Device classification based data encryption for internet of things

Rishabh* and T.P. Sharma

Department of Computer Science and Engineering,
National Institute of Technology Hamirpur,
Hamirpur, Himachal Pradesh – 177005, India
Email: cs14mi508@nith.ac.in
Email: teek@nith.ac.in
*Corresponding author

Abstract: The internet of things (IoT) has gained much popularity and has become an essential topic of research, because of its vast implementations. It has emerged as a field of great potential, impact, and growth. Despite its privacy concerns and security issues, it still is growing in demand for large-scale deployment. In this paper, we propose class-specific data encryption techniques for heterogeneous IoT devices. Devices are classified based on their computational and communication capabilities. Accordingly, different schemes for data encryption/decryption are proposed at different levels of interconnection across devices of different classes. The classification makes it easy to develop, study, and analyse the behaviour of the devices, as the devices of the same class have similar properties and performance. It also helps to develop standards of security protocols, policies, and frameworks based on the device class. Simulation experiments reveal significant improvements in the solution of encryption techniques for given scenarios.

Keywords: internet of things; IoT; security; challenges; issues; threats; privacy.

Reference to this paper should be made as follows: Rishabh and Sharma, T.P. (2020) 'Device classification based data encryption for internet of things', *Int. J. High Performance Computing and Networking*, Vol. 16, No. 1, pp.36–42.

Biographical notes: Rishabh received his Bachelor's and Master's degree in Computer Science and Engineering from the National Institute of Technology Hamirpur. He is a two-time Google Summer of Code student and an active open-source contributor. His area of interest is information security, internet of things, computer networks, and opportunistic encryption.

T.P. Sharma is an Associate Professor at the Department of Computer Science and Engineering at the National Institute of Technology Hamirpur. He has completed his PhD from the Indian Institute of Technology, Roorkee, India. He has more than 23 years of teaching and research experience. He has published numerous research papers in international journals and conferences. His area of interest is distributed systems, wireless sensor networks, MANETs and VANETs.

1 Introduction

Internet of things (IoT) refers to the integration of a large number of uniquely identifiable physical objects, devices, sensors and smart nodes over a network (Conti et al., 2018). These devices are capable of transmitting data, i.e., communicating with each other, without the need for human intervention (Alaba et al., 2017). The devices work autonomously in connection with each other. These devices transmit, gather and monitor all types of data on machines and human life. These devices even transmit the vital information regarding the owner's personal life, e.g., health status as well as the information regarding the devices user owns. When all of the collected information from various devices is combined, it can reveal the critical things about the personal life of the owner/user, e.g., the health condition, daily schedule. If this information is mishandled or falls prey to the hands of a threat actor, this can put the life of owner/user at risk (Yan et al., 2014). So, it becomes essential to ensure the security of the IoT devices as well as providing the data confidentiality and integrity of data to be transmitted by the devices. There are various privacy and security issues such as authorisation, verification, access control, information and storage management, system configuration. These have become some of the significant challenges in the domain of IoT (Jing et al., 2014). The development in the domain of IoT depends significantly on the address of these privacy and security concerns (Sicari et al., 2015).

The concept of IoT has become widely popular in the past decade, and the IoT devices connected to the internet are increasing at a faster rate. Some of the typical applications of IoT like Google Home, Alexa, Smart

parking, Smart cars have contributed a lot towards the increasing popularity of this concept. With increasing use of IoT in the vast domains require the security standards to be maintained to ensure user privacy and network security without compromising on the service quality of the application. Achieving the above motive is a bit difficult as the security standards in IoT are lagging far behind.

2 Related work

Alaba et al. (2017) discussed various IoT scenarios and provided an analysis of possible attacks. Also, the open research issues and the security challenges in the implementation of IoT are described as well. Possible solutions are proposed for improving the IoT security architecture. The security threats in the communication channels in the IoT application domain have also been compared.

Various solutions for the IoT architecture and applications are proposed by Guo et al. (2017) and Granjal et al. (2015). A secure architecture for IoT using the key management system (KMS) for smart cities was proposed by Chakrabarty and Engels (2016) and Haroon et al. (2016). The KMS provided efficient key distribution approach along with providing privacy, confidentiality, and integrity.

Singh et al. (2017) discussed various lightweight cryptographic techniques, including stream ciphers, lightweight block ciphers, hash functions, and high-performance systems in detail. Various cryptographic algorithms, including lightweight ones, are analysed based on their structure, key and block size and number of rounds. Also, various security architectures were discussed, along with open research challenges, issues, and solutions. A security scheme is also proposed for the improvement of resource-constrained IoT environment.

Security and forensic challenges in the domain of IoT were introduced and then discussed in Conti et al. (2018). The various security challenges discussed are authentication, authorisation and access control, privacy, and secure architecture. Evidence identification, the collection, and preservation along with evidence correlation after analysis and attack of deficit attribution were some of the discussed forensic challenges in IoT. The potential promising solutions were also presented in the paper after discussing various security and forensics-related issues in the IoT.

