login phase, the smart card is used by the user to login into the system with the supplied. In the mutual authentication phase, a session key is established between the accessed sensing node and the user through the gateway node. Finally, at the password update phase, the legitimate user updates the password without involving the gateway node. The proposed ECC-based authentication scheme is analyzed using the metrics, such as detection rate, delay, and throughput for varying number of rounds [4].

Aside from this, smart consumer electronic devices are mostly area constrained and operate on a limited battery supply and therefore, have tight energy budgets. Lightweight Cryptography (LWC) such as PRESENT-80 allows for minimal area usage and low energy for secure operations. However, CMOS implemented LWCs are vulnerable to side-channel attacks such as Correlation Power Analysis (CPA) [5]. The authentication and key agreement protocol is one of fundamental building blocks for securing communications over the Internet. It enables protocol participants to authenticate each other's identities and establish shared session keys subsequently used by encryption algorithms and is widely implemented in many areas, such as

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.6997861

online-shopping, Internet banking, electronic governance, and electronic medical record system [6]. Employing a graphical modeling tool (Unified Modelling Language), the design integrates an additional input, through an inbuilt IP Camera that stealthily captures the ATM user facial image, which is automatically transmitted to the mobile device of the bank account owner, through some dedicated artificial intelligent agents, for remote certification, which either authorizes the transaction appropriately or signals a security-violation alert to the banking security system [7].

In summary, the smart card systems security is a combination of computational intelligence with digital communication strategies and designs. In this paper, section 2 discusses the existing IoT research, section 3 presents the proposed methodology, section 4 discusses the comparative results and section 5 concludes the findings.

2. LITERATURE REVIEW

Message Queue Telemetry Transport (MQTT) is one of promising protocol for data exchange in IoT that could encounter such issues because it relies on central broker and gateway devices, and this may lead to increase network congestion, performance overhead or bottleneck. Firstly, security procedures need to be modified because MQTT that based on distributed architecture require additional multiple brokers and different communication standards that may increase security threats and increase security management complexity. Secondly, MQTT is inherently lacking efficient security features because it performs username/password-based authentication in a plain text, that protected by cryptographic protocol SSL/TSL which is not consider as lightweight protocol for resources constrained devices [8]. To ensure secure access to the data held in internet of things, many lightweight authentication schemes have been developed using approaches such as symmetric cryptography or hashing operations. However, some of these schemes are still susceptible to smart card loss attacks among others. In this paper, stochastic security ephemeral generation protocol for 5G enabled internet of things is presented. It is demonstrated to offer mutual authentication and session key agreement. It is also robust against packet replays, eavesdropping and man-in-the-middle attacks. In terms of performance, it has the lowest computation and communication overheads [9].

To deal with these attacks, there are many protocols for authentication for internet of things. In fact, an appropriate authentication protocol plays an important role in ensuring secure communications for internet of things. In this paper, author proposed an authentication scheme with key agreement on elliptic curve cryptography (ECC) [10]. Information leakage in cloud-assisted IoT devices may invite dangerous activities and phenomena. This paper proposes a novel and efficient protocol based on the Elliptic Curve property known as Elliptic Curve Discrete Logarithm Problem (ECDLP) with hash and XOR functions for the authentication in cloud-based IoT devices. In comparison to the existing protocols, the proposed protocol is resistant to attacks and other security vulnerabilities [11].

Author implemented an anonymous, mutual, and secures two-factor authentication and key agreement scheme applied to the computing environment. Author used elliptic curve cryptography and a fuzzy verifier to strengthen security of smart cards and reader [12]. In this

ISSN 1533-9211

DOI 10.5281/zenodo.6997861

paper, author proposed a lightweight secure secret key-sharing system based on a secret-sharing scheme for resource-constrained IoT devices. The proposed system uses a (k, n)-threshold secret-sharing scheme to securely share a secret key for data encryption between the publisher and its subscriber hosts without compromising the lightweight nature of the MQTT protocol [13]. A security scheme in the MQTT protocol uses cryptographic smart cards for encrypting the client-to-broker data communication without changing protocol message specifications. This authentication scheme meets the requirements of both data secrecy and data integrity. The implementation of the Keyed-Hash Message Authentication Code (HMAC) generation algorithm has been employed instead of a complex encryption algorithm to improve the efficiency with less time for the client to retrieve the messages [14].

