Security Enhancement of Internet of Things Using Service Level Agreements and Lightweight Security

Shu-Ching Wang[1], Ya-Jung Lin[1], Kuo-Qin Yan[2(✉)], and Ching-Wei Chen[1]

[1] Department of Information Management, Chaoyang University of Technology, Taichung, Taiwan, ROC
{scwang, sl06l4903, sl0ll490l}@cyut.edu.tw
[2] Department of Business Administration, Chaoyang University of Technology, Taichung, Taiwan, ROC
kqyan@cyut.edu.tw

Abstract. In the era of the Internet, people can interconnect and obtain information via the network. Through the combinational use of network and various wireless communication sensing networks, objects can now communicate with each other through the Internet environment. Furthermore, as IT evolves and as IPv6 technology eventually matures, data transmission can be carried out between smart objects by using sensing networks, networking, and computing functions. This concept which is emerging into a network environment is known as the Internet of Things (IoT). However, the related researches of the IoT have not discussed the data insecurity issues. This study establishes security level agreements to ameliorate excessive computational loads with the lightweight security mechanism so that data can be protected in the perception layer, then the computational cost of data encrypted in the perception layer.

Keywords: Internet of Things · Security level agreements · Digital signature

1 Introduction

Currently, computation capability and storage capacity of end devices are developing rapidly; the end devices have gradually become portable mobile devices. In addition, as a result of the vigorous development of information and network technology, the network types are more diversified, such as Wireless Network, Wireless Sensor Network, etc. The network environment has become ubiquitous; it is also always connected. Network patterns have evolved from the Internet of People to the Internet of Things (IoT) [4].

The IoT concept was first proposed in 1999 by Kevin Ashton. It was based on RFID (Radio Frequency Identification) technology and was proposed in Massachusetts Institute of Technology [5]. Through RFID technology, all objects were interconnected via a network, and smart identification and management could be implemented. Sensing devices, such as RFID, Zigbee, IR (Infrared), GPS (Global Positioning System), WiFi and UMTS (Universal Mobile Telecommunications System) devices are

K. Arai et al. (Eds.): FICC 2018, AISC 887, pp. 221–235, 2019.
https://doi.org/10.1007/978-3-030-03405-4_15

now connected via the Internet. They carry out information exchange and communication based on different protocols. Furthermore, intelligent identification, positioning, tracking, monitoring and management [16, 17] are implemented. These objects can be operated and can perform data exchange remotely [23]. Hence, development of the IoT is no longer limited to the RFID technical scope [3, 11, 18, 25]. In the IoT, there are thousands of different types of sense devices. Therefore, the IoT will form a more complex entity subject to a deluge of data and the security of IoT must to be considered.

In this study, a discussion on the security of data transfer between the sensor nodes is contained; a Security Level Agreement (SLA) is proposed herein. Since the sink node may cover tens of thousands of sensor nodes, the security of the data transmission is very important. However, when the data must be encrypted with high-security via the sensor nodes, the calculations may be huge. Otherwise, if the data used the low-security encryption, the remote sensor nodes may face the risk of data enduring malicious attacks.

In our study, a SLA of the sink node's coverage is proposed to enhance the security of data transmission between the sensor nodes within the perception layer. The sink node is treated as the center point, and extends around a regular hexagon of coverage; the hexagon will be divided into three phases of security level agreements to reduce the risk of data being subjected to malicious attack, as well as the computational cost of data encryption.

Through the framework of middleware layer in IoT, the identity of the application and the lightweight security between the middleware layer and the perception layer can be realized. Therefore, a digital signature mechanism is added in our study; the perception layer will require verification and non-repudiation, so that the reliability of the IoT can be obtained and maintained.

The remainder of this paper is arranged as follows: Sect. 2 illustrates the related works of this study. Section 3 illustrates the IoT structure used in our study. The proposed security mechanism is given in Sect. 4. Finally, conclusions are presented in Sect. 5.

2 Related Works

The Internet of Things and the security level agreements are introduced in this section.

2.1 Introduction of Internet of Things

According to the ITU (International Telecommunication Union) definition, the development areas of IoT are divided into three dimensions: time, place, and object, as shown in Fig. 1 [9]. In other words, any person can be connected with any object at any time and at any place. Furthermore, along with the continuous development of the IoT, three categories are also included. They are: human to human, human to thing, and thing to thing respectively [9, 13]. After the relevant technologies come to maturity, in 2008, IBM proposed the "Smart Planet" concept. In connecting objects through the internet and applying intelligent technology and services to objects, sensors are now

embedded and loaded in various places such as power grids, roads, railways, buildings and oil and gas pipelines [20]. They are interconnected in general, so that objects can communicate with each other to form the so-called "Internet of Things". Moreover, by integrating the information via supercomputers and cloud computing, the objects are integrated into the mass society to achieve the integration of human society and physical systems. On this basis, mankind can manage production and living in a more refined and dynamic way, thus achieving the state of "intelligence" [7, 12, 14, 27].

