2015 Third International Conference on Artificial Intelligence, Modelling and Simulation

SECURING DATA IN INTERNET OF THINGS (IOT) USING CRYPTOGRAPHY AND STENOGRAPHY TECHNIQUES

ELANCHELIAN V
Dept. of Computer Science & Engineering
Dr.M.G.R Educational and Research Institute
Chennai, India
elanchelian1044@gmail.com

MADHIVENDHAN M
Dept. of Computer Science & Engineering
Dr.M.G.R Educational and Research Institute
Chennai, India
madhii5812@gmail.com

MADHAN B
Dept. of Computer Science & Engineering
Dr.M.G.R Educational and Research Institute
Chennai, India
madhan1602gmail.com

Done under the guidance of **"Dr.SARAVANAN ELUMALAI (Professor, Dept. of Computer Science & Engineering) Dr.M.G.R Educational and Research Institute, Chennai, India"**

***Abstract* - Internet of Things (IoT) is a common thing (object) in today's world, which serves as part of our routine life activities. Although it benefits the residential district in several ways, various challenges such as data confidentiality and privacy are created. As a matter of fact, the community is concerned what information may leak out via IoT. Therefore, the needs of a secure environment is vital in order to secure the transmitting data from it devices over the network. As a result, in this paper, a secure scheme is suggested on using image steganography as an alternative security mechanism in conjunction with a home server to secure the transmitted data from IP camera as the IoT device to the other devices, either in LAN or WAN networks.**

Keywords- Internet of things; Image steganography; Information disclosure;

I. INTRODUCTION

Internet of Things (IoT) is among the emerging technologies that would be the greatest agents to change the modern world. It involves machine-to-machine communications with mobile, virtual and instantaneous connections. Not just typical computing devices, IoT system consists of household devices and many other data-gathering sensors. With IoT, people may control their household appliance with just a few touch on their smart devices. In addition, Cisco's Internet Business Solutions Group had predicted the amount of IoT devices to be double (50 billion devices) by 2020 [1]. The convenience and "smartness" of IoT devices helps in the growth of number of these devices. However, some people may still be afraid to have these devices in their homes. Although IoT devices may make people's life a whole lot easier, security experts had mentioned their concerns on the potential security problems (The Insecurity of Things), which make the IoT devices among top five security threats in 2015 [2].

As a matter of fact, information disclosure is the main security problems in IoT system that must not be neglected [3]. Moreover, IoT devices with weak security level and processing power, such as IP cameras, smart TV and other home appliances, which have the lack of confidentiality features can be the main targets for hackers. Therefore, with heterogeneous structure and its characteristic of distributed over the Internet, active and passive attacks could be made easier in the IoT system in order to steal private information or threaten human assets compared to other networks that contain only powerful computing devices. For example, the attackers have a greater chance to intercept and intercede on going data transmission between IoT devices as it requires a wide distribution of networks to connect them together, which usually involves the Internet. The information that the hackers might be interested are related to authentication, payment or even organizational secrets. By acquiring authentication information through eavesdropping or intercepting with a connection, the attacker can access or have control of certain IoT devices by using the retrieved information for further exploitations [4].

To solve the problem of confidentiality in the IoT network, we propose a security scheme that involves connections to the Internet. Since the IP camera is considered as the IoT device in

978-1-4673-8675-3/15 $31.00 © 2015 IEEE
DOI 10.1109/AIMS.2015.56

this study, transmitting the sensitive information between IP cameras and home server is relied on using image steganography within the LAN, while data transmission between a home server and the other devices out of the LAN (Internet) will be encrypted. This can provide more security on the transmitted sensitive data such as image of user face in the LAN network since the existence of sensitive information can be hidden using image steganography. Therefore, the attackers have less suspicious of the transmitted data in order to eavesdrop them (sniffing).

The remainder of the paper is structured as follows. In section II, several related works on how the information disclosure in IoT devices can be resolved. Section III illustrates the proposed scheme. In the end, a discussion and conclusion are drawn in section IV.

II. RELATED WORKS

In order to resolve the information disclosure among the IoT devices, several techniques have been suggested. The cryptography technique contains a pair of algorithms, which converts plaintext (secret messages) into ciphertext (encryption) in the sender side and converts it back to plaintext (decryption) in the recipient side [5]. Neverthless, due to the constraint of conventional cryptography in IoT devices, which demands more processing and memory, lightweight cryptography is used [6]. Lightweight cryptography is a method that specialized in constrained environments such as RFID tags, sensors, contactless smart cars and healthcare devices. In software implementation, lightweight applications are preferred with smaller code and RAM size, which does not always exploit the security-efficiency trade-offs. In addition, lightweight cryptography needs to adopt in IoT because it has a high efficiency of end-to-end communication and applications to low resource devices. The challenges that faced by lightweight cryptography is a degree of security, due to decreasing the encryption rounds as well as key length [7].

