Journal of Engg. Research Vol. 7 No. (3) September 2019 pp. 90-104

Data importance and feedback based adaptive level of authorization for the security of Internet of Things

Vivek V. Jog* and Dr. T. Senthil Murugan

**Department of Computer Science and Engineering, Don Bosco College of Engineering, Fatorda, Margao 403603, Goa, India.*
Department of Computer Engineering, Vel Tech Dr. RR and Dr. SR Technical University, Avadi, Chennai 600062, Tamil Nadu, India
**Corresponding Author: jog.vivek@gmail.com*

ABSTRACT

With the rapid development of Internet of Things (IoT), it becomes more widely used in various applications. Generally, the IoT is used to interconnect each computing device assisted by the unique identity of the Internet. Due to interconnections, the IoT constitutes intruder on the wireless communication channel, tampering with device, unauthorized access to the device, and privacy risks. To enhance the IoT security, the data importance and feedback based adaptive level of authorization is proposed in this paper. The proposed method comprises token initialization phase, request phase, and authorization phase. The request phase is done between the IoT device and IoT server. Then, the authorization between the devices is performed by the proposed method. The log file and feedback table are the major concern, which are stored in the authorization centre of the IoT system. These files consist of behaviour and performance among the IoT devices. Then, data importance is also included for the proposed authorization scheme based on the data size. Thus, the data importance and feedback based adaptive level of authorization is performed significantly. Finally, the simulation results of the proposed method are validated using DPWSim implementation. Then, the verification phase is analysed against the various security issues, and attack analysis is compared with that of the existing systems. Thus, the proposed adaptive level of authorization enhances the security level for the Internet of Things.

Keywords: -IoT device and server, Authorization, Log file, Feedback, Data importance.

INTRODUCTION

Recently, Internet of Things (IoT) becomes the novel paradigm, which is rapidly growing in the area of the wireless communications and networking. Everything in the IoT network is an essential one since each thing has the ability to locate, be addressable, and be readable, countermeasure on the Internet. The main purpose of IoT network is robust against the different attacks in the network (Khemissa & Tandjaoui, 2015). Thus, Internet of Things is defined as the evolution of Internet by integrating machines and people towards connecting the objects or things (Bekara, 2014). Examples of object are utilized in the IoT such as smart phones, power metres, heart beat monitors, and temperature metres and also sensors that are designed by the memory, processor, and storage (Mashal *et al.,* 2016). Thus, Internet of Things is employed to incorporate the cyber entities, physical perceptions, social attributes, and physical objects with the embedded intelligence (Cirani *et al.,* 2014).The IoT network consists of some typical devices such as Intelligent Transport System (ITS), remote-monitoring, smart cities and smart energy, and terminal nodes gathering information and transmitting it to the IoT platform via multi hop relay network. Subsequently, the acknowledgement is sent from the platform to the terminal nodes using the relay devices (Hu *et al.,* 2012).

Nowadays, the IoT is widely used in various applications like smart cards, intelligent transportation, and smart grid, but it cannot provide the security of the system and the information may also be dripped at any time. Thus, the security is considered as the major issue in the Internet of Things network (Jing *et al.,* 2014). The major security problem in IoT

is authentication and data integrity. Then, the authentication and authorization are the two significant countermeasures in the security paradigm, which are used to manage, control, and connect a device. The IoT network could not provide the enhanced security schemes due to low capacities in terms of both energy and computing resources (Khemissa & Tandjaoui, 2015). Security of the IoT comprises several tasks, which are as follows: i) entrench the key material while manufacturing process; ii) when operation process, the new keying material is required; iii) key is obscured by the hardware security models; iv) process and update secure software; and v) efficient cryptographic techniques (Keoh *et al.,* 2014).

The IoT security consists of three aspects, which are i) System security, ii) Network security, and iii) Application security. To provide the systemic security frameworks, security measures and guidelines, as well as system security concerns with the entire IoT system, have been taken to determine the security and privacy challenges. Network security is undergone by the key distribution algorithm, authentication protocols, and access control mechanisms. This security includes certain wireless communication networks such as wireless sensor networks, Internet, and Radio Frequency Identification (RFID) (Cirani *et al.,* 2014). In application security, it mitigates the practical problems using IoT applications like multimedia, smart home, and smart grid. Then, the security issue is caused by the information privacy, user authentication, track of data stream, information access, and destroy (Jing *et al.,* 2014).

The ultimate aim of this paper is to design the adaptive level of authorization based on feedback and data importance for the security of Internet of Things (IoT). The idea behind the proposed method is to perform the authorization among the IoT devices. Here, log file and feedback table are the major concern in the proposed protocol. The proposed methodology comprises request phase and authorization phase. Based on the data size, the data importance is also included to perform the adaptive level of authorization. The IoT device sends the request message along with its identity and private key. Then, the request message is forwarded to the IoT server. Once the request message is obtained, the server exploits the verification phase to perform the authorization between the IoT devices. Then, the behaviour of the IoT device and server is stored in the log file and also the performance among the IoT devices is stored in the feedback table. These two files are maintained by the authorization centre. Thus, the verification is undergone by the private key, log file, and feedback in the proposed security protocol. To perform authorization, the authority centre releases the channel key to the IoT server and devices. Finally, the feedback based adaptive level of authorization is performed significantly using the communication channel key.

The two main contributions of this paper are as follows:

- The adaptive level of authorization is proposed based on the data importance for the security of Internet of Things (IoT).
- The log file and feedback table are utilized for the proposed adaptive level of authorization, which is stored in the authorization centre.

