Quick Response Technique based Security Mechanism Design for Digital Hubs and LOT Systems

Abbas M. Al-Ghaili, Marini Othman, Hairoladenan Kasim, Zainuddin Hassan

ABSTRACT--- In this paper, the Quick Response (QR) technique is used to generate an encrypted QR-Code. This paper designs a security mechanism to verify certain related information used to access an Internet of Things (IoT) based system. Only authorized requests are enabled to access the IoT system. To achieve this goal, the proposed security mechanism has used a three-Layer-Policy Verification Procedure (3LPVP). The proposed 3LPVP is applied on the QR-Code; this code is used as an IoT-key dedicated for a secure access. The proposed mechanism is important for a number of IoT-based systems that require information being shared and/ or transmitted between two parties or more, e.g., digital hubs, digital ecosystems, and other industry 4.0 related technologies. The 3LPVP needs to verify IoT-key's contents during the first layer to authenticate issue of the IoT-key. In addition, the IoT-key is periodically generated using a 1-session cryptographic key to keep the IoT-key confidential. To verify the IoT-key's integrity, related values are compared to original hash values using a secret question to which the user needs to answer. In the third layer, data is stored using an offline mode to disable any access caused by threats; to preserve the IoT-key available and responsive. The 3LPVP is evaluated in terms of security factors and then compared to a number of competitive techniques. Results have shown good performance of 3LPVP against brute force attack and encryption's computation time.

Keywords—Internet of Things; security systems; QR-code; digital hubs; Industry 4.0

I. INTRODUCTION

Many researchers from different fields have used the Quick Responsive Code (QR-Code) technique for different purposes [1] e.g., remote user authentication process with smart cards has been discussed [2]. However, this technique could be used for verification procedures for security purposes [3], [4]. The variety of IoT systems is one of the reasons that many researchers have been attracted to design secure systems [5]. These systems are used for different purposes e.g., biometrics-based home access system [6], and location detection [7].

The QR-Code is a very effective and usable technology on which Internet of Things (IoT) systems rely [8]. It plays an important role as a connector between IoT and secure systems due to its features e.g., smart application reliability, data integrity, availability and responsiveness [9], usability (ease-to-use). In addition, it stores a huge number of data in a simple image with small size, so that QR tags are easily scanned. Once, QR-Code data (i.e., IoT-key contents) is extracted, a verification process is implemented to compare between values. Thus, IoT-key based verification process is essential in IoT systems in terms of privacy [10].

Additionally, in order for the IoT technology performs better, the encryption scheme applied on the IoT-key is highly considered by smart IoT systems. There are many attempts by researchers to enhance security mechanisms for IoT systems [11]. Many reviewed studies have used a single layer of encryption [11], so that threats might attack sensitive data of IoT systems. Thus, the 3LPVP is proposed in order to include more than one layer of both encryption and verification mechanisms. The 3LPVP design has also considered the key length in order to increase the decryption time caused by an attack.

Such security mechanisms should have enhanced intelligent digital systems and IoT based systems such as industry 4.0 applications in terms of data privacy. These systems and applications require a strong security scheme. In literature, there have been various applications reviewed [12]. These have included, for example, in [13], a digital hub technology based system is proposed to provide solutions to disable people using digital information collection to be shared. Some other examples have used the technology of digital hub to allow connected cars [14], Hub-based web [15], and sensor city [12] to transform digital information and private data.

This paper is organized as follows: Section II explains the proposed Research Method. Section III discusses the design of 3LPVP Security Mechanism for digital hub and/ or IoT related systems. Results and Analysis are presented in Section IV. Conclusion is provided in Section V.

II. RESEARCH METHOD

A. Overview - The Proposed 3LPVP Design

The proposed QR-Code based 3LPVP is designed for verification purposes. The verification procedure is associated with an encryption algorithm. The encryption algorithm uses a 1-session key. Additionally, the QR-Code is periodically generated using these encrypted values. Then, information is stored in an offline database as illustrated in

Revised Manuscript Received on 14 February, 2019.