3. RESEARCH METHODOLOGY

As smart card and card reader is considered as a device-to-device communication, we identified that, the three layer IoT architecture prone to different kind of attacks based on digital data communication. Thus, authentication considered a core security requirement for all IoT layers [15, 16]. The three layer IoT architecture comprises:

- Perception layer: this contains sensors which need node authentication to prevent such as replay attack and forgery attack.
- Network layer: where data transmission and routing occur, vulnerable to eavesdropping and MITM attack.
- Application layer: this is based on messaging protocols such as MQTT and CoAP, is responsible for delivering IoT services to users which require to be authenticated.

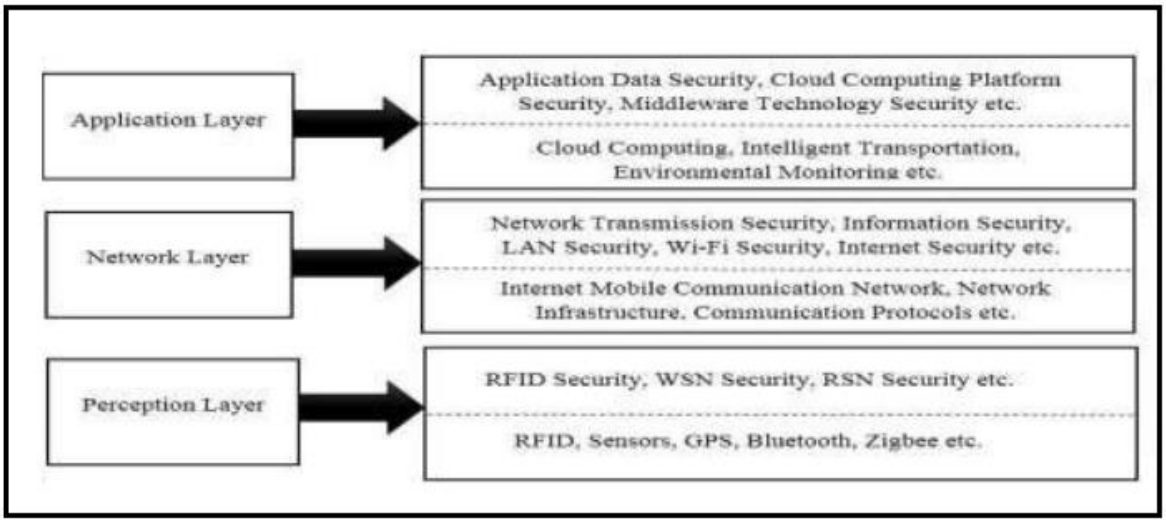

Fig. 1: Three Layer IoT Architecture (Md. Tareq Hasan, 2017)

Based on the three layer IoT architecture, application layer and perception layer security can be provided for MQTT protocol by means of duel verification mechanism. The flow of

ISSN 1533-9211

DOI 10.5281/zenodo.6997861

proposed methodology is depicted in Fig. 2 below. This method first gets smart card details as an input to system where card reader is considered as a separate device of communication transfer unit. We consider here the financial transaction event of smart card.