This paper is structured as follows: Section 2 discusses the authorization scheme for the security of the Internet of Things. The problem statement and challenges behind the proposed model are described in section 3. Section 4 demonstrates the proposed methodology for the adaptive level of authorization based log file and feedback. The simulation results are evaluated and security performance is analysed in section 5. Finally, section 6 concludes this paper.

LITERATURE REVIEW

Ioannis Chatzigiannakis *et al.*(2014) presented an Elliptic Curve Cryptography (ECC) for the public key encryption. ECC was an ideal candidate, which was based on constrained devices. The major computational resources like speed and memory were limited and then low power communication protocols were employed. Due to these constraints, the same level of security was obtained. To resolve this problem, the smart parking application domain was presented in IoT network. It was then used to protect the privacy of the users by avoiding the exchange of confidential information. Thus, the performance was analysed in terms of execution time and network overhead, which enhanced the security

level but the utilization of ECC increases the size of the encrypted messages and also, it increases the likelihood of implementation issues.

Kun-Hee Han and Woo-Sik Bae (2015) proposed a hash function based IoT communication system for verifying a security protocol. In IoT technology, the attack leads to attain the system malfunction, remote control, and authorization. The mutual authentication and security were the important aspect of communication. This paper was used to design the secure communication protocol using hash locks, security key, passwords, and timestamps. Thus, the experimental results were validated using the Casper/FDR tool, which confirmed the high level security of the protocol in terms of deadlock, safety, and livelock. The design of security protocol was mainly concentrated based on the hashing function, which does not provide the flexibility in security layer.

Huansheng Ning *et al.*(2015) designed an aggregated-proof based hierarchical authentication scheme for the layered networks. Consequently, i) to determine the forward and backward anonymous data transmission, the aggregated proofs were established for multiple targets; ii) homomorphism functions, directed path descriptors, and Chebychev chaotic maps were combined for the mutual authentication; and iii) distinct access authorities were defined to achieve the hierarchical access control. Thus, the performance was analysed and it proved that the proposed APHA method had no security defects and robust for the U2IoT architecture and IoT applications but the key resilience issues were not effectively handled in the aggregated-proof based hierarchical authentication scheme.

Sye Loong Keoh *et al.* (2014) explained the Internet Engineering Task Force (IETF) to standardize security solutions for the IoT ecosystem. Initially, the standard security protocol was used in conjunction with the Constrained Application Protocol (CoAP). This paper discussed the latest standardization efforts and then improved the DTLS because the Datagram Transport Layer Security has been chosen as the channel security for CoAP. The proposed IETF consists of raw public key in DTLS, extending DTLS record layer to protect group communication, and profiling DTLS to mitigate the size and complexity. Thus, the proposed IETF proved to decrease the message fragmentation issue but the communication cost to transmit and receive the messages seems larger.

Jongseok Choi *et al.*(2015)presented a secure IoT framework to ensure the end-to-end security from IoT application to IoT devices. The proposed framework was comprised of IoT application, IoT broker, and the IoT devices. Thus, the IoT devices could be organized with boundary area or board line of IoT broker. The sensing data was collected by the IoT broker who managed their own devices. We were required to access the sensing data to use the IoT services. However, most of the IoT protocols had no concern about the end-to-end security since it depends only on the DTLS security. Finally, the proposed framework improves the efficiency of communication by encrypting and decrypting the data but the multiple level of security parameters and verification was not used optimally.

Thomas Kothmayr *et al.*(2014)described the fully implemented two-way authentication security scheme for the IoT based on existing Internet standards, especially the Datagram Transport Layer Security (DTLS) protocol. The proposed security scheme was developed for the Low power Wireless Personal Area Networks, which was based on the RSA public key cryptography algorithm. When compared to the existing implementations, the system architecture and scheme's feasibility were demonstrated through the hardware implementation of the Internet of Things. The two-way authentication developed in this paper failed to include the dynamic level of security layer, which reduces the time of authorization.

Javier Suarez *et al.*(2012) developed an Information-Centric Networking (ICN) to support the IoT management architecture. This architecture was designed with the naming, interoperation, security, and energy-efficient requirements. This paper provided the flexible architecture, which allowed the suitable operation of IoT devices based on the ICN network domain. Then, the communication overhead was introduced at both IoT device and IoT server by the security procedure. In addition to, this proposed ICN domain enhanced the potential of the architecture efficiently. Thus, the experimental results were validated using an Arduino board, which provided the feasibility of the solution. The main drawback of this architecture is that the feedback and data importance based trust reputation were not considered for end to end to communication.

Ting Hu *et al.*(2016) proposed a mutual authentication and key update for multi-hop relay in the Internet of Things. In the IoT network, the terminal node had limited computation abilities and information flow through the relay devices. But the relay device leads to the improvement of the algorithm complexity based on computation and communication costs. Thus, the modified elliptic mapping scheme was introduced in the authentication and key update mechanisms. Thus, the proposed update mechanism proved that the scheme was feasible, secure, and highly effective for the typical multi-hop relay networks. Even though this mutual authentication proved better security, the adaptive level of authorization scheme is missing.

MOTIVATION BEHIND THE APPROACH

Problem Statement

- The problem arises with the disparity in devices and access technology, which leads to generate the complex heterogeneity and does not address the Internet as a whole (Suarez, *et al.,* 2016).
- Because IoT components contain the low capacity in terms of energy and resources, the IoT cannot support the implementation of complex security schemes (Khemissa & Tandjaoui, 2015).
- In general, the IoT platform transmits the command to the terminal node by the relay channel. But the crucial problem is to evaluate the IoT security in this platform (Hu *et al.,* 2012). Thus, the major issue in the IoT system is to ensure the integrity and confidentiality of the data and privacy of the IoT devices (Chatzigiannakis *et al.,* 2016).