Abbas M. Al-Ghaili, Institute of Informatics and Computing in Energy (IICE) Universiti Tenaga Nasional (UNITEN) 43000 Kajang, Selangor, Malaysia. (abbasghaili@yahoo.com & abbas@uniten.edu.my)

Marini Othman, Institute of Informatics and Computing in Energy (IICE) Universiti Tenaga Nasional (UNITEN) 43000 Kajang, Selangor, Malaysia (marini@uniten.edu.my)

Hairoladenan Kasim, College of Computer Science and Information Technology Universiti Tenaga Nasional (UNITEN) 43000 Kajang, Selangor, Malaysia (hairol@uniten.edu.my)

Zainuddin Hassan, (College of Computer Science and Information Technology Universiti Tenaga Nasional (UNITEN) 43000 Kajang, Selangor, Malaysia (zainuddin@uniten.edu.my)

Fig. 1. The 3LPVP consists of 3 layers, which are as follows: Verification Layer (VL), Encryption Layer (EL), and Database Layer (DL).

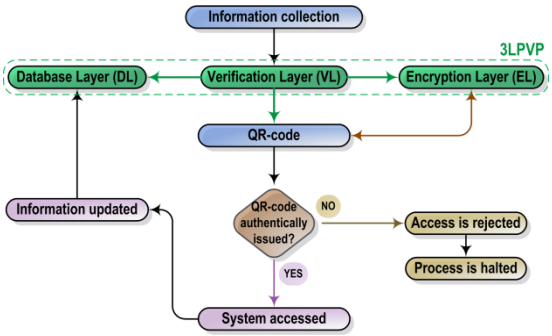

Fig. 1 The 3LPVP Blockdiagram

B. Verification Layer (VL)

VL consists of 3 processes as illustrated in Fig. 2. The first process scans and verifies values stored in IoT-key patterns. It also verifies the face and thumbprint values with their corresponding values stored in the system's database, as shown in Fig. 3. The second process asks the user to enter a reference value (RV) to determine the IoT-key expiry date. If RV is wrong, then the IoT-key is expired. The third process checks the user's ID using a comparison based algorithm.

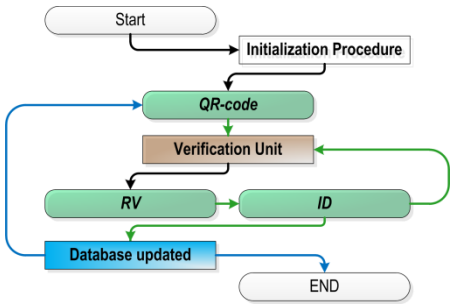

Fig. 2. VL Processes - Blockdiagram

1) Process 1: IoT-key Verification

A new user's information is collected as shown in Fig. 1. Here, values are extracted from the scanned QR-Code. These values include face image features and thumbprint properties. A series of digital image processing conversions is used to extract images' features. Values of extracted features are obtained from three sources, shown in Fig. 3, are validated. If, the result is 'true', the system can be accessed.

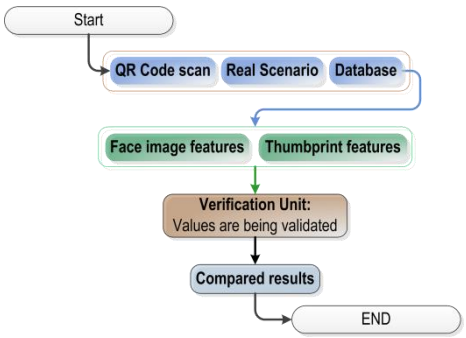

Fig. 3. IoT-key Verification (Process 1)

2) Process 2: RV Verification

The RV has been designed in a way that it periodically produces a new value. Thus, the RV is dependent on the number of access times for each user to guarantee a varied value. It varies at each time the user with the number *i*, *user(i)*, has successfully accessed the system. This activity made by the user can produce a new RV and new hash values used to encrypt the new IoT-key. Thus, a User's Activities History (UAH) is created to generate RV values. To apply the RV verification, the hash value for the user's RV is compared to the one already updated in the system database. There will be two initiated sub-routines applied in order to verify the RV, which are encryption scheme using Eq. (1) and hash function using Eq. (2) applied on Eq. (1). Both sub-routines have different secret keys.

$$E_{RV} = E(SP \odot k_p, RV) \tag{1}$$

whereas E_{RV}, $E(\dots)$, SP, k_p, $SP \odot k_p$, and RV are an obtained encrypted value, encryption function, special value obtained from UAH, 1-session secret key generated using Secure Hash Algorithm 1 (SHA-1), combined secret keys, and message, respectively.