In general, the lightweight cryptography algorithms are divided into symmetric and asymmetric categories. In symmetric encryption, both parties need to hold a shared key and the key will be used for encryption and decryption. Some examples of symmetric encryption are XOR, AES, CS (compressive sensing)-based, Tiny Encryption Algorithm (TEA), Scalable Encryption Algorithm (SEA), PRESENT, HIGHT and SM1 / SM3 in security system. A lightweight cryptography protocol based on XOR operation is proposed to prevent data transmission eavesdropping in RFID tags and readers [8]. This technique is able to protect data transmission from any passive attack. Besides that, the researchers proposed a design for encryption node in IoT devices based on fingerprint features and CC2530 [9] which is a true system-onchip (SoC) micro controller for IEEE 802.15.4, developed by Texas Instruments [10]. The micro controller allows data encryption and decryption using AES algorithm. However, user's fingerprint feature information detection may have error with any physical changed, such as dry, injured or dirty skin. In addition, it is proposed that using channel measurements, more particularly, utilizes Received-Signal-Strength-Indicator (RSSI), to perform key extraction, and thus, any key distribution mechanism is not necessary [11]. The authors also suggested to use the keys from encryption/decryption in compressed sensing theory to allow encryption and compression to be done simultaneously with CS-based encryption. With CS (compressive sensing), it allows lightweight and compression to be performed simultaneously with high energy-efficiency. But, the drawback of this method is that if there is any interference or malicious changes in the properties of the wireless channel, the reconstruction error would be high as the keys will not be similar. Besides that, if the eavesdropper is located at a very close (within half a frequency wavelength) of the carrier, he would be able to get a key that is similar to the sender and recipient.

On the other hands, Asymmetric encryption uses a key pair, consists of a public key known by anyone that is a potential sender and private key only known by the receiver himself. The public key is used by the sender to encrypt a message, while a matching private key is required for decryption. In fact, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Elliptic Curve Cryptosystem (ECC) are two examples of asymmetric encryption. In CP-ABE, encryptor is able to intelligently decide the entities that allowed access to the data and the ones not. The authors proposed a new technique to further improve CP-ABE is Cooperative Ciphertext-Policy Attribute-Based Encryption (C-CP-ABE) [12]. The nature of IoT allows resource-constrained devices to delegate costly exponentiation computation to other trusted neighbor devices which is known as "assistant nodes" [12]. The researchers had successfully implemented of ECC into RFID authentication and TinyPK [13]. TinyPK is a security scheme for authentication and key exchange based on the RSA cryptosystem [14]. The RSA in TinyPK is replaced with ECC which provides better security performance and efficiency.

Additionally, since the communication between IoT devices can be wireless, Computational intelligence (CI) is introduced to create Wireless Intrusion Detection System (WIDS) that is more flexible, robustness, higher computation speed and good adaptively in changing environments [15]. It also improves tolerance for imprecision, uncertainty and approximation while having low overhead, improved latency and the ability to learn preferences. The purpose of creating CI is to replace weak cryptography.

In a case that the Wireless Sensor Network (WSN) is embedded into IoT devices in order to collect adjacent devices, which leads to improve the performance of the IoT devices within the network, self-jamming can be used as a security mechanism to protect data from disclosure. In fact, selfjamming is a technique which receiver stops the passive attack by purposely jamming incoming and corrupting the messages, which is collected by eavesdropper [16]. This can be made out by putting in noise during data transmission. In addition, since the recipient is the source of introducing noise, he can distinguish the original message and the noise to extract the message. Moreover, it is shown that the receiver needs to maintain a low increase in received power of 3dB, otherwise it would not work properly. It was also mentioned that if the sender's signal arrives 20dB from eavesdropper's receiver

sensitivity, the framework would not be efficient even if the receiver maintains the low increase.

III. PROPOSED SCHEME

In the real word scenario, the IP camera provides this capability to authenticate user face to unlock doors (e.g. server room door, house front door). In this case, the IP camera can obtain face images of the users and send them to server for authentication purpose or the other devices outside the LAN network (e.g. cloud storage) for storage as shown in figure 1. Any eavesdropping attack, especially in the LAN network violates the confidentiality of information being transmitted. For example, the attained face image is considered as sensitive information in figure 1 and any hacker that can successfully obtain it through eavesdropping attack can be able to authenticate himself with the authentication server [17].