Challenges

- The IoT consists of potential vulnerabilities (Cirani *et al.,* 2014) due to complication in sensor, heterogeneous targets, and backend management systems.
- The authorization and end-to-end data protection are the major challenges in the Internet of things since some of the intruders access the communication channel, and the malicious node is presented while transmitting the data (Hummen *et al.,* 2014).
- The significant challenge (Moosavi *et al.,* 2015) is to utilize the security protocol because i) IoT nodes have limited power, memory, and communication bandwidth and, ii) because of the small size of IoT nodes and wireless communication, the nodes get lost easily.

PROPOSED METHODOLOGY: FEEDBACK BASED ADAPTIVE LEVEL OF AUTHORIZATION FOR THE SECURITY OF IOT

This section presents the proposed methodology of authorization phase based on data importance and feedback based adaptive level for the security of Internet of Things. Here, the authorization is considered as the major concern between IoT devices. Figure 1 shows the block diagram of proposed methodology. The authorization is adapted between the two devices based on the data importance. The proposed authorization scheme comprises two phases: a) Request phase and b) Authorization phase. IoT device 1, IoT device 2, IoT server, and authorization centre are the prerequisites for the proposed method. The proposed protocol consists of log file and feedback, which is used to store the behaviour of the device and server and also its performance. In the request phase, the IoT device sends the request message to the IoT server for authorization process. Then, the verification level is done through the private key, log file, and feedback. After verifying, the authorization centre provides the channel key to perform the authorization between the devices securely. Table 1 demonstrates the symbol description of the proposed method.

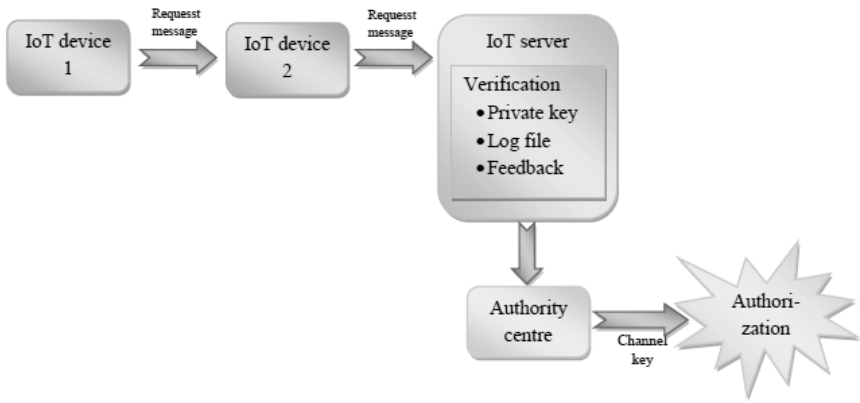

Fig. 1. Block diagram of proposed methodology.

Table 1. Symbol description of the proposed method.

Symbol	Description
AC	IoT authorization centre
II_y^1	Identity of IoT device 1
II_y^2	Identity of IoT device 2
IS_x	Identity of IoT server
$K_{IOT}^s(y)$	Secret key of IoT devices
$K_s^p(x)$	Private key of IoT server
K^p	Public key
K_c	Key of communication channel
$h(\cdot)$	Hash function
$h^*(\cdot)$	Computed hash at the IoT server
SD_R	Size of data requested to be shared
SD_A	Size of data allowed
REQ	Request message
RL	Reputation factor based on log file
RF	Reputation factor based on feedback
y_1, y_2, y_3	Intermediate messages
C	Counter for the level of authorization
T_1, T_2, T_3	Thresholds

a) Token initialization phase

The token initialization is the initial step in the adaptive level of authorization. Whenever the IoT device wants to communicate with other IoT devices, it should obtain the token from the server. So, the request message will be sent by the IoT device to the server by requesting the token for communication. The server releases a onetime token to the IoT device through the private channel. This token should be then transmitted to the other IoT devices who want to do communication. This token will be verified by both devices before proceeding to the request phase.

b) Request phase

The request phase is the next step for the adaptive level of authorization scheme. Generally, the device sends the request message to the server along with its identity and private key. The private key should be encrypted for security purpose. Here, the request message is transmitted firstly between IoT devices and then between the device and IoT server. Figure 2 shows the schematic representation of request phase.

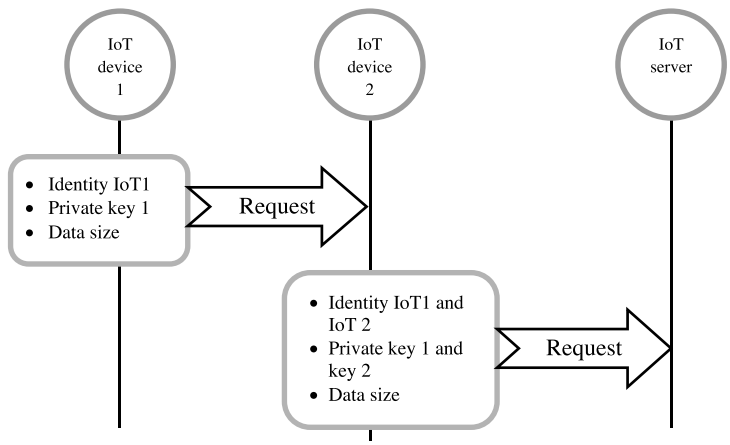

Fig. 2. Schematic representation of the request phase.