$$H_{RV} = Hash(E_{RV} \oplus k_s) \tag{2}$$

3) Process 3: ID Verification

A series of encryption and hash functions has been used in this process to generate a strongly encrypted distinctive user ID. The ID verification process is going to compare three IDs from three sources marked in Fig. 4. During the encryption process, hash function has been used to generate new user ID with help of real values taken from database for each user. To increase the complexity of vulnerability possibility, each user *id* is hashed depending on two neighboring IDs. There is a hash function is used before the 1st round encryption is applied. ID Verification performs two-round decryption processes D1 and D2, as in Eq. (3) and Eq. (4), followed by a hash function, H, as in Eq. (5), to extract the *User_id* for values typed by the user and extracted from the IoT-key when the access is needed, see Fig. 4, marked: ①②. If the user has wrongly typed a *user_id*, there will be two wrong neighboring ids considered.

$$D1 = D(Normalized\_ID, K_2) \tag{3}$$

$$D2 = H = D(D1, K_1) \tag{4}$$

$$User\_id = Hash(id1 \oplus id2 \oplus M) \tag{5}$$

whereas Normalized_ID, K1, K2, id1, id2, and User_id are the id value given to the user, public key used to decrypt D2, public key used to decrypt D1, first neighbor id, second neighbor id, and the user id stored in database, respectively.

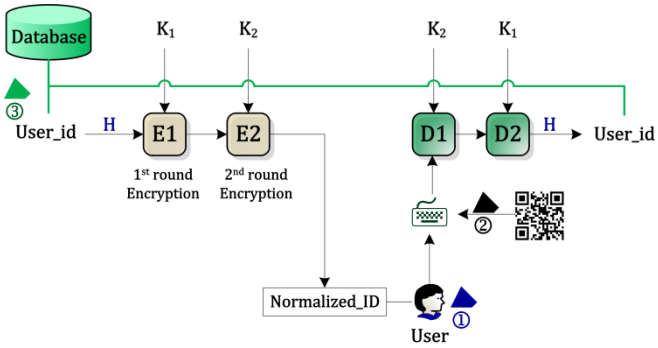

Fig 4 ID Verification (Process 3)

C. Encryption Layer (EL)

As mentioned above, VL has verified values being encrypted and hashed. Meaning, VL has compared encrypted values to original ones e.g., real scenario based values. But, EL has mainly focused on the technique being used to encrypt values and how to choose distinctive values from database e.g., UAH. It used image processing conversions to find binary values extracted from converted images. The EL has also used patterns' color inside IoT-key for the new encryption. That is, when an IoT-key is scanned, certain values are asked from the user whereas their hash values must be matched with some patterns on IoT-key in order to be read successfully; otherwise, the IoT-key is considered not real. Additionally, the EL has used a 1-session private key to prevent any disclosure of encrypted data and even though the 1-session key has been deduced. Hash functions and pseudorandom number generators are used during RV and ID processes to keep data originality. Finally, EL has considered a periodically generated IoT-key policy every 24 hours.

D. Database Layer (DL)

DL considers the system database modification caused by an authorized access. DL, periodically and in-offline mode, stores updated values. To reduce access to the database, DL has determined the Database Access Upon Necessary Requests (DAUNR). Once the process has been completely done, i.e., *process_requests_access==0*, certain values are stored in a smart way to reduce the data size and access times. More criteria on DAUNR are, less vulnerability is expected as shown in Fig. 5.

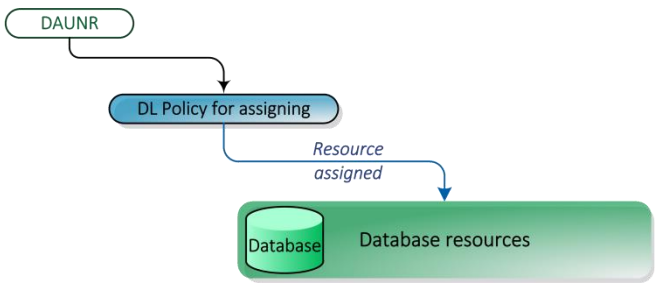

Fig 5. DL policy for an authorized access;

DAUNR recalls a time function, *Calc_Time()*, to assign a certain period of time and convert the connection status to 'Disable' by using the function: *Disconnect()* in order to update database while there is no connectivity

III. THE PROPOSED 3LPVP SECURITY MECHANISM FOR DIGITAL HUBS AND IOT SYSTEMS

This section concerns on how the 3LPVP design is secure by verifying the IoT-key to make sure that the IoT system is being in an authorized manner accessed as shown in Fig. 6. To verify the IoT-key availability, the IoT-key always recalls encrypted values from offline database to update related fields accordingly. It is then guaranteed that an authorized access to database is occurred when needed.