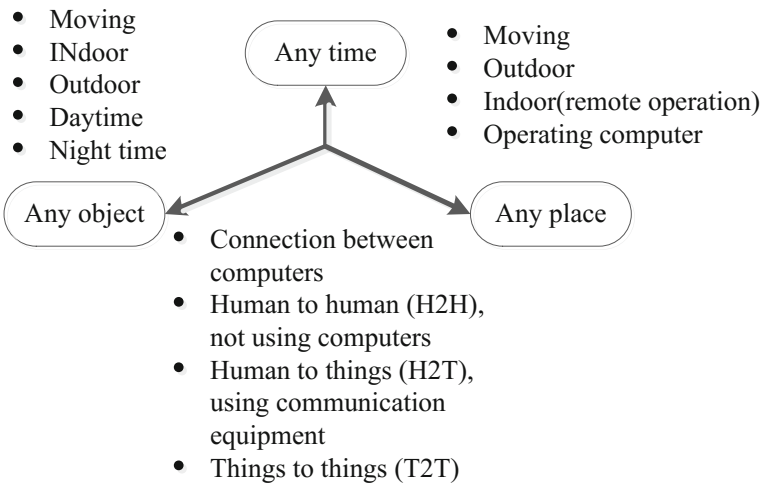

Fig. 1. The dimensions of IoT [9].

The IoT is not a new technology and is actually a very broad concept. "Things are made intelligent through the implantation of various micro-sensing chips in them. Wireless network is used to connect those intelligent things to the Internet. Hence, the information of things can be shared to implement dialogue between people and things, and communication between things. In this way, the things people interact with in their daily lives can automatically report their states. The things also automatically communicate with other things and people [6]."

The idea is to make real-life things communicate with each other in the virtual world. This way, the state of "interconnected things" is attained. "Things" mean objects in our daily lives. Through the "Internet", they are interconnected to form the IoT. In other words, the IoT attempts to connect objects in the world into a virtual, addressable network. Through the Internet based on a standard protocol, objects in the real world can be interconnected and communicate with each other to form a virtual world of networks [2, 10, 22].

As the IoT brings great benefits in various industries and livelihoods, governments are actively pursuing research and application development in related industries to promote and enhance the construction of perceptual technology and smart infrastructure to organize the vision of "smart planet", such as the implementation of: smart cities, intelligent transportation, the smart home, intelligent health care, intelligent

logistics, intelligent energy saving, smart consumption and disaster prevention monitoring. As a conclusion, the application server of the IoT and the combination of using a large number of intelligent equipment and the Internet allows people to remotely enjoy the convenience of the IoT [2].

2.2 Security Level Agreements

Due to the development of IT (Information Technology), enterprises gradually use IT more frequently to assist their business processes via the LAN (Local Area Network) or WAN (Wide Area Network), to form an electronic operating environment. In addition, enterprises rely on the hardware and software vendors to provide leased or outsourced services because these services can reduce the cost for enterprises [8].

The SLA (Service Level Agreement) signed between enterprises and vendors is meant to ensure that the demands of the enterprises have been satisfied. However, enterprises only know the content of the services provided by the vendors, while the security level of services remains unknown. In the past, many studies began to explore the SLA; the level of security and guarantee regarding the data or systems of the enterprise were placed in the hands of the vendors [8].

In recent years, the concept and technology of cloud computing have gradually achieved today's web services, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). SLA has been considered in relation to Service-oriented Architecture (SOA) and web services [1, 11]; these are currently widely used in cloud computing environments. Due to cloud computing being based on the Internet, SLA must formulate non-repudiation of content of contract, but the vendors are still unable to quantify the level of security for the demanders [15].

Therefore, SLA security is still an important issue. The European Network and Information Security Agency (ENISA) believes that the SLA in cloud computing must have different levels of security; thus, they defined the Cloud Security Level Agreement (SecLA) in order to enhance the security of SLA in cloud computing in Europe [26].

The perception layer of IoT has different types of sensor nodes; the sensor nodes may be sensors, mobile devices of users and micro-controllers. Therefore, since an area may cover tens of thousands of sensor nodes, this study will formulate a suitable SecLA in the perception layer of the IoT.

3 IoT Architecture

The topology of the IoT defined by Wang et al. [21] is used in this study: the sink node of each region is responsible for the collecting requirement for the cloud service providers and deals with the sense devices of different services; thus, each service provider may correspond to multi topology architecture. The middleware layer is defined as authenticating and processing of the cloud data, manages the secret key of the sensors, and stores the signature of authenticate completion, as shown in Fig. 2. This section describes the three-layer framework of the IoT, as well as the relationship between the various layers in reaching the goal.