i) Request between two IoT devices

Every IoT device contains its identity and secret key to perform the authorization phase. The identity of IoT device 1 is represented by and denotes a private key. The request message consists of device identity, key, request, and shared data size. It is represented by

$$D_1 = \left\{ II_y^1, h_1\left(K_{IOT_1}^s(y)\right), SD_R, REQ \right\}$$

where II_y^1 is the identity of the IoT device 1, $h_1\left(K_{IOT_1}^s(y)\right)$ represents the hash function of IoT device private key since the key should be known to its corresponding device, and *REQ* is the request message. The size of data to be shared between the devices is expressed by SD_R

ii) Request between device and server

After receiving the request from IoT device 1, the IoT device 2 forwards the message along with its identity and private key. Thus, the request message is sent to the IoT server. Thus, the IoT server determines the authorization step using the verification phase. It is expressed as

$$D_2 = \left\{ D_1, II_y^2, h_2\left(K_{IOT_2}^s(y)\right) \right\}$$

where II_y^2 is the identity of IoT device 2 and $h_2\left(K_{IOT_2}^s(y)\right)$ denotes the encrypted secret key. Thus, the request message is received at the IoT server side. Then, the server verifies whether it is a legitimate device or not based on the certain condition.

c) Authorization phase

Normally, the authorization is performed between the two devices to transmit the data. The proposed protocol is designed to the adaptive level of authorization based on the data importance. Once the server receives the request message, the allowed data size is computed by the shared data size, which is sent from IoT device 1. Based on the data importance, the authorization is adapted between the devices. The behaviour of IoT devices and server is stored as the log file in the authorization centre. The feedback of every session is stored in the authority centre. Based on the log file, feedback, and private key verification, the proposed protocol performs the adaptive level of authorization between the devices. If it verifies correctly in each subsequent step, then the IoT server releases the communication channel key to the devices. Then, the data is transmitted significantly between the devices. Thus, the allowed data size is formulated as follows:

$$SD_A = f\left(SD_R\right)$$

where

$$f\left(SD_R\right) = \begin{cases} 1, & if \quad R < 0.25 \\ 2, & if \quad 0.25 \le R \le 0.5 \\ 3, & if \quad 0.5 \le R \le 0.75 \\ 4, & if \quad R > 0.75 \end{cases}$$

where R is a factor, which is computed as

$$R = X_{\min} + \left(X_{\max} - X_{\min}\right) * \left(\frac{SD_R}{T_3}\right)$$

where $X_{\min}$ and $X_{\max}$ are the minimum and maximum values of the data and T_3 is the threshold value, which ranges from zero to one. Thus, the computed R value is varied from zero to one by the aforementioned condition. Figure 3 depicts the diagrammatic representation of the authorization phase.

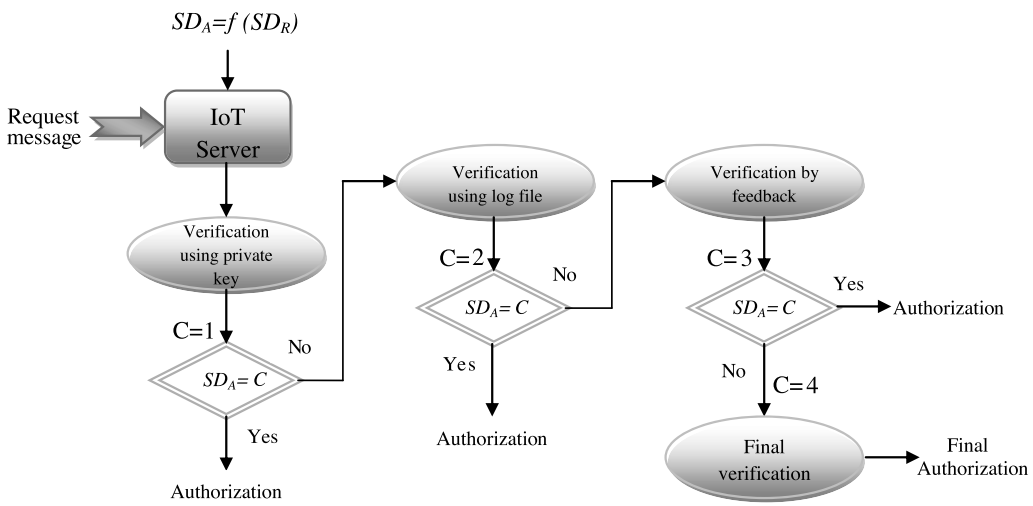

Fig. 3. Diagrammatic representation of authorization phase.

Step 1: *Verification by secret key:*

The data size is determined by the obtained shared data size from the IoT device. In general, the IoT server should be aware of the private key of the two IoT devices. In the verification step 1, the hash function is applied to the secret key in the IoT server. Thus, the hashed private key is represented as $h^*\left(K^s_{IOT_2}(y)\right)$ and $h^{**}\left(K^s_{IOT_2}(y)\right)$.

i) Then, the IoT server verifies the computed hashed key and obtained hashed key from the device. If they are similar, the IoT server provides the counter level for authorization, which is one. It is defined as

$$C = 1 \quad when \quad h_1 = h^*, h_2 = h^{**}$$

where C is the counter for the authorization level.

ii) Consequently, the data size SD_A is also determined based on the R factor. Finally, if the acquired data size is equal to the counter level, then the IoT server releases the communication channel key to IoT device 2 and device 1.

$$A = \begin{cases} K_c, & SD_A = C \\ nextcounter, & otherwise \end{cases}$$

where A is the authorization process and K_c defines the communication channel key. This key is evaluated at the IoT server since the identity of two IoT devices and server is known. Thus, the K_c is defined by

$$K_c = h\left(IS_x \| SD_R \| II^1_y \| II^2_y \right)$$

where IS_x is the identity of IoT server. The key channel is acquired by the hash function of identity and data size for the security purpose. Thus, the channel key is sent to both devices. The device utilizes the channel key, which is comprised of identity of device, server, and shared data size. Finally, the data is transmitted between IoT device 1 and device 2.