Security attacks of various kinds are discussed and classified into various categories by Deogirikar and Vidhate (2017). The study also examines various countermeasures in finding the most noteworthy attacks in the domain of IoT. Various attacks have also been compared by the authors based on their efficiency and damage level in IoT. The author has divided the security attacks into four categories named physical attack, network attack, software attack, and encryption attack. The physical attacks concentrate on the hardware devices present in the system, whereas the network attacks are more focused on the networks of the IoT system. The software attacks are formed using worms virus spyware, and the only motive is to steal the user data or deny the services. The main focus of the encryption attack is to destroy the encryption technique used and to obtain the private key.

Major security issues were surveyed and presented by Khan and Salah (2018). The paper reviews and categorises popular security issues concerning IoT architecture, communication protocols used for networking and management. The author also focuses on using blockchain for solving many IoT security problems, issues, and challenges. The author classifies the IoT security issues as low-level security issues, intermediate level security issues, and high-level security issues.

Security problems and other related challenges are discussed in the paper presented by Tewari and Gupta (2018). The paper also discusses various cross-layer integration and security issues (heterogeneous). The authors have very well discussed the integration issues in various domains such as data storage, cloud, big data, RFID. In each domain, they have discussed various issues.

In all the above-mentioned papers various IoT scenarios have been discussed along with analysis of possible attacks. Various protocols for the secure transmission of data have been presented and analysed along with discussing security issues and challenges. The content presented in this paper is similar to all of the above papers in terms of the domain, i.e., we have discussed various protocols for the secure transmission of data along with discussing various issues and challenges. But one different thing is that first we have divided the available devices into various classes and then proposed class-specific data encryption/decryption techniques. We chose this approach because not all devices which are connected to a network and performing tasks for a specific purpose are the same. They all have different computation and communication capabilities that is why we have classified the devices and have proposed different schemes for data encryption and decryption at different levels of interconnections for devices connected across different classes.

Wu et al. (2016) discussed various relevant challenges and relationships between the trend of big data era and that of new generation green revolution. As IoT devices are a significant contributor of big data, it becomes essential to study the correlations among big data and green objectives. Wu et al. (2018) discussed the seventeen sustainable development goals present in the 2030 development agenda which was approved by the UN. The paper discussed the roles and opportunities that information and communication technologies play in pursuing the seventeen SDGs.

Atat et al. (2018) have provided a broad overview of big data analysis, access, processing, collection and storage. The paper also provides an overview of various security solutions proposed for big data analysis, access and storage. It also discusses various security vulnerabilities and security solutions for cyber-physical systems. The paper also discusses the expected significant increase in the raw sensed data. The paper also has some open issues for the cyber-physical systems that are yet to be addressed.

An end-to-end intelligent attack detection method is proposed by Jiang et al. (2018). This method is based on neural networks and uses long short term memory recurrent neural networks to generate classifiers which can differentiate the attack from normal traffic. This method has achieved better accuracy by introducing a voting algorithm to determine whether input data is an attack or not. Singh and Vardhan (2019) proposed a secure decentralised peer-to-peer network architecture for property transaction. The paper also proposed the use of smart contract based verification system using IoT devices. The proposed mechanism saves the computation power as well as network bandwidth. A review of data compression and optimisation techniques in cloud storage for IoT is done by Hossain et al. (2019). The paper along with discussing data compression and storage optimisation also discusses their implications and concluded that implementing algorithms in middle layers (i.e., between the device and cloud) can deliver better results.

3 Proposed approach

Problem statement – to find various parameters for classifying IoT devices and finding suitable encryption techniques for different classes.

Objectives to achieve the above goal:

- Classification of the IoT devices based on performance (throughput, processing power, device lifespan, and memory size). The classification makes further development, studying, and analysing the behaviour of devices easy. As the devices of the same class have similar properties and performance, the standards of security protocols, policies, and frameworks can be developed/followed/applied based on device class.
- Encrypting the dataflow using suitable encryption techniques based on different classes. Every class has a suitable encryption technique to interact with the devices of the same or other classes.
- Different devices belonging to the same network use different encryption techniques for intercommunication based on their class.

3.1 Parameters for classification

The proposed approach has used some parameters for classification of IoT devices, which are as follows:

1 data transfer rate/throughput

2 processing power

3 device lifespan [in one charge (battery backup, wired)]

4 memory size.

On the bases of the above parameters, the classification of IoT devices is done into three classes. The parameters have been classified into various groups, with each group representing a particular entity from the parameter. Tables 1–4 are the tabular representation of the same.

