INTERNET OF THINGS (IoT): A REVIEW OF SECURITY ISSUES

Prashant Kumar Yadav
Dept. of Computer Science & Enginering
UNS IET VBS
Purvanchal University, Jaunpur

Surjeet Kumar
Dept. of Computer Application
UNS IET VBS
Purvanchal University, Jaunpur

ABSTRACT:

Now-a-days, a new generation of computing technology i.e. Internet of Things (IoT) is taking place. IOT is a network of intelligent things, connected together using the concept of cloud to make our lives much easier and safer and to reduce our impact on the environment. Every organization such as companies and civil institutions needs up-to-date information about people. In this regard, most establishments either use of websites, emails or notice boards, are performed. However, in most of countries internet access is available to people on systems and their mobile devices, so that the transferring information can be much easier and less costly through the internet. IoT uses internet to establish connection between things and user, hence security concern of that communication channel will become most important. Here we will discuss about security issues, arise in IoT communication.

KEYWORDS:

Arduino, RaspaberryPi, Cryptography, PKI.

1.INTRODUCTION:

Because of no any common definition for the IoT, the concept used behind this is that everyday objects may have the capabilities of identifying, sensing, networking and processing that will allow them to communicate with other devices and services over the Internet to obtain some useful objectives. Benefits from IoT will allow improving the services as perceived by the users, for example saving energy, enhancing comfort, getting better healthcare, and increased independence. In recent years, use of various sensing devices to monitor human activities and health has gained great research interest. Especially, sensor network applications in healthcare have the potential to make major impacts. These sensor networks can be used for real-time, continuous vital monitoring of patient status and providing immediate alerts of changes. The data can also be relayed to the hospital or correlate with patient records and soon. Human lives are directly involved in these applications. On the other hand, IoT raises new technical and ethical challenges. All wireless systems have some inherent technical vulnerabilities and limitations. Many of the sensor network applications used in healthcare heavily rely on technologies that can pose security threats. So, security and privacy are the most challenging issues raised in IoT.

Along with the involvement of computer as an embedded part of daily life, the need of some automated tools for protecting files and other information stored on the computer was felt. Introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer also congregated the requirement of security. Security is required to protect data while communicating.

In this digital world of IoT, security can be achieved by cryptography. Cryptography is a science that applies complex mathematics and logic to design strong encryption methods. Cryptography is the art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible (noise), and then retransforming that message back to its original form. Cryptography helps in storing sensitive information and transmitting it securely over insecure media (like Internet). But, how cryptography can be used to ensure privacy in Internet of Things (IoT)? The answer could be found by the following study.

2. BASIC OF CRYPTOGRAPHY

Cryptography is “Secret (crypto-) writing (-graphy)”. Cryptography is the science of using mathematics to encrypt (transform) and decrypt (retransform) data. A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm requires a key—a word, a number, or phrase—to encrypt the plaintext. Any given plaintext may be encrypted to different

ciphertext with different keys. This process can be written as:

$C=E_k(P)$

$P = D_k(C)$

where P = plaintext, C = ciphertext, E = the encryption

method, D = the decryption method, and k = the key.

The strength of the cryptographic algorithm and the secrecy of the key determine the security of encrypted data.

3. THE BASIC PRINCIPLES TO BE MET BY CRYPTOGRAPHY

3.1 Encryption

The process of converting the readable data in some unreadable form is called encryption. This helps in protecting the privacy while sending the data from sender to receiver through unsecured communication media. The receiver can decrypt the received ciphertext and find out the original message. This process of getting the original message back is called decryption. Some extra information is required for encrypting and decrypting the data. This information is known as key. Same key or different keys can be used for both encryption and decryption.

3.2 Authentication:

This is another important principle of cryptography. Authentication ensures that the message was originated from the sender claimed in the message.

3.3 Integrity:

Integrity means that the messages that are sent by sender and received by the receiver are not changed anywhere on the communication path. Cryptographic hash algorithms can be used to achieve this.

3.4 Non-Repudiation:

Cryptography should prevent the originator or sender to deny about its message. Digital signatures can be used to achieve nonrepudiation.

3.5 Key exchange:

It is the method by which crypto keys are shared between sender and receiver.

4. Various cryptographic algorithms:

In this section, different cryptographic techniques are reviewed. The algorithms can be classified on the basis of number of keys used in encryption decryption method.