Step 2: *Verification using log file*

The IoT server verifies the device for the authorization scheme with the aid of reputation factor based on log file. The proposed method exploits the log file to gather the performance of the IoT device and server. This log file is stored in the authority centre to perform the authorization between the devices, respectively. Thus, the reputation factor based log file is determined as

$$R_{(\log)} = \frac{1}{nTx * nRx} \sum_{i=1}^{nTx} \sum_{j=1}^{nRx} \left(\frac{SD^{ij}_R}{T_3} \right) * p_{ij}$$

where nTx and nRx are the numbers of transmitter and receiver, T_3 is the threshold value, and p determines whether the performance is success or failure.

i) Then, the IoT server utilizes the public key, private key of two IoT devices, and identity of the server. Thus, z_1 and z_2 are the keys, which are computed from the IoT server. They are expressed as

$$z_1 = K^p * K^s_{IOT_2}(y) * IS_x$$

$$z_2 = K^p * K^s_{IOT_1}(y) * IS_x$$

where K^p is the public key, which is known to IoT device and server. These two values are used to compute the intermediate message for the two IoT devices. Also, the XOR operation is utilized for generate the intermediate message and hash function is also used to obscure the key. It is formulated by

$$y_1 = h(z_1) \oplus RL_1$$

$$y_2 = h(z_2) \oplus RL_2$$

where y_1 and y_2 are the intermediate messages and RL is the reputation factor based on log file. The IoT server sends the message y1 to the IoT device 2. Similarly, the message y_2 is sent from the server to the IoT device 1.

ii) After receiving the intermediate message, the IoT device computes the reputation factor using the intermediate message and key z_1 which sends further to the IoT server. Subsequently, the reputation factor for device 1 is determined by the intermediate message y_2 and hashed key z_2. Thus, the reputation factor for the two IoT devices is defined as

$$RL_1 = y_1 \oplus h^*(z_1)$$

$$RL_2 = y_2 \oplus h^*(z_2)$$

where RL_1 is the reputation factor for the device 2 and RL_2 represents the reputation for IoT device 1. These are the two values, which are obtained at the IoT server and then the server itself calculates the reputation factor using $R_{(\log)}$ equation. Then, the server verifies the reputation value based on the log file. If the obtained and estimated values are equal, then the server yields the second counter level for authorization. The estimated reputation at the IoT server is denoted as RL_1^* and RL_2^*.

$$C = 2, \quad when \quad RL_1^* = RL_1, RL_2^* = RL_2$$

iii) Then, the counter level is ensured with the data size SD_A at the IoT server. If both the values are equal, then the server gives the communication key channel K_c to IoT devices. Then, the authorization is performed significantly between the two IoT devices. Otherwise, the verification phase is undergone further using the reputation factor based on feedback.

Step 3: Verification by feedback

The feedback mechanism in the proposed method is used to store the performance among the devices and server. This feedback also stores in the authorization centre. The feedback file includes each session of the transmitter and receiver between the devices. Usually, the feedback value to be given by every other IoT devices is varied between 0 and1. Here, the IoT server determines the authorized device using the reputation factor based feedback. The threshold value is also employed in the verification process to enhance the security level. Thus, the reputation factor based feedback is calculated by

$$R_{(fb)} = \frac{1}{nTx * nRx} \sum_{i=1}^{nTx} \sum_{j=1}^{nRx} \left(\frac{SD_R^{ij}}{T_3} \right) * f_{ij}$$

where i and j are the numbers of transmitter and receiver in the device and f is the feedback of the IoT device. Then, the IoT server considers the two threshold values, which are then used to compare with the reputation factor. Using the aforementioned equation, the server computes the two reputation values for IoT device 1 and device 2. Thus, the value is defined as RF_1 and RF_2. The third counter level for authorization is obtained by comparing the reputation and threshold value. It is represented as

$$C = 3, \quad if \begin{cases} RF_1 > T_1 \\ RF_2 > T_2 \end{cases}$$

Once the counter for authorization level is attained, it is compared with the data size. If both values are equal, the IoT server releases the channel key K_c to both devices. Thus, the device exploits the key for the authorization between the devices.

Step 4: Final verification

The final verification is done using the private key of two IoT devices and IoT server. The intermediate message is generated in the IoT server using hash function. The intermediate message y_3 is evaluated by

$$y_3 = h\left(K^{s}_{IOT_1}(y)\right) \| h\left(K^{s}_{IOT_1}(y)\right) \| h\left(K^{p}_{s}(x)\right)$$

where $K^{p}_{s}(x)$ is the private key of the server. The message y_3 is transmitted from the IoT server to the authorization centre. Since the authorization centre knows the private key of two IoT devices and IoT server, it verifies the obtained message. Similarly, the message is generated at the authorization centre itself. Thus, the intermediate message y^{*}_{3} is attained. If both are equal, then the authorization centre offers the communication channel key to the IoT server and two IoT devices. It is represented as

$$A = K_c, \quad when \quad y_3 = y^{*}_{3}$$

Thus, the proposed adaptive level of authorization is performed securely based on the log file, feedback, and data importance for the Internet of Things (IoT).

c) Description of log file and feedback table

The proposed method exploits the log file table, which is stored in the authorization centre. The log file consists of the behaviour of the IoT device and sender. The behaviour is characterised by the authorization between the two devices either success or failure. Table 2 demonstrates the structure of the log file. The data size is 200MB, which is requested to send from the IoT sender device to the IoT receiver device. Thus, the proposed authorization method is employed to determine whether it successfully transmits the data or not. The value one represents the success transmission between the two IoT devices. Simultaneously, the value zero denotes the failure transmission of the data. Similarly, the behaviour of the devices is stored in the log file table for every time of transmission. Finally, this log file is maintained by the IoT authorization centre.