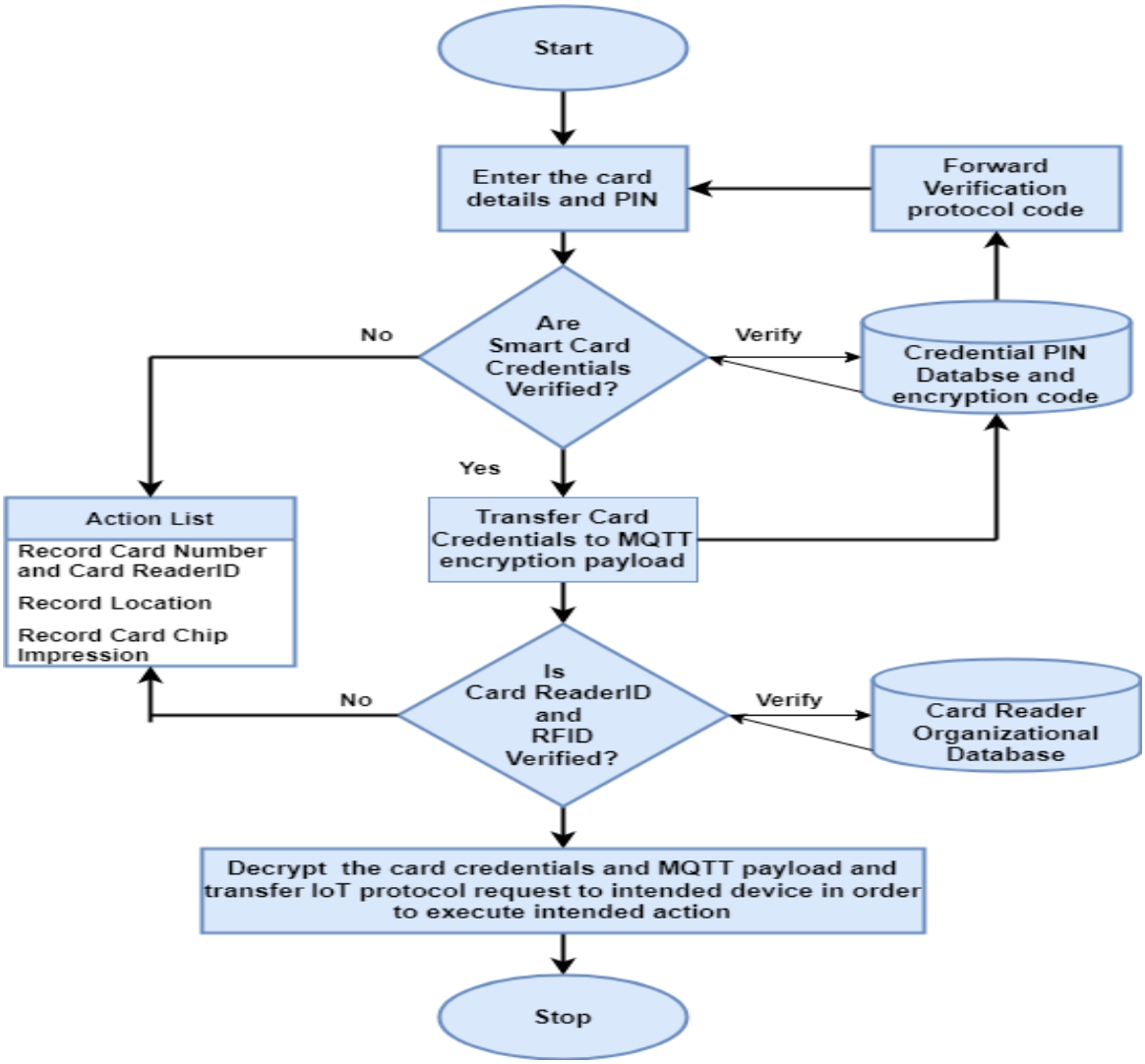

Fig. 2: IoT Security Provision with MQTT protocol security for Smart Card

In a traditional security mechanism, only user credentials are verified and/or used cipher text mechanism but in proposed system, IoT protocol MQTT is considered to provide end-to-end digital communication security along with device securities.

4. RESULTS AND ANALYSIS

The proposed system performance is compared with existing system [12] for parameters like Average User Login Time, Car reader response time, Average card blocking time, Average

ISSN 1533-9211

DOI 10.5281/zenodo.6997861

card reader locator. The details of comparison of proposed security system and existing system are shown in following Table 1.

Table 1: Proposed System Performance comparison for Smart card security

Parameters	Proposed System –MQTT protocol security	Existing System [12]
Average User Login Time (ms)	60	80
Car reader response time (ms)	0.85	0.98
Average card blocking time (ms)	1.56	1.92
Average card reader locator (ms)	1.45	2.15

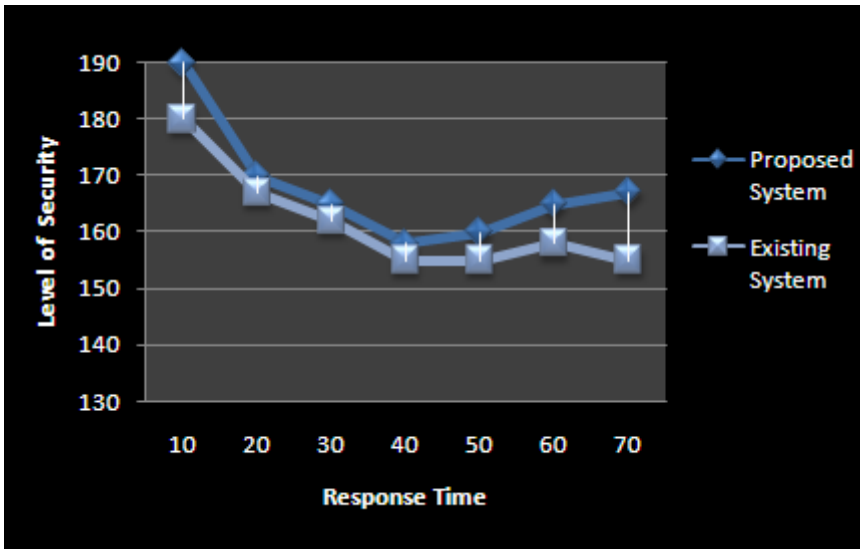

Fig. 3: Performance Comparison Chart

From the above Fig. 3 it is clear that the MQTT protocol enabled system security for Smart Card and Card reader is most promising than the existing encryption based system in terms of utility security of any electronics devices.