Secret Key Cryptography (SKC): The sender applies a key to encrypt a message while the receiver applies the same key to decrypt the message. As only single key is used so this is a symmetric encryption method. SKC is primarily used for privacy and confidentiality. The need of key management and their secure use present a significant disadvantage of symmetric ciphers. A key must be shared by both members of each communicating party, and perhaps each ciphertext exchanged as well.

Public Key Cryptography (PKC): The cryptographic system which involves two keys for a secure communication to take place between receiver and sender over insecure communication channel is PKC. Being the involvement of a pair of keys here so this technique is also known as asymmetric encryption. This technique uses one key for encryption and another for decryption. PKC is primarily used for authentication, non-repudiation, and key exchange.

Hash Functions: This technique does not involve any key. A fixed length hash value is used which is computed on the basis of the plain text message. Hash uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint. One of the feature of a good hash function is that it becomes just very difficult for an attacker to find two messages that produce the same hash. Hash functions are used to check the integrity of the message to ensure that the message has not be altered, compromised or affected by virus.

Various SKC algorithms are present, but the most commonly used SKC algorithms are DES, 3DES, Blowfish and AES.

Data Encryption Standard (DES):

DES uses the Data Encryption Algorithm (DEA), a secret key block-cipher employing a 56-bit key operating on 64-bit blocks.

Operations of DES: DES uses a 56-bit key. All the 56-bits of the key are divided among eight blocks of 7-bits. An 8th odd parity bit is added to each block (i.e., either a "0" or "1" is added to the block so as to make the number of 1 odd in each 8-bit block). The use of 8 th parity bits for rudimentary error detection makes DES key 64 bits in length for computational purposes although it only has 56 bits worth . Then DES acts on 64-bit blocks of the plaintext, imploring 16 rounds of permutations, swaps, and substitutes. The basic DES steps are:

1. The 64-bit block of plaintext for encryption, first undergoes an initial permutation (IP), where each bit is shifted to a new bit position. Then this 64-bit permuted input is divided into two 32-bit blocks, called left block and right block, respectively. The initial values assigned to the left and right blocks are L 0 and R 0 .

2. There are then 16 rounds of operation on the L and R blocks. During each iteration (where n ranges from 1 to 16), the following formulae apply:

$L_n = R_{n-1}$

$R_n = L_{n-1} \text{ XOR } f(R_{n-1}, K_n)$

It is clear that during the process, the new value of L block is simply the previous value of R block. A DES cipher function, f, is applied to key K n (K n is a 48-bit value derived from the 64-bit DES key) and value of R block. The resultant is then bit wise

XORed with values of L block to generate new values of R block. The cipher function, f, combines the 32-bit R block value and the 48-bit subkey in the following manner:

Firstly, the 32 bits which are fed in the R block are expanded to 48 bits by an expansion function (E); the extra 16 bits are constructed by repeating the bits in 16 predefined positions. This newly formed 48-bit expanded R-block is then Ored with the 48-bit subkey. The result is a 48-bit value which is then divided into eight 6-bit blocks. These are fed as input into 8 selection (S) boxes, denoted S 1 ,...,S 8 . Each 6-bit input yields a 4-bit output using a table lookup based on the 64 possible inputs; this results in a 32-bit output from the S-box. The 32 bits are then rearranged by a permutation function (P), generating the results of the cipher function.

4.1 Secret Key Cryptography (SKC)

Symmetric-key cryptography ascribe that encryption method in which both the sender and receiver use the same key to encrypt and decrypt a message (and even if the keys are different then it is very easy to compute them). SKC converts a message into something different form that resembles random noise. The conversion can only be determined by a key. If the transformation is done character wise then it is called as stream cipher and if transformation is done on entire block then it is referred as block cipher. One of the requirement of SKC is that key must be shared to both members only and must be kept secret.

4.2 Public Key Cryptography (PKC)

In Public key cryptography (PKC) technique, two different keys i.e. a pair of public key and private key are used. Because of use of two different keys, this algorithm is known as asymmetric algorithm. PKC algorithm can be used for secure data transmission. In PKC, sender encrypts the message with its public key whereas the receiver uses its private key to decrypt the ciphertext and obtain the sent message. PKC encryption emerged to meet the growing demands of secure communication in multiple sectors and industries, such as the military. In PKC, one of the keys is designated the public key and may be advertised widely . The other key is termed as the private key and is never revealed to another party. Despite of being a lot of encryption algorithms, the most commonly used PSK algorithms are RSA, DH, ECC.