Table 2. Structure of Log file.

Time	IoT device (Sender)	IoT device (Receiver)	SD_R	Success/failure
t=1	II^{1}_{y}=2	II^{2}_{y}=3	200MB	1

Consequently, the feedback of every session of IoT devices is also stored in the authorization centre. The feedback value is computed based on the legitimate devices. Here also, the data should be transmitted between the IoT devices. Thus, the performance among the devices is stored as the feedback value in the authority centre. Table 3 represents the structure of the feedback table. When the identity of the IoT device is five and six and then the data size is 300MB, the feedback of this transmission is zero. Here, the feedback value ranges between zero and one based on the reputation guessed by the receiver. Thus, we infer from the feedback table that the IoT device is not an authorized one. Similarly, the feedback of all IoT devices is stored in the AC. Thus, the log file and feedback table are further used for the verification phase.

Table 3. Structure of feedback table.

Time	IoT device (Sender)	IoT device (Receiver)	SD_R	Feedback
t=1	II^{1}_{y}=5	II^{2}_{y}=6	300MB	0

SIMULATION RESULTS

This section described the simulation results of the proposed system using DPWSim (Han *et al.,* 2015) simulation tool and the attack performance is analysed against the password guessing attack, impersonation attack, server spoofing attack, stolen verifier attack, reply attack, reconnaissance attack, and theft attack.

Security measures

i) Data confidentiality: Since the systems are employed to manage the information, data confidentiality is the measure of ability of the system to obscure the data. Here, the data confidentiality is measured between the IoT devices and IoT server. Normally, the server includes the private key and identity of the devices. After receiving the message from the IoT device, it should ensure whether the device is authorized or not. Finally, the server verifies the private key and identity with the obtained message.

ii) Data integrity: The hash function is used to enhance the data integrity while transmitting the key through the channel. In the proposed method, the hash function is applied to the private keys of the IoT device and server. The data is transmitted between the devices in terms of hashed value for identity verification. Thus, the hashed key is send from the IoT device to server to prevent the access of key by the eavesdropper.

iii) Multi-level authentication: The proposed method verifies the identity of the IoT device through the verification phase. Thus, the multilevel of verification ensured that the security of the proposed protocol provides the enhanced and robust security against the security attacks.

iv) Mutual authentication: The mutual authentication in the proposed protocol is performed by the identity of the IoT device II_y and server identity IS_x. Thus, the proposed protocol proves their identity for the authentication mechanism.

v) Feedback based adaptive level authorization: The proposed method performs the adaptive level of authorization. The authorization is done through the data importance, log file, and feedback. The adaptive level is determined by the data size and the counter level. Thus, the proposed protocol verifies the IoT devices with the aid of log file and feedback. After verifying the identity of the device, the server provides the communication channel key to perform the authorization.

Attack analysis

a) Password guessing attack: This attack tries to access the device by the password. The two password attacks are brute force attack and dictionary attack. In the proposed protocol, the private key of the two devices is encrypted in terms of hash function. The secret key is known at its corresponding device and server. Thus, the attacker identifies the key by all possible combinations. Thus, the proposed method is burdensome to the password guessing attack.

b) Impersonation attack: The adversary is intended to achieve the private key and identity of the legitimate users. But in the proposed authorization scheme, the private key of two IoT devices is secured by the hash function. The hashed private key is difficult to retrieve by the imposter. Thus, the proposed method ensures robust against the impersonation attack.

c) Server spoofing attack: The IoT server receives the request message from the IoT device in the proposed authorization method. However, the server itself estimates the hashed value of two private keys. Then, the IoT server verifies the estimated hash with the obtained hash value. After verifying the identity of the device, the server must send the communication channel key to perform the authorization. Thus, the server spoofing attack is mitigated by the proposed authorization phase.

d) Stolen verifier attack: This attack leads to steal the verification data by the intruder from the IoT server. Normally, the verification data does not have encrypted information or use XOR operation. But our proposed protocol ensures the hash function, which is used to secure the data at the verification phase. Thus, the adaptive level of authorization is secured against the stolen verifier attack.

e) Reply attack: It is a form of network attack in which the valid data is repeated fraudulently or maliciously. The adaptive level of authorization sends the request in terms of hashed value to the server. Then, the server verifies the data and transmits the relevant response to the IoT device. Subsequently, the adversary cannot estimate the data while transmitting over the channel. Thus, the proposed protocol achieves the high security against the replay attack.

f) Reconnaissance attack: This attack gathers as much information about the system, as server location, IP address range, software version, etc. But the log file plays a vital role in the proposed authorization level. The authorization behaviour between the IoT devices and IoT server is stored in the log file. The authorization centre includes all the information about the device, server, and log file also. The log file contains the value as zero and one, in which zero represents the failure authorization and one is the successful authorization. If the attacker uses the information to transfer the data to the system, then the server examines the identity of the device in the log file whether it belongs to success or failure. Thus, the high level of security is attained against the reconnaissance attack by the proposed method.

g) Theft attack: This attack is intended to steal the secret data from the IoT server. The server poses both the verification data and the secret key. Then, the imposter exploits the stolen information to send the data to the server. But in the proposed authorization scheme, the feedback table is utilized. The performance among the IoT devices is stored in the feedback table, which is maintained by the authorization centre. The imposter should not be aware of the feedback table in the IoT system. If an imposter sends the data from the existing device, then the server verifies with the feedback table of the AC. Then, the IoT server finally declares it as the illegitimate user. Thus, the proposed feedback based adaptive level of authorization proves to enhance the IoT security level.