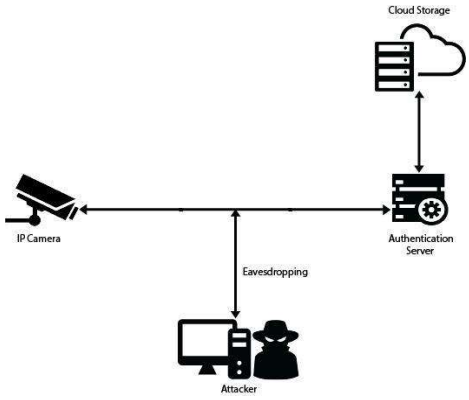

Fig .1. Real scheme

Figure 2 illustrates the proposed scheme in order to secure the transmitted images as sensitive data using IoT device. In this case, image steganography is used in order to secure sensitive information such as user face image, which is sent from IP camera (IoT device) in the LAN network. In addition, a home server can be used as a centralized device within the LAN network to receive the face image, which are already hidden using image steganography to encrypt them in order them to the devices that are located on the Internet (cloud storage).

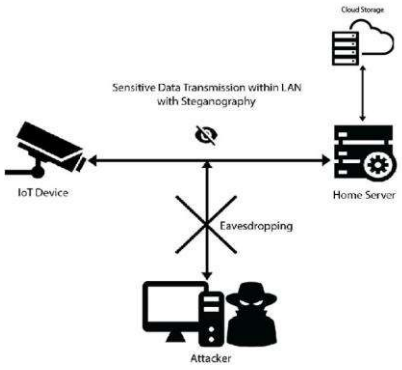

Fig .2. Proposed scheme

As we have mentioned before, the IoT devices are not able to process strong and complex encryption schemes, therefore, lightweight encryption cryptography methods can be used. Although the sensitive information is in unreadable format, attackers may still be able to uncover or decrypt it with sufficient time or processing power. In addition, the encryption does not hide the existence of information or messages from the sight of the attackers [18]. As a result, steganography approach can be used as an alternative security mechanism for transferring the data in a secure manner. Accordingly, since the IP camera mainly deals with the image in our scheme, hence, we introduce image steganography to secure any sensitive image (face), which requires to be transmitted from the IP camera to the home server.

In order to make the scheme simple, we consider Bob, who is the owner of a house, approaches the IP camera for face detection. After IP camera detected Bob's face successfully, it stores it as an image and randomly captures another image without any face detected, which is called cover image. Instead of sending the face image directly to the home server, the face image is hidden (embedded) in the selected random image (cover image) with steganography technique to produce another image (stego image), which contains the original face image. Later on, the stego image will be sent to the home server in order to retrieve the original face image from the stego image using the same steganography technique, but in a reverse way. On the other hand, an eavesdropper, Eve, has successfully attacked in Bob's network to intercept data transmission between IP camera and home server for any sensitive information. She knew that the IP camera functions as a face detection authenticator for Bob's house in the front door. Therefore, Eve captures all images, including stego image, but she does not suspect with that image as it appears to be similar to other captured images.

Steganography is a method to make confidential information and messages undetectable and prevent hackers from detecting them [19, 20]. With steganography, attackers will not be aware of the information being transmitted through a channel. In addition, several researchers have used image steganography on low processing power devices, such as embedded devices and mobile phones for hiding the data [2125]. In the following, least significant bit (LSB) technique is described as one of the image steganography methods for the

proposed scheme. This is due to its less complexity compare to complicated cryptography methods as well as high capacity in order to transfer more data [26-28].

Least significant bit (LSB) is a type of replacement method that is one of the most popular image steganography techniques [29]. In fact, the cover image pixel value (e.g. 100) can be represented as a string of zeroes and ones (bits). Similarly, the sensitive information (image face) can be shown as the other string of bits (1, 0) in order to be replaced with some of the bits of the cover image. As a matter of fact, this replacement can be occurred on the least significant bits of cover image pixels, which cannot generate a significant change on the appearance of the image (up to 4 LSBs). In contrast, any modification on most significant bit (MSB) of pixel can lead to make a major degradation on the quality of image, which can be identified through human perception [30]. However, using the LSBs of pixel to hide the sensitive information can be recognized using statistical analysis, such as x^2 analysis rather than human vision. This is due to the fact that selecting the LSBs for hiding the information is not considered to be randomized [29], which can generate an indicator for the attacker to use statistical analysis on the image to find the alteration.