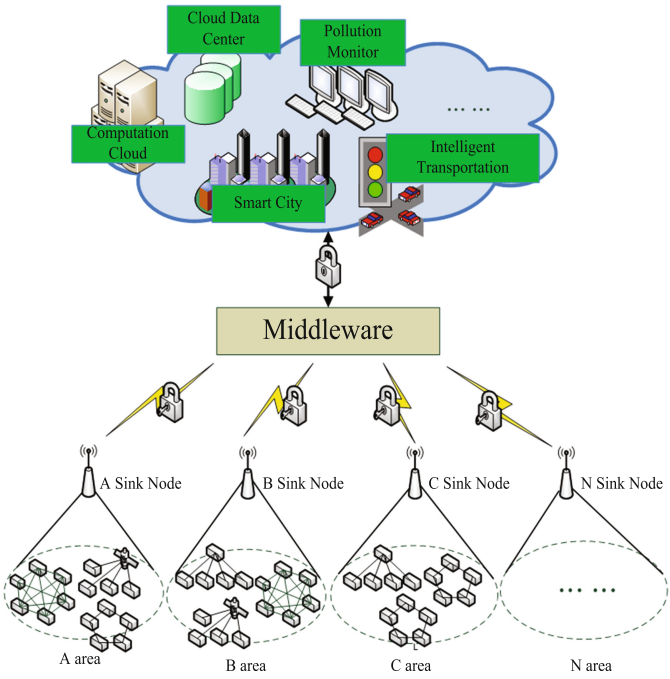

Fig. 2. The three-layer framework of the IoT.

3.1 Three-Layer Framework of IoT

The framework of the IoT is mainly divided into a three-layer: the application layer, middleware layer and the perception layer.

Application layer can provide a wide range of network services, such as today's Internet services and the services of networked smart objects by the object. The processing procedures of middleware layer include devices and services monitoring, event identification, communication management, policy management, input and output handling, remote management, and information logging. However, each network service will correspond to more perception layers. The middleware layer locates between application layer and perception layer to provide information transfer and data process.

When the demand request is sent from application layer to perception layer via the middleware layer, the application layer will send the service identity to the middleware layer. Then, the collected data of perception layer will be encrypted by a lightweight security mechanism and sent to application layer. However, when the encrypted data through middleware layer sent to application layer, the middleware layer can identify the data packets received from the source end, in order to improve the security of packet delivery.

The middleware layer entails two parts of the processing: Data Authentication and Data Processing. Data Authentication involves three components: Devices and Services Monitoring Agent (DSMA), Authentication Center (AC) and Information Logging. And Data processing involves Communication Management, Event Identification,

Policy Management, and Remote Management. Through the Devices and Services Monitoring Agent and the Authentication Center data are authenticated, with the signature stored in the Information Logging. The data are authenticated successfully via the Event Identification, the Communication Management, the Policy Management and the Remote Management, and completed by the middleware layer send data to the application layer. Smart objects of the perception layer comprise the application layer's service deployment; the application layer needs to collect the data sent to the middleware layer via the middleware layer implementation of data processing and data transmission, as shown in Fig. 3.

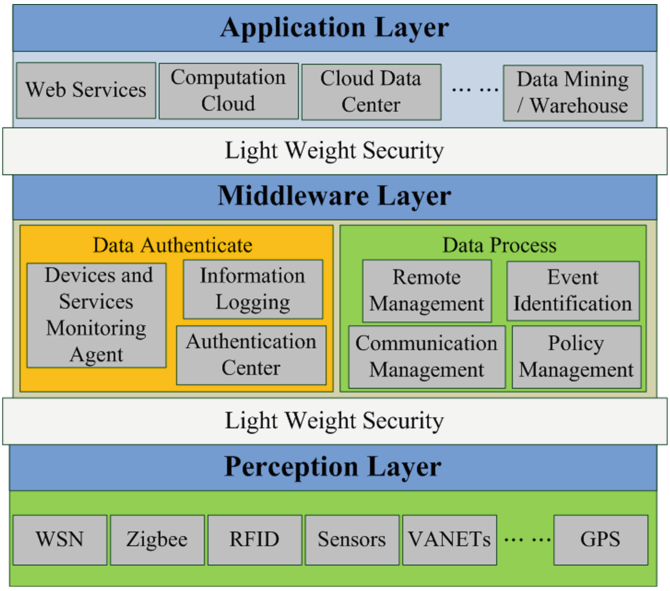

Fig. 3. The three-layer framework of the IoT.