Comparative analysis

This section presents the comparative analysis based on the various security issues. Then, the analysis is compared with the existing three protocols and the proposed protocol. The first protocol is the aggregated-proof based authentication scheme (Ning *et al.,* 2015) for the IoT system. Then, the second protocol is the (Odelu *et al.,* 2015) multi level authentication scheme by the hashing function. The previous work describes the threat profiling and elliptic curve cryptography based multi level authentication. Thus, the existing and proposed protocol performance is compared with security issues like stolen verifier attack, man-in-the-middle attack, impersonation attack, replay attack, server spoofing attack, denial of service attack, reconnaissance attack, and theft attack. Thus, the proposed adaptive level of authorization is performed efficiently when compared to the existing system, which is demonstrated in table 4.

Table 4. Comparative analysis for the proposed authorization scheme.

Security Issues	Huansheng Ning *et al.'s* scheme (2015)	Existing (Odelu, *et al.,* 2015)	Previous work	Proposed
Provides mutual authentication	Yes	Yes	Yes	Yes
Provides multi-level authentication	Yes	Yes	Yes	Yes
Requires identity-verification table	Yes	Yes	Yes	Yes
Server spoofing attack resistance	Yes	Yes	Yes	Yes
Stolen verifier attack resistance	No	Yes	Yes	Yes
Privileged insider attack resistance	Yes	Yes	Yes	Yes

Password guessing attack resistance	Yes	Yes	Yes	Yes
Provides strong user anonymity	Yes	Yes	Yes	Yes
Known session-specific temporary information attack resistance	No	Yes	Yes	Yes
Impersonation attack resistance	Yes	Yes	Yes	Yes
Reply attack resistance	Yes	Yes	Yes	Yes
Man-in-the-middle attack resistance	Yes	Yes	Yes	Yes
Provision for revocation and re-registration	Yes	Yes	Yes	Yes
Free from denial of service attack	No	Yes	Yes	Yes
Profile table-stolen resistance	No	No	Yes	Yes
Key resilience	No	No	Yes	Yes
Reconnaissance attack resistance	No	No	No	Yes
Free from theft attack	No	No	No	Yes

CONCLUSION

In this paper, the data importance and feedback based adaptive level of authorization we reproposed for the security of Internet of Things (IoT). Here, the proposed method was employed to perform the authorization securely between the devices. The proposed protocol was comprised of two IoT devices, IoT server, and authorization centre. Initially, the request phase was undergone between the IoT devices and IoT server. Once the server acquired the request message, the authorization was performed by the data size. Thus, the data importance was employed to determine the counter level for the authorization. Furthermore, the log file and feedback table were utilized to the proposed authorization scheme. The value of log file represented the behaviour between the IoT devices and server. Then, the performance of the IoT devices was stored in the feedback table. Based on the log file and feedback, the server verified the identity and reputation factor for the proposed method. After verifying, the authority centre provided the channel key to transmit the data between the two devices. Finally, the simulation results were evaluated using DPWS simulation, and the comparative performance was analysed with the existing system. Thus, our proposed protocol improved the security level against various attacks.

REFERENCES

Bekara, C. (2014). Security Issues and Challenges for the IoT-based Smart Grid, *Procedia Computer Science*, 34:532-537.

Chatzigiannakis, I., Vitalettia, A. & Pyrgelisc, A. 2016. A Privacy-Preserving Smart Parking System based on an IoT Elliptic Curve Based Security Platform, *Computer communications,* 90: 165-177.

Choi, J., In, Y., Park, C., Seok, S., Seo, H. & Kim, H. 2016. Secure IoT framework and 2D architecture for End-To-End security, *The Journal of Supercomputing*,1-15.

Cirani, S., Picone, M., Gonizzi, P., Veltri, L. & Ferrari, G. 2014. IoT-OAS: An OAuth-Based Authorization Service Architecture

for Secure Services in IoT Scenarios, *IEEE Sensors Journal*, 15 (2): 1224-1234.

Han, S.N., Lee, G.M., Crespi, N., Luong, N.V., Heo, K., Brut, M. & Gatellier, P. 2015. DPWSim: A Devices Profile for Web Services (DPWS) Simulator, *IEEE internet of things journal,* 2 (3): 221-229.

Han, K.H. & Bae, W.S. 2016. Proposing and verifying a security protocol for hash function-based IoT communication system, *Cluster Computing*, 19(1): 497-504.

Hu, T., Wang, J., Zhao, G. & Long, X. 2012. An Improved Mutual Authentication and Key Update Scheme for Multi-Hop Relay in Internet of Things, *In proceedings of IEEE Conference on Industrial Electronics and Applications*,1024-1029.