5. CONCLUSION

As the smart card is the heart of application technologies with IoT architecture, paper presented the generic approach to protect smart card transactions. In case of healthcare, banking, agricultural and international tourist cards; it is the base need to provide security. Card transaction can face SQL injection, jitter or delay issues by hacker but MQTT protocol communication sequence can enroll such activities and blocks smart card within milliseconds of duration. Hence, it is very helpful for any electronic chip design organization to provide middleware broker facility to communicate with server for fast response. As a future approach, this can be developed with other IoT protocols like CoAP, AMPQ etc.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.6997861

REFERENCES:

[1] Sharma, Geeta, and Sheetal Kalra. "A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications." Journal of information security and applications 42 (2018): 95-106.

[2] Das, Ashok Kumar, et al. "On the security of a secure and lightweight authentication scheme for next generation IoT infrastructure." IEEE Access 9 (2021): 71856-71867.

[3] Sanjuan, Eduardo Buetas, et al. "Message queuing telemetry transport (MQTT) security: a cryptographic smart card approach." IEEE Access 8 (2020): 115051-115062.

[4] Joy, A. Shakeela, and R. Ravi. "Smart card authentication model based on elliptic curve cryptography in IoT networks." International Journal of Electronic Security and Digital Forensics 13.5 (2021): 548-569.

[5] Kahleifeh, Zachary, and Himanshu Thapliyal. "Adiabatic logic based energy-efficient security for smart consumer electronics." IEEE Consumer Electronics Magazine 11.1 (2020): 57-64.

[6] Zhao, Yan, Shiming Li, and Liehui Jiang. "Secure and efficient user authentication scheme based on password and smart card for multiserver environment." Security and Communication Networks 2018 (2018).

[7] Popoola, Olugbemiga Solomon, et al. "Design of a Customer-Centric Surveillance System for ATM Banking Transactions using Remote Certification Technique." 2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA). IEEE, 2021.

[8] Kurdi, Hassan, and Vijey Thayananthan. "Authentication mechanisms for IoT system based on distributed MQTT brokers: review and challenges." Procedia Computer Science 194 (2021): 132-139.

[9] Al Sibahee, Mustafa A., et al. "Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things." International Conference on Internet of Things as a Service. Springer, Cham, 2022.

[10] Asghari, Rahim. "A Mutual Lightweight Authentication Protocol for Internet of Things Environment Using smart card." Computational Sciences and Engineering 2.1 (2022).

[11] Alam, Irfan, and Manoj Kumar. "A novel protocol for efficient authentication in cloud-based IoT devices." Multimedia Tools and Applications 81.10 (2022): 13823-13843.

[12] Bouchaala, Mariem, Cherif Ghazel, and Leila Azouz Saidane. "Enhancing security and efficiency in cloud computing authentication and key agreement scheme based on smart card." The Journal of Supercomputing 78.1 (2022): 497-522.

[13] Noguchi, Taku, et al. "A Secure Secret Key-Sharing System for Resource-Constrained IoT Devices using MQTT." 2022 24th International Conference on Advanced Communication Technology (ICACT). IEEE, 2022.

[14] Siddharthan, Hariprasad, T. Deepa, and Prabhu Chandhar. "SENMQTT-SET: An Intelligent Intrusion Detection in IoT-MQTT Networks Using Ensemble Multi Cascade Features." IEEE Access 10 (2022): 33095-33110.

[15] Zaman, Umar, et al. "Towards Secure and Intelligent Internet of Health Things: A Survey of Enabling Technologies and Applications." Electronics 11.12 (2022): 1893.

[16] Gupta, Ankita, et al. "IoT and RFID-Based Smart Card System Integrated with Health Care, Electricity, QR and Banking Sectors." Artificial Intelligence on Medical Data. Springer, Singapore, 2023. 253-265.