When the application layer sends the data requirements to the perception layer via the middleware layer, the application layer sends the identity recognition to the middleware layer. Then the perception layer data collected via the lightweight security enables the middleware layer to identify the source end of the packet, and uses a suitable encryption format to improve the security of packet transmission.

When data of the perception layer have been processed via the middleware layer, according to identification, via the application layer, of each service, and are sent back to the application layer. The cloud computational resource layer primarily offers effective allocation of resources for each service requirement. Each service requirement in the cloud computational resource layer will be assigned to the respective service queue for scheduling.

3.2 Relationship of the Three-Layer Framework of IoT

In the IoT environment, the service providers of the application layer deploy several smart objects in the perception layer based on service characteristics, and the function of each smart object is based on the service requirement settings. Thus, the smart objects of the perception layer have to follow the requirements of the service providers: the data collected are authenticated, processed and transferred to the cloud computational resource layer via the middleware layer.

Due to the application layer providing diversified services, when the service requirements have been proposed, a huge amount of data will probably result. Therefore, the purpose of the cloud data center of application layer is to store the non-urgent data of the middleware layer to be processed, and according to a fixed time, sent back to the service providers of the application layer. Since the service providers of the application layer may need urgent data to satisfy service requirements quickly.

Before the service providers of the application layer obtain the data of the perception layer, it is necessary to confirm non-repudiation and verifiability of the data via data authentication of the middleware layer, in order to ensure the reliability before the data is transferred to the application layer. Thus, the Sink Node in each region is at the center of the perception layer, according to the distance sense device and the Sink Node, to extend a triple overlapping coverage of a regular hexagon from small and large, and to formulate three level security agreements. The purpose of this method is to improve the load capacity and shorten the time encryption of the data Sink Node of each region. Nearest Sink Node uses a low computational complexity encryption mechanism. The second level range sense device, joins the Sink Node generated encryption key to transfer the data. Farthest Sink Node calculates the center of gravity of each isosceles triangle to cover the first and second levels, as multi-Mobile Agent Node (multi-MAN), to transfer the data. When the Sink Node of the perception layer has collected complete data, it verifies the data by the lightweight security mechanisms.

The middleware layer mainly processes the requirements of the service provider, and verifies the return data of the perception layer; it extracts available data and, then responds to the service provider. Therefore, the middleware layer is mainly composed of data authentication and data processing components.

Data authentication is responsible for monitoring and verifying the identity of the Sink Node and data of transmission. The Devices and Services Monitoring Agent must monitor service requirements and generate the secret key and session key. Before the data is sent to data processing, the Authentication Centre must inspect the final secret key and session key; if they are correct, plaintext is converted to cipher text. Finally, the Information Log records the whole process.

Data processing is responsible for collecting/handling complete data from the perception layer, and performing the commands from the service providers. Event Identification is responsible for determining whether the data of the perception layer is an event, to define urgent data and immediately respond to the service providers. Communication Management is responsible for handling the non-urgent data; according to the service features of the service provider, data are classified, useful data are extracted by data filter, and the data transfers are reduced in size by compression. Remote Management is responsible for implementing the commands of the service

providers. Policy Management is available to service providers for mining and analysis for the Information Log, and finally developing appropriate strategies.

4 Proposed Security Mechanism

Smart objects, the main elements in collecting data in the IoT environment, are deployed in the perception layer; the characteristics of the services of the application layer determine the number and type of smart objects to be deployed. Thus, the diversification of smart objects can reach tens of thousands or even more. Furthermore, it is possible to collect data on weather values, on geological values, on defense security detection, etc. So in order to protect data security, data encryption security mechanisms must be added to ensure that data will not be altered or invaded. However, with the large number of smart objects, every object can return collected data in microseconds. If the use of encryption technology is too complex, the load calculation may also become too large. Therefore, this study establishes security level agreements to ameliorate excessive computational loads with the lightweight security mechanism so that data can be protected in the perception layer.

4.1 Security Level Agreements of Perception Layer

This study used the concept of regular hexagon coverage to formulate the suitable security level agreements for the perception layer. The hexagon coverage usually applied in the wireless network environment [19, 24], such as the 3rd-Generation (3G), Long Term Evolution (LTE) and Worldwide interoperability for Microwave access (WiMax), etc. The concept of the hexagon is extended from the round, thus each the angle have the same distance from the center in the hexagon, namely, the hexagon is composed of six isosceles triangles. Advantage of the hexagon is approaches the seamless coverage, let the sink node can received more data of the sensor nodes, and sensor nodes can seamlessly transferred the data to other sensor nodes or sink node.