As for the IoT-key integrity verification, the VL verifies extracted biometrics values such as face image to check whether IoT-key contents are correct in terms of authorized modification or not. Thus, information of an IoT or a digital hub system transferred is safe. Based, the system is integrated.

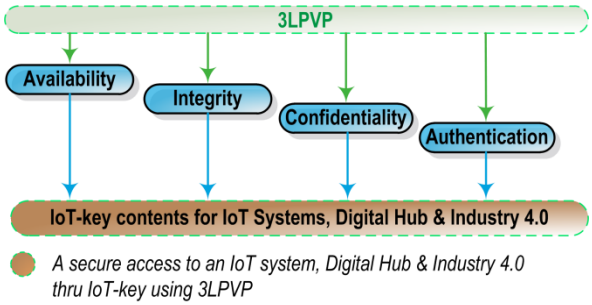

Fig 6. Security Mechanisms of 3LPVP for Digital Hub and IoT Systems

In regard to IoT-key *confidentiality* verification, contents of IoT-key are the encrypted user's information on which a collection of sequential cryptographic operations are applied. This collection has used one-time private key policy to make IoT-key confidential. The IoT-key *authentication* verification is considered. The 3LPVP policy verifies that the IoT-key is periodically produced to authenticate its issue.

IV.RESULTS AND ANALYSIS

This section presents and evaluates the performance of the proposed research work in terms of a number of security and computation factors.

A. Confidentiality

It is supposed that, there will be two units encrypted information will be transferred between. Usually, the IoT-key is scanned and then its related values are verified. These two units are close to each other and they are authorized because they are installed on a site. There will be no such long transferring data. Thus, the confidentiality will be achieved. Additionally, the secret key is used only one-time.

Integrity

As mentioned above that IoT-key values will be scanned and verified. In this type of evaluation, there will be a number-based comparison between encrypted values and original ones. If they are not equal to each other, the integrity of both IoT-key and 3LPVP is considered weak. At

this case, the VL halts this process immediately and doesn't allow an access to IoT system by the currently verified IoT-key. Additionally, in this case, that means a third party has modified IoT-key contents and no originality issue of IoT-contents and its integrity.

Availability

The 3LPVP adopted to store original and encrypted values using an offline database policy in order to control an access to this database. So that any unauthorized attempt made by a third party will be prevented. This policy has aimed to overcome any interruption of service provided which mean keep the IoT-key and its related available and responsive.

Authentication

The authentication factor to be verified is denoted by: F_{AuthN}. The IoT-key is encrypted every 24 hours in order to guarantee the authority of IoT-key issue. To make a comparison, hash values of the IoT-key produced during the last 24 hours, H_u and values of database, H_{DB} are compared using Eq. (6):

$$F_{AuthN} = \begin{cases} 1 & H_u = H_{DB} \\ 0 & H_u \neq H_{DB} \end{cases} \quad (6)$$

whereas F_{AuthN} is a logical returned value and if $F_{AuthN} = 1$; IoT-key is original.

Computation Time

The computation time of IoT-key encryption will be compared to two competitive techniques as shown in Table I. This comparison shows that 3LPVP encrypts the IoT-key faster than Certificate and [2]. The proposed 3LPVP usually needs more time for EL and VL. In addition, the hash function used is applied more than one time to increase the system security. Fig. 7 shows the 3LPVP average computation time.

Table 1. IoT-key Computation Time Compared to Other techniques

No. tests / Technique; time	10	50	100	200	500
Certificate, mS	45.2	212.6	452.2	921.6	2198.6
Ref. [2], mS	31.4	149.0	313.3	645.7	1542.5
Proposed 3LPVP, mS	28.6	132.1	226.7	521.4	1430.4