RSA:

RSA is primarily used to encrypt the session key used for secret key encryption (message integrity) or the message's hash value (digital signature). The RSA uses a variable size encryption block and a variable size key. The two prime numbers chosen according to special rules are used to produce a key-pair, n, which is the product of these two prime numbers. The primes numbers may be 100 or more digits in length each, producing an n with roughly twice as many digits as there in the prime factors. n and a derivative of one of the factors of n are present in the public key information. From this information alone, an attacker cannot determine the prime factors of n (and, therefore, the private key) and this ensures the secrecy of the RSA algorithm.

The basic steps involved in generating an RSA public/private key pair are:

1. Select two prime numbers, p and q. From these numbers

calculate the modulus, n = pq.

2. Select a third number, e, that is relatively prime to (i.e., it does not divide evenly into) the product (p-1)(q-1). The number e is the public exponent.

3. Calculate an integer d from the quotient (ed-1)/[(p-1)(q-1)]. The number d is the private exponent.

The public key is the number pair (n,e). Although these values are publicly known, if p and q are large enough, it is just not possible to determine d from n and e. Using the public key, the ciphertext, C, can be created from a message M using the equation:

C = M e mod n

The ciphertext can be decrypted by receiver with the private key using the equation:

M = C d mod n

DH algorithm

The mathematical "trick" used in Diffie-Hellman key exchange is that it is comparatively easy to compute exponents than to compute discrete logarithms. Two parties — the A and B who want to to exchange some information over an unsecure communications channel need to generate a secret key using DH algorithm such as an eavesdropper cannot determine the shared secret key based upon this information.

Diffie-Hellman algorithm is used to generate secret keys, not to encrypt and decrypt messages. Diffie-Hellman algorithm works like this. A and B start by agreeing on a large prime number, N. They also choose some number G so that G<N. There is actually another constraint on G, namely that it must be primitive with respect to N. G is primitive to N if the set of N-1 values of G i mod N for i = (1,N-1) are all different. Keys X A and X B are kept secret while Y A and Y B are shared; these are the private and public keys, respectively. A and B compute their secret keys, K A and K B , respectively, based on their own private key and the public key, which are equal to GXAXB mod N.

5. EVALUATION

IoT applications require acquiring knowledge and real time data from various sensors. The acquired data with the help of linguistic technology and comprehensive tools can be represented and integrated to extract knowledge from it. Various constraints like limited resources, mobility, scalability, dynamics, insecure communication media etc. introduce challenges for using the semantic technologies in IoT environment. In the previous sections of paper, we study the use of various techniques on IoT data for acquiring actionable knowledge by applying state-of-the-art semantic technologies. For understanding these studies, we have analyzed proposed semantic reasoning systems and cryptography techniques operating in the realistic IoT environment. Thus, it is a matter to rethinking about the best desired approach.

6. Conclusion

This paper examines the best practices for providing semantic data and reasoning actionable knowledge with well-known cryptography techniques and methods on context aware IoT environment. IoT systems work on real data set to evaluate the real time response and scalability. In this paper, analytical comparison of various cryptographic techniques on realistic scenarios for IoT applications is proposed.

References

[1] C. C. Aggarwal and P. Yu, "A General Survey of Privacy- Preserving Data Mining Models and Algorithms, in Privacy-Preserving Data Mining: Models and Algorithms,," Springer, 2008.

[2] K. C. A, "Strategies for de-identification and anonymization of electronic health record data for use in multicenter research studies," 2012.

[3] J. C. D. Garc, "The Internet of Things: connecting the world," Verlag London, 2013.

[4] E. B. Ashish Kundu, "Privacy-preserving authentication of trees and graphs," International Journal of Information Security, vol. 12, no. 6, pp. 467-494, 26 May 2013.

[5] Y. L. et.al, "Secure Key management Scheme based on ECC algorithm for Patient's Medical Information in Healthcare System," in 2014 International Conference on Information Networking (ICOIN), 2014.

[6] Danan Thilakanathan, "A platform for secure monitoring and sharing of generic health data in the cloud," Future Generation Computer Systems 35 , p. 102–113, (2014).

[7] Chang Liu, "MuR-DPA: Top-Down Levelled Multi-Replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud," IEEE TRANSACTIONS ON COMPUTERS,, pp. 2609-2622, 2015.