In order to reduce the overload and calculation cost of encryption for the sink node, divided into three phase security level agreements. In the initial definition, 1/3 multiples of the intra-cell as level I, 2/3 multiples of the intra-cell as level II and the all of the intra-cell as level III, as shown in Fig. 4.

In general, the level I covers minimum number of the sensor nodes, and the sink node will be within the range. Therefore, the sensor nodes do not need too complex encryption costs in the level I, this study use the hash function $h(.)$ to encrypt the original data (OM).

The level II covers number of sensor nodes more than the level I, and far away from the sink node. The security level agreements of the Level II must be generated key of sensor nodes, the key only belong the used for the sensor nodes of level II. The data of the sensor nodes of level II not only to used h(OM), but also used the key by the sink node $r_{SNi}(.)$ generated. The final result of encryption is $E(K_{L2,SNi} \parallel h[\text{OM}])$.

The level III covers the maximum rage, in other words it covers most the sensor nodes. Therefore, the data cannot be used the complex encryption algorithm, but if used a simple encryption algorithm, the data may be stolen or tampered of the risk.

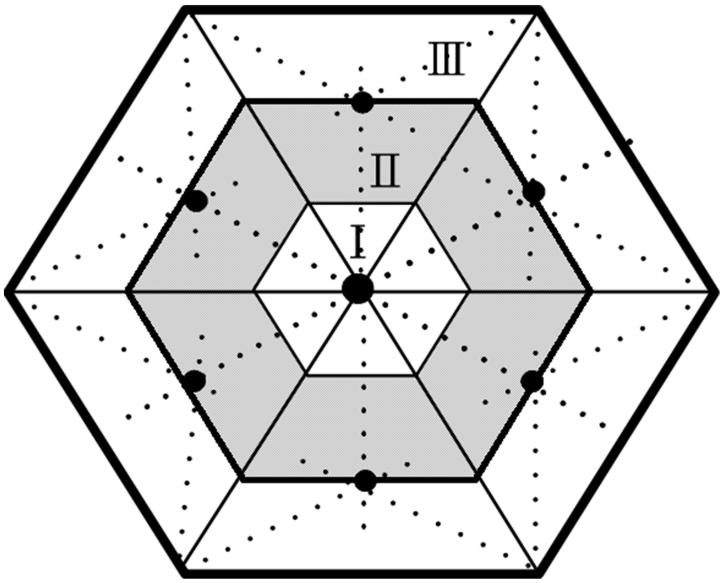

Fig. 4. Three phase security level agreements of IoT.

The centroid of each isosceles triangle underlying the total coverage of the sink node is calculated in this study, the centroid as the multi-Mobile Agent Node (multi-MAN). The multi-MAN receives the data from the level III area of each isosceles triangle. Each multi-MAN will have the key by the sink node $r_{SNi}(.)$ generated, $K_{L3,MANi}$. Finally, the result of the encryption is $E(K_{L3,MANi} \| h[OM])$. When the sink node received the data from each phase, the data will be integrated and transferred to the middleware layer that certification and processing of data. Table 1 employs mathematical symbols to denote the parameters for the security level agreements.

Table 1. The mathematical symbols of the lightweight security

r_{SNi} (.)	Random number generator with SN_i as a seed
$r_{DSMA}(.)$	Random number generator with DSMA as a seed
K_{SNi}	Secret key of SN_i
K_{AC}	Secret key of AC
K_{MW}	Secret key of MW
$K_{SNi,MW}$	Session key with SN_i and MW
$E(K,[OM])$	Encrypted original message OM using K
SR_y	The service request of service provider y
$DSMA_{pro}$	The probe request of DSMA
AC_{Kreq}	The request of secret key update send by AC
$SN_{i,areq}$	The request of data transfer by SN_i

4.2 Workflow of Lightweight Security Mechanisms

This study applied the concept of the digital signature to ensure the reliability of data, by using the third-party arbitration approach, with the middleware layer as third-party authentication to ensure data transmission between the source and destination.

Lightweight security mechanism proposed in this study is divided into two phases: Generated $K_{SNi,MW}$, K_{SNi}, K_{MW} and K_{AC} and Authentication phase.

4.2.1 Generated $K_{SNi,MW}$, K_{SNi}, K_{MW} and K_{AC}

In the framework of this study, the perception layer must make identity authentication through the middleware (MW) layer. The Devices and Services Monitoring Agent (DSMA) starts to calculate the secret key for SN_i of every area, MW and the Authentication Centre (AC); via $r_{DSMA}(SN_i)$, $r_{DSMA}(MW)$ and $r_{DSMA}(AC)$ it generates K_{SNi}, K_{MW} and K_{AC}, finally loading to the sensor node, middleware layer and authentication center, respectively.