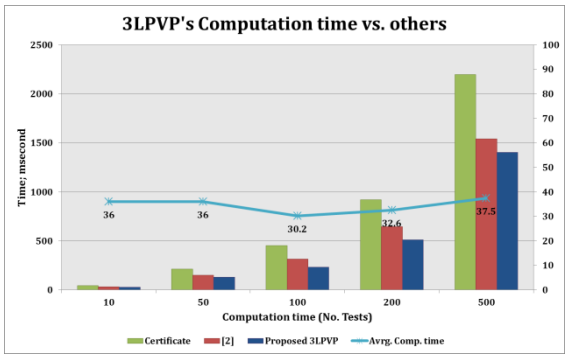

Fig .7 3LPVP average computation time compared to other techniques

V. CONCLUSION

A 3-layer policy for verification procedure (3LPVP) is proposed in order to verify whether an access to IoT systems is authorized or not. Here, technical details of the security mechanism (i.e., 3LPVP) applied on IoT-key is explained. A number of security factors have been evaluated. Results have confirmed that 3LPVP is strong against brute force attack and has less computation time compared to competitive techniques. Since digital information shared and transferred between parties in terms of data privacy could be affected, the proposed mechanism in this paper could be exploited by several digital systems and IoT such as Industry 4.0, digital hub, digital transformation applications, and software academy.

ACKNOWLEDGMENT

This research is funded by FGRS/1/2017/SS09/UNITEN/02/3, Ministry of Higher Education Malaysia; which is supported by Universiti Tenaga Nasional.

REFERENCES

1. A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A Review of Enabling Technologies, Challenges, and Open Research Issues," *Computer Networks*, 2018.
2. Y. G. Kim and M. S. Jun, "A design of user authentication system using QR code identifying method," in *2011 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*, 2011, pp. 31-35.
3. Y. Qin, Z. Wang, H. Wang, and Q. Gong, "Binary image encryption in a joint transform correlator scheme by aid of run-length encoding and QR code," *Optics & Laser Technology*, vol. 103, pp. 93-98, 2018.
4. Y. Zhou, J. Hu, S. Yuan, L. Zhang, D. Huo, J. Li, et al., "Method of multiple-image hiding in QR code based on compressed sensing and orthogonal modulation," *Optik*, vol. 159, pp. 265-274, 2018.
5. P. Nazemzadeh, D. Fontanelli, D. Macii, and L. Palopoli, "Indoor Localization of Mobile Robots Through QR Code Detection and Dead Reckoning Data Fusion," IEEE/ASME *Transactions on Mechatronics*, vol. 22, pp. 2588-2599, 2017.
6. L. Kanaris, A. Kokkinis, G. Fortino, A. Liotta, and S. Stavrou, "Sample Size Determination Algorithm for fingerprint-based indoor localization systems," *Computer Networks*, vol. 101, pp. 169-177, 2016.
7. M. Ghaffari, N. Ghadiri, M. H. Manshaei, and M. S. Lahijani, "P4QS: A Peer-to-Peer Privacy Preserving Query Service for Location-Based Mobile Applications," *IEEE Transactions on Vehicular Technology*, vol. 66, pp. 9458-9469, 2017.
8. Z. Liu, K. K. R. Choo, and J. Grossschadl, "Securing Edge Devices in the Post-Quantum Internet of Things Using Lattice-Based Cryptography," *IEEE Communications Magazine*, vol. 56, pp. 158-162, 2018.
9. G. D. Addio, A. Smarra, A. Biancardi, M. Cesarelli, and P. Arpaia, "Quick-response coding system for tracking rehabilitation treatments in clinical setting," in *2017 IEEE International Workshop on Measurement and Networking (M&N)*, 2017, pp. 1-5.
10. T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on Human-Centered IoT-Connected Smart Labels for the Industry 4.0," *IEEE Access*, vol. 6, pp. 25939-25957, 2018.

11. A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Generation Computer Systems*, 2018.
12. R. Ferrero, E. Beattie, and J. Phoenix, "Sensor city- A global innovation hub for sensor technology," *IEEE Instrumentation & Measurement Magazine*, vol. 21, pp. 4-16, 2018.
13. Y. Xie and D. Bray, "A Digital Hub Solution for the Blind," in *2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT)*, 2013, pp. 257-260.
14. A. C. Marosi, R. Lovas, K. Á, and E. Simonyi, "A novel IoT platform for the era of connected cars," in *2018 IEEE International Conference on Future IoT Technologies (Future IoT)*, 2018, pp. 1-11.
15. S. Ahn, H. Oh, and J. K. Choi, "Hub-based Personal Web-Enabled Cross-Device Application," in *2017 IEEE 6th Global Conference on Consumer Electronics (GCCE)*, 2017, pp. 1-3.