To solve the above problem, inverted LSB image steganography is suggested to use in this scheme [30]. With this technique, the sensitive information has less chance to be detected by attackers due the using of bit inversion that leads to improve the quality of stego image. The authors have proposed 2 schemes for LSB inversion method, which scheme 2 required the cover image to be received by the receiver in prior. Since the IP camera is used to send the face (sensitive information) of the user only once, hence, the first scheme is adapted as the image steganography technique in this scheme. The explanation of the mentioned technique with an example is given as follows.

Assuming **1 0 1 1** are 4 bits of the message, which are needed to be embedded in image pixels 10001100, 10101101, 10101011 and 10101101. By applying classical LSB steganography, the pixels in the stego image will be converted into 10001<u>10</u>***1***, 10101<u>10</u>***0***, 10101011 and 10101<u>10</u>**1**. It is shown that the second and third LSB of three cover image pixels (highlighted by <u>underline</u>) is 0 and 1 respectively. In addition, the LSB of two of these three pixels has changed after steganography (highlighted by *italic*). In fact, inverting the LSB of bits of the certain pixels can be occurred if the pattern 0 and 1 will be occurring in the second and third bits of a pixel. Therefore, the LSB of these three pixels (first, second and fourth), which can be matched with the mentioned rules will be changed to 10001100, 10101101, 10101011 and 10101100, respectively. By comparing with the original cover image, the stego image has only one pixel different, which is the last bit of pixel four (highlighted by underline). To this end, the stego image that contains a user's face will be sent to the home server.

To strengthen the security of data transmission, especially the confidentiality, we assume that there is a home server within the IoT network, which can separate LAN network that contains IoT devices with the Internet. In this case, the home server serves as a device that retrieves (extract) the face image from the stego image. Since the home server has sufficient processing capabilities, the retrieved sensitive data (face image) from IoT devices will be encrypted with strong and complex encryption algorithms (symmetric or asymmetric) before passing it to the other devices such as cloud storage. Using the home server as a higher processing power node for encryption purpose is similar to the technique which is introduced in [12] but the difference is that they have multiple assistant nodes and a remote server (to assemble the encrypted message from assistant nodes) while in this paper, only a single home server is used. Thus, a single home server is sufficient in proposed scheme and it would be more cost efficient. In addition, using a centralized server is suggested in [31] where the wireless nodes are used to encrypt the data while the centralized server is used to decrypt the data only.

IV. DISCUSSION & CONCLUSION

Internet of Things (IoT) is a norm in the 21st century. It is getting more important and we used it as part of our daily life. One of the major concerns that need to look into it is information confidentiality and privacy. The needs for a secure and trustworthy smart environment is vital. In addition, hackers are able to attack the network due to the existence of vulnerability within IoT and low processing power devices, which can threaten the privacy of the users.

In this paper, a scheme is suggested based on the image steganography since the IP camera with low processing and memory capabilities is used as the IoT device to solve the privacy issues during the transmission between smart device and home server. Due to the limitations of smart devices, especially lower memory and computational power, the least significant bit technique is being adapted. With this technique, changes least significant bit would not result in any major degradation of quality through human perception as well as statistical analysis.

In addition, the probability of having a suspicion on transmitted data by the attacker is lower using steganography compare to the lightweight encryption since the format of data is changed in cryptography. In addition, high amount of data can be sent due to usage of image as well as inverted LSB image steganography technique, which requires less bits for embedding. Since the LSBs selection is randomized in this method, the security of the steganography algorithm can be increased.

However, selecting the proper cove image to fit the image face is one of the drawbacks of the proposed scheme. In other words, the size of cover image and its content (pixels) must be big enough in order to embed the face image within itself. Moreover, since the secure communication using image steganography is a one way mechanism, in a case that the server is required to send any information (e.g. verifying the authentication) to the IoT device (IP camera), this information will be sent in the plaintext, which can be captured and misused by the attacker.

Further research should be carried out to implement the lightweight cryptography in conjunction with steganography techniques (dual steganography) to provide more security on the transmitted data using IoT devices over the network. In addition, resizing the face image (making its size smaller than

the cover image) can be useful to select any image by IP camera as the cover image.

REFERENCES

[1] J. Brandt. (2015). *50 billion connected IoT devices by 2020*. Available: http://www.smartgridnews.com/story/50-billion-connected-iot-devices-2020/2015-04-21

[2] T. Bradley, "Experts pick the top 5 security threats for 2015 | PCWorld," 2015-01-14 2015.

[3] A. W. Atamli and A. Martin, "Threat-Based Security Analysis for the Internet of Things," in Secure Internet of Things (SIoT), 2014 International Workshop on, 2014, pp. 35-43.

[4] M. J. Covington and R. Carskadden, "Threat implications of the internet of things," in Cyber Conflict (CyCon), 2013 5th International Conference on, 2013, pp. 1-12.