Let SN_i be the Sink Node (SN) identifier i where $i \geq 0$. Between the SN_i and MW a session key $K_{SNi,MW}$ will be generated. $K_{SNi,MW}$ is generated by K_{SNi} and K_{MW}, converted to XOR. The session key function is building a secure communication channel for SN_i and MW because K_{SNi} may face the risk of being compromised. In the transmission process, the session key enhances the security of transmission for SN_i and MW.

$$SN_i \rightarrow DSMA: OM||E(K_{SNi}, K_{SNi,MW}, [SN_i||h(OM)])$$
$$DSMA \rightarrow AC: E(K_{AC}, [SN_i||OM||E(K_{SNi}, (K_{SNi,MW}), [SN_i||h(OM)||TS])$$

4.2.2 Authentication Phase

SN_i collected the original message (OM) through the hash function to be converted to a fixed-length message digest h(OM). It then used the secret key of SN_i, K_{SNi}, and session key $K_{SNi,MW}$ to encrypt a signature that was transferred to DSMA of MW and AC performed authentication. DSMA executed authentication of the first phase K_{SNi} and $K_{SNi,MW}$, verifying the identity of SN_i. Then DSMA sends that verified message to AC; AC used K_{AC} obtain the plaintext of SN_i, and stores the signature $E(K_{SNi}$, $(K_{SNi,MW})$, $[SN_i \| h(OM)])$ and the timestamp (TS) in the Information Logging. The plaintext data are delivered to the subroutine of the middleware layer that processes the data.

In this study, there are two scenarios of the authentication process, one is the service provider or DSMA to send out a probe message to collect data, and the other is the SN_i to collect the urgent data that must be immediately undergone DSMA authentication and be transmitted to the service provider. The scenario of the service provider or DSMA sends out a probe message to collect data is shown in Fig. 5.

The scenario of the SN_i collects urgent data that must be immediately undergone DSMA authentication and be transmitted to the service provider is shown in Fig. 6. The authentication process is shown in Fig. 7. SN_i active sends out the requirements for transferring the data. In addition to periodic collected data under the IoT environment, when the sensor device discovers unreasonable data, they are immediately transferred for analysis and processing by the middleware layer.

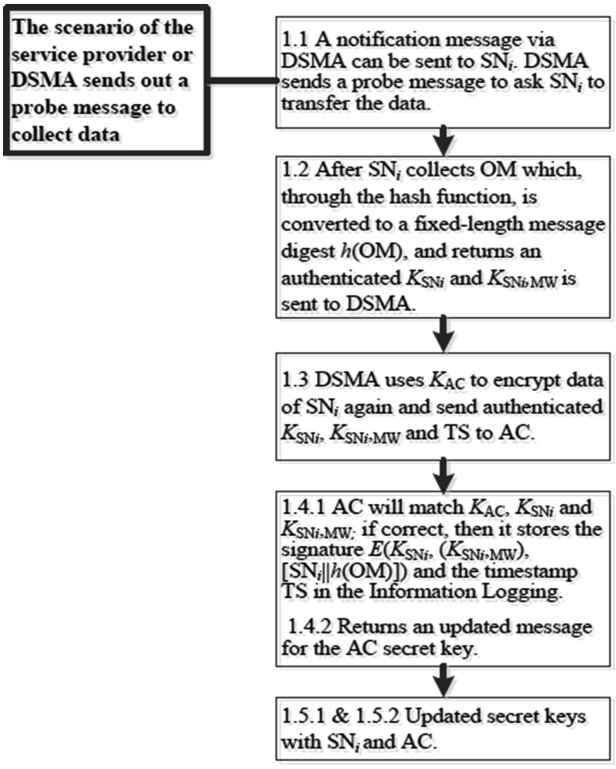

Fig. 5. The scenario of the service provider or DSMA sends out a probe message to collect data.

The perception layer may include thousands of different types of sense devices; to simplify the complexity of security encryption technology, this study uses the Sink Node as the center, and the concept of a regular hexagon coverage formation of three overlapping regular hexagons. Divided into three phases of security level agreements, and from near to far using a hash function, the private Sink Node key and multi-MAN are used for encryption. In addition to reducing the amount of computing for the encryption technology, the data obtains protection via encryption technology.