Hummen, R., Shafagh, H., Razaz, S &Voigt, T. 2014. Delegation-based Authentication and Authorization for the IP-based Internet of Things, In proceedings of IEEE International Conference on Sensing, *Communication, and Networking*,284-292.

Jing, Q., Vasilakos, A.V. & Wan, J. 2014. Security of the Internet of Things: perspectives and challenges, *Wireless Networks,* 20 (8): 2481-2501.

Keoh, S.L., Kumar, S.S. & Tschofenig, H. 2014. Securing the Internet of Things: A Standardization Perspective, *IEEE Internet of Things Journal,* 1 (3): 265-274.

Khemissa, H. & Tandjaoui, D. 2015. A Lightweight Authentication Scheme for E-health applications in the context of Internet of Things, *In proceedings of IEEE International Conference on Next Generation Mobile Applications, Services and Technologies*,90-95.

Kothmayr, T., Schmitt, C., Hub, W., Brünig, M. & Carle, G. 2013. DTLS based security and two-way authentication for the Internet of Things, *Ad Hoc Networks,* 11, (8): 2710-2723.

Leo, M., Battisti, F., Carli, M. & Neri, A. 2014. A federated architecture approach for Internet of Things security, *in proceedings of Euro Med Telco Conference (EMTC),*1 – 5.

Mashal, I., Alsaryrah, O. & Chung, T.Y. 2016. Testing and evaluating recommendation algorithms in internet of things, *Journal of Ambient Intelligence and Humanized Computing,*1-12.

Moosavi, S.R., Gia, T.N. & Rahmani, A.M. 2015. SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways, *Procedia Computer Science,* 52:452-459.

Ning, H., Liu, H & Yang, L.T. 2015. Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things, *IEEE transactions on parallel and distributed systems,* 26 (3): 657-667.

Odelu, V., Das, A.K. & Goswami, A. 2015. A Secure Biometrics-Based Multi-Server Authentication Protocol using Smart Cards, *IEEE transactions on information forensics and security,* 10 (9): 1953 – 1966.

Sicari, S., Cappiello, C., Pellegrini, F.D., Miorandi, D. & Porisini, A.C. 2016. A security-and quality-aware system architecture for Internet of Things, *Information Systems Frontiers*, 18 (4): 665-677.

Suarez, J., Quevedo, J., Vidal, I. & Corujo, D. 2016. A secure IoT management architecture based on Information-Centric Networking, *Journal of Network and Computer Applications,* 63: 190-204.

Wang, X., Sun, X., Yang, H. & Shah, S.A. 2011. An anonymity and authentication mechanism for internet of things, *Journal of Convergence Information Technology*, 6(3): 98–105.

Wu, F., Xu, L., Kumari, S. & Li, X. 2016. A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security, *Journal of Ambient Intelligence and Humanized Computing1*-16.

Zhao, G., Si, X., Wang, J., Long, X & Hu, T. 2011. A Novel Mutual Authentication Scheme for Internet of Things, *In proceedings of IEEE International Conference on Modelling, Identification and Control (ICMIC),*563-566.

Submitted: 29/08/2017
Revised: 28/11/2017
Accepted: 09/01/2018

مستوى الترخيص التكيفي لأمن انترنت الأشياء (IoT) المرتكز على أهمية البيانات واسترجاع المعلومات

***فيفك جوغ وسينثيل مورغن**

*قسم هندسة الحاسوب، تخصص الشبكات، كلية سمت كاشيباي نافال للهندسة، فاتوردا، مارغاو 403603، غوا، الهند

قسم هندسة الحاسوب، تخصص الشبكات، جامعة فيل تك التقنية، تشيناي، تاميل نادو

الخلاصة

يُستخدم انترنت الأشياء على نطاق واسع في تطبيقات IoT المختلفة بسبب تطوره السريع. وبشكل عام، يتم استخدام انترنت الأشياء لربط كل جهاز حوسبة بالهوية المميزة له في الانترنت. ونظراً للوصلات البينية بين الوحدات، يُعتبر IoT دخيلاً على قنوات الاتصال اللاسلكي، يعبث بالجهاز، ويسمح بالدخول غير المصرح به إلى الجهاز ومخاطر الخصوصية. ولتعزيز أمان IoT، تم عرض مستوى الترخيص التكيفي المرتكز على أهمية البيانات واسترجاع المعلومات. تتألف الطريقة المقترحة من مرحلة التهيئة الرمزية ومرحلة الطلب ومرحلة الترخيص. تتم مرحلة الطلب بين جهاز وخادم انترنت الأشياء. ومن ثم، يتم تنفيذ الترخيص بين الأجهزة بالطريقة المقترحة. يعتبر ملف السجل وجدول استرجاع المعلومات الشاغل الرئيسي الذي يتم تخزينه في مركز الترخيص لنظام IoT. ويتضمن هذا الملف السلوك والأداء بين أجهزة انترنت الأشياء. وبعد ذلك، يتم إدراج أهمية البيانات لمخطط التفويض المقترح استناداً على حجم البيانات. وبالتالي، يتم تنفيذ مستوى الترخيص التكيفي المرتكز على أهمية البيانات واسترجاع المعلومات بشكل ملحوظ. وأخيراً، يتم التحقق من نتائج محاكاة الطريقة المُقترحة باستخدام تطبيق DPWSim. وبعد ذلك، تم تحليل مرحلة التحقق مقابل مختلف مشكلات الأمان وتم مقارنة تحليل الهجوم بالأنظمة الحالية. وبالتالي، فإن مستوى الترخيص التكيفي المُقترح يعزز مستوى الأمان لإنترنت الأشياء.