[5] D. R. Stinson, Cryptography: theory and practice: CRC press, 2005.

[6] M. Katagi and S. Moriai, "Lightweight cryptography for the internet of things," Sony Corporation, pp. 7-10, 2008.

[7] T. Bhattasali, "LICRYPT: Lightweight Cryptography Technique for Securing Smart Objects in Internet of Things Environment."

[8] J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, "A lightweight authentication protocol for internet of things," in Next-Generation Electronics (ISNE), 2014 International Symposium on, 2014, pp. 1-2.

[9] Z. Bohan, W. Xu, Z. Kaili, and Z. Xueyuan, "Encryption Node Design in Internet of Things Based on Fingerprint Features and CC2530," in Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, 2013, pp. 14541457.

[10] (2015). Second Generation System-on-Chip Solution for 2.4 GHz IEEE 802.15.4 / RF4CE / ZigBee. Available: http://www.ti.com/product/cc2530

[11] A. Fragkiadakis, E. Tragos, and A. Traganitis, "Lightweight and secure encryption using channel measurements," in Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 2014 4th International Conference on, 2014, pp. 1-5.

[12] L. Touati, Y. Challal, and A. Bouabdallah, "C-CP-ABE: Cooperative Ciphertext Policy Attribute-Based Encryption for the Internet of Things," in Advanced Networking Distributed Systems and Applications (INDS), 2014 International Conference on, 2014, pp. 6469.

[13] S. Guicheng and Y. Zhen, "Application of Elliptic Curve Cryptography in Node Authentication of Internet of Things," in 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2013.

[14] R. Watro, D. Kong, S.-f. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "TinyPK: securing sensor networks with public key technology," in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, 2004, pp. 59-64.

[15] A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, S. Mathur, and A. Ingle, "Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks," in Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, 2013, pp. 1-7.

[16] T. Prabhakar, "Self-jamming: Who wins? An implementation study," in Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on, 2013, pp. 502-506.

[17] S. Chakraborty and D. Das, "An overview of face liveness detection," arXiv preprint arXiv:1405.2227, 2014.

[18] N. Tiwari and D. M. Shandilya, "Evaluation of Various LSB based Methods of Image Steganography on GIF File Format," International Journal of Computer Applications (0975–8887) Volume, 2010.

[19] S. Katzenbeisser and F. Petitcolas, Information hiding techniques for steganography and digital watermarking: Artech house, 2000.

[20] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," Security & Privacy, IEEE, vol. 1, pp. 32-44, 2003.

[21] B. Lakhsmi and B. V. Raju, "FPGA Implementation of Lifting DWT based LSB Steganography using Micro Blaze Processor," International Journal of Computer Trends and Technology (IJCTT), vol. 6, pp. 6-14, 2013.

[22] M. N. B. NAIK and M. A. N. NAIK, "Steganographic Secure Data Communication using ZIGBEE."

[23] M. S. Shahreza, "An improved method for steganography on mobile phone," WSEAS Transactions on Systems, vol. 4, pp. 955-957, 2005.

[24] M. Shirali-Shahreza, "Steganography in MMS," in Multitopic Conference, 2007. INMIC 2007. IEEE International, 2007, pp. 1-4.

[25] D. Stanescu, V. Stangaciu, I. Ghergulescu, and M. Stratulat, "Steganography on embedded devices," in Applied Computational Intelligence and Informatics, 2009. SACI'09. 5th International Symposium on, 2009, pp. 313-318.

[26] C.-K. Chan and L.-M. Cheng, "Hiding data in images by simple LSB substitution," Pattern recognition, vol. 37, pp. 469-474, 2004.

[27] S. A. Laskar and K. Hemachandran, "High Capacity data hiding using LSB Steganography and Encryption," International Journal of Database Management Systems (IJDMS) Vol, vol. 4, 2012.

[28] T. Morkel, J. H. Eloff, and M. S. Olivier, "An overview of image steganography," in ISSA, 2005, pp. 1-11.

[29] M. Paik, "Blacknoise: Low-fi Lightweight Steganography in Service of Free Speech," M4D 2010, p. 150, 2010.

[30] N. Akhtar, S. Khan, and P. Johri, "An improved inverted LSB image steganography," in Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on, 2014, pp. 749755.

[31] B. Adiga, M. Rajan, R. Shastry, V. Shivraj, and P. Balamuralidhar, "Lightweight IBE scheme for Wireless Sensor nodes," in Advanced Networks and Telecommuncations Systems (ANTS), 2013 IEEE International Conference on, 2013, pp. 1-6.