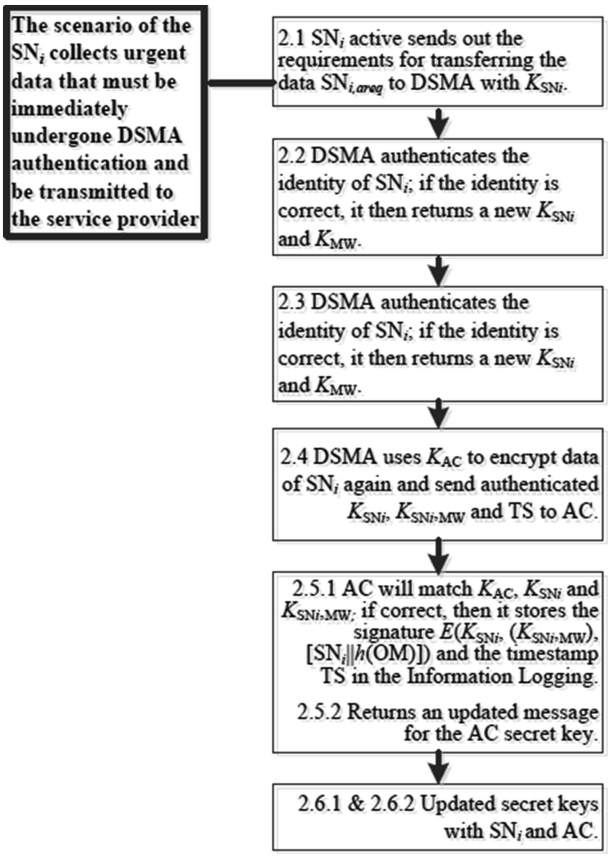

Fig. 6. The scenario of the SNi collects urgent data that must be immediately undergone DSMA authentication and be transmitted to the service provider.

In the lightweight security mechanism which this study proposes, the sense devices of the perception layer collect data sent back to the middleware layer. Four secret keys and one session key are used to perform data encryption and authentication twice from the Sink Node to the DSMA and then the AC to enhance the data transmission of the security mechanism between the perception and middleware layers.

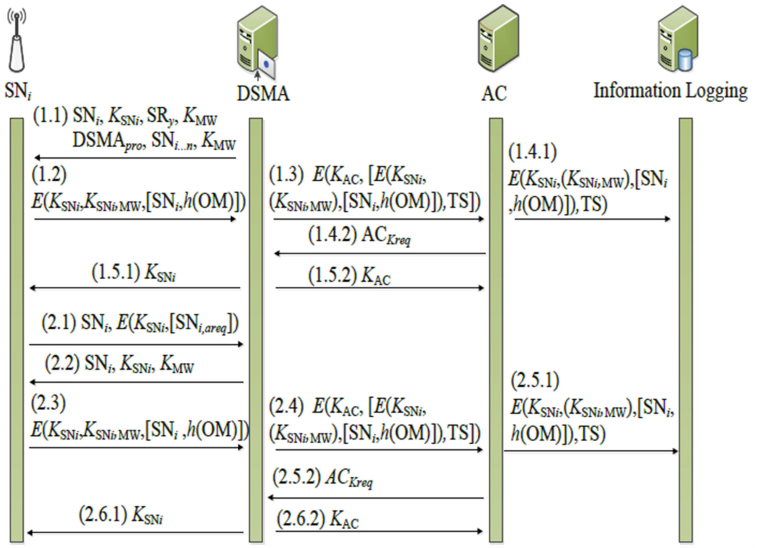

Fig. 7. Process of the data authentication.

5 Conclusion

There are a large number of heterogeneous smart objects in the IoT; thus, the data are huge and complex. Therefore, a security level agreement of IoT is proposed in this study; this agreement can reduce the vast costs of encryption to obtain the acceptable security.

When the collected data is transmitted to the middleware layer by sensor node SN_i, SN_i must have the private key issued by DSMA (Devices and Services Monitoring Agent) to transmit the data. In order to avoid the $K_{SNi,MW}$ being attacked by the attacker, $K_{SNi,MW}$ of SN_i and middleware layer is added in the transmission process to ensure the integrity of data, verifiability of identity and the principle of non-repudiation. In addition, the signature of the transmission process and the time stamp is stored in the log of middleware layer. However, the agreement presented herein is only a preliminary concept; it only considers the threats occurring when the data are transferred. Future studies can explore the back-up of the sink node and data transfer to the inter-region, thereby establishing complete security level agreements of the IoT.

In this study, the proposed security level agreement of IoT is a preliminary concept that considers only the threats that may occur when data is delivered. In the future works, the backup node mechanism of sink node and the cross-regional data transfer to establish a complete IoT security level agreement will be continued to explore.

Acknowledgment. The authors like to thank the Ministry of Science and Technology, ROC (MOST-106-2221-E-324 -009) to support this research.

References

1. Andrieux, A., Karl, C., Dan, A., Keahey, K., Ludwig, H., Nakata, T., Pruyne, J., Rofrano, J., Tuecke, S., Xu, M.: Web services agreement specification (WS-agreement). In: Open Grid Forum, vol. 128 (2007)
2. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)
3. Chan, H., Perrig, A.: PIKE: peer intermediaries for key establishment in sensor networks. In: Proceeding of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 1, pp. 524–535 (2005)
4. Coetzee, L., Eksteen, J.: The internet of things-promise for the future an introduction. In: Proceedings of IST-Africa Conference, pp. 1–9 (2011)
5. Gavras, A., Karila, A., Fdida, S., May, M., Potts, M.: Future internet research and experimentation: the fire initiative. ACM SIGCOMM Comput. Commun. Rev. **37**(3), 89–92 (2007)
6. Gershenfeld, N., Krikorian, R., Cohen, D.: The internet of things. Sci. Am. **291**, 76–81 (2004)
7. He, M., Ren, C., Wang, Q., Shao, B., Dong, J.: The internet of things as an enabler to supply chain innovation. In: Proceedings of the International Conference on e-Business Engineering (ICEBE), pp. 326–331 (2010)
8. Henning, R.R.: Security service level agreements: quantifiable security for the enterprise? In: Proceeding of the ACM Workshop on New Security Paradigms, pp. 54–60 (1999)
9. ITU Internet Reports: The Internet of Things. International Telecommunication Union, Geneva (2005)
10. Jara, A.J., Zamora, M.A., Skarmeta, A.: Global IP: an adaptive and transparent ipv6 integration in the internet of things. In: Proceedings of the Mobile Information Systems, vol. 8, no. 3, pp. 177–197 (2012)
11. Lee, H., Kim, Y.H., Lee, D.H., Lim, J.: Classification of key management schemes for wireless sensor networks. In: Proceeding of the International Workshop on Application and Security Service in Web and PervAsive eNvironments, vol. 4537, pp. 664–673 (2007)
12. Lin, M., Zhang, J.: The application and development of internet of things with its solutions of restrictive factors. In: Proceedings of the International Conference on Mechatronic Science, Electric Engineering and Computer (MEC), pp. 282–285 (2011)
13. Lu, T., Neng, W.: Future internet: the internet of things. In: Proceedings of the International Conference on Advanced Computer Theory and Engineering, vol. 5, pp. 376–380 (2010)
14. Luigi, A., Antonio, I., Giacomo, M.: The internet of things: a survey. Comput. Netw. **54**, 2787–2805 (2010)
15. Luna, J., Ghani, H., Vateva, T., Suri, N.: Quantitative assessment of cloud security level agreements: a case study. In: Proceedings of Security and Cryptography, pp. 64–73 (2012)
16. Perrig, A., Szewczyk, R., Wen, V., Cullar, D., Tygar, J.D.: SPINS: security protocols for sensor networks. Wirel. Netw. **8**(5), 521–534 (2002)
17. Sarma, A.C., João, J.: Identities in the future internet of things. Wirel. Pers. Commun. **49**(3), 353–363 (2009)
18. Sarma, S.E., Weis, S.A., Engels, D.W.: RFID systems and security and privacy implications. In: Proceeding of the 4th International Workshop on Cryptographic Hardware and Embedded Systems, pp. 454–469 (2002)
19. Schoenen, R., Walke, B.H.: On PHY and MAC performance of 3G-LTE in a multi-hop cellular environment. In: Proceeding of the International Conference on Wireless Communications, Networking and Mobile Computing, pp. 926–929 (2007)

20. Wang, B.: Review on internet of things. J. Electron. Meas. Instrum. **23**(12), 1–7 (2009)
21. Wang, S.C., Chen, C.W., Wang, S.S., Yan, K.Q.: To achieve data availability and reliability by a middleware framework underlying the IoT environment. In: BAI2013 International Conference on Business and Information, Bali, Indonesia, pp. E24–E31, 07–09 July 2013
22. Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M., Borriello, G.: Building the internet of things using RFID: the RFID ecosystem experience. In: Proceedings of the IEEE Internet Computing, vol. 13, no. 3, pp. 48–55 (2009)
23. Xue, Y., Zhihua, L., Zhenmin, G., Haitao, Z.: A multi-layer security model for internet of things. In: Internet of Things. Communications in Computer and Information Science, vol. 312, pp 388–393 (2012)
24. Yen, S.P., Talwar, S., Lee, S.C., Kim, H.: WiMax femtocells: a perspective on network architecture, capacity, and coverage. IEEE Commun. Mag. **46**(10), 58–65 (2008)
25. Zhou, Q., Zhang, J.: Research prospect of internet of things geography. In: Proceeding of the 19th International Conference on Geoinformatics, pp. 1–5 (2011)
26. Dekker, M., Hogben, G.: Survey and analysis of security parameters in cloud SLAs across the european public sector. European Union Agency for Network and Information Security. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector
27. IBM: Smarter planet-United States. http://www.ibm.com/smarterplanet/us/en/