Table 1 Class description on the basis of throughput

Group	*Throughput*
A0	<10 Kbps
A1	10 Kbps–100 Kbps
A2	100 Kbps–1 Mbps
A3	>1 Mbps

Table 2 Class description on the basis of processing power

Group	*Processing power*
C0	<500 MHz
C1	500MHz–1 GHz
C2	>1 GHz

Table 3 Class description on the basis device lifespan

Group	*Device lifespan*
D0	<1 day (in one charge)
D1	1 day–1 week (in one charge)
D2	>1 week (in one charge)
D3	Always connected to the source of power supply

Table 4 Class description on the basis of memory size

Group	*Memory size*
E0	<10 Kb
E1	10 Kb–256Kb
E2	256 Kb–1 Mb
E3	>1 Mb

3.2 Classification on the basis of parameters

On the basis of parameters for classification the devices are divided into three classes which are as follows:

3.2.1 Class 1 (low-end devices)

The devices which belong to this class have a data transfer rate which is less than 10 Kbps, and they have the low-end processing power, i.e., they have processing power < 500 MHz, they can have a lifespan of up to 1 week on a single charge or may remain connected to a source of power supply throughout their lifetime. They have memory size of up to 256 Kb. Some devices belonging to this category are typical IoT sensors and smart room heater.

3.2.2 Class 2 (average devices)

The devices which belong to this class have a data transfer rate which is 10 to 100 Kbps, and they have the average processing power, i.e., they have processing power between 500 MHz to 1 GHz, they can have the lifespan ranging from

one day to over one week on a single charge or may remain connected to a source of power supply throughout their lifetime. They have a memory with a size between 256 Kb to 1 Mb. Some devices belonging to this category are wearable devices and smart home assistants.

Table 5 Summary of devices in class 1

Throughput	A0
Processing power	C0
Device lifespan	D0, D1, D3
Memory size	E0, E1
Example	IoT sensors, smart room heater

Table 6 Summary of devices in class 2

Throughput	A1
Processing power	C1
Device lifespan	D1, D2, D3
Memory size	E2
Example	Wearables, smart home assistants

3.2.3 Class 3 (high-end devices)

The devices which belong to this class have a data transfer rate of over 100 Kbps, and they have the high-end processing power, i.e., they have processing power > 1 GHz, they can have a lifespan ranging from one day to over one week on a single charge or may remain connected to a source of power supply throughout their lifetime. They have a memory with size over 1 Mb. Some devices belonging to this category are computers, tablets, and cloud servers.

Table 7 Summary of devices in class 3

Throughput	A2, A3
Processing power	C2
Device lifespan	D1, D2, D3
Memory size	E3
Example	Computers, tablets, laptops, cloud servers

3.3 Assumptions

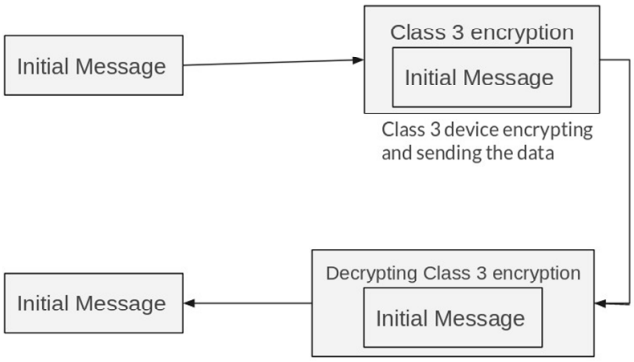
1 The volume of data is constant: the total volume of Data at any intervals of the same duration remains constant.

2 The encryption technique to be used for the device is preloaded onto the device by the device manufacturer/ vendor. The user does not install the encryption scheme code in the device.

4 Encryption technique based on different classes

Based on the classification in the previous section (Section 3) we can use various encryption techniques suitable for sending data between the devices belonging to the same or different classes in different scenarios.

Figure 1 Sending data from class 3 to class 3



4.1 Sending data from class 3 to class 3

Data can be sent from a class 3 device to other devices of the same class after encrypting using any of the following encryption techniques:

1 Key management protocol (with implicit certificates) (Sciancalepore et al., 2015). This enables fast key negotiation, lightweight node authentication, protection against replay attacks.

The authentication field in the protocol is calculated using function:

$$\alpha A = \text{Auth}\left(P_K\left(P_A, P_B, \rho_A, \rho_B\right)\right)$$

where P_K: pre link key, (P_A, P_B): public keys, and (ρ_A, ρ_B): nonce.

2 PKI encryption using digital certificates (Doukas et al., 2012).

Provides data confidentiality, authentication, add 24.5% overhead in total transmission time, certificate authority required.

3 DTLS using public certificates (Panwar and Kumar, 2015). Data confidentiality is provided, authentication, the memory requirement is maximum 17 MB, certificate authority required, no pre-shared key is required.

4 RSA with key sharing mechanism (Suo et al., 2012). Enables public key encryption, ensures authenticity, non-repudiation and confidentiality.

4.2 Sending data from class 2 to class 2

Sending data from a class 2 device to other devices of the same class OR devices of some higher class can be encrypted using the following encryption techniques:

1 AES-128 (advanced encryption standard) (Singh et al., 2017; Tsai et al., 2018) with key sharing mechanism (Suo et al., 2012). Vulnerable to side channel attacks.

2 HEIGHT (high security and lightweight) (Singh et al., 2017). Works well for low energy devices, is vulnerable to saturation attacks.

3 Attribute-based encryption (ABE) on AES key (Wang et al., 2014). Considerable delay at higher security levels for class 2 devices and unnoticeable delay for class 3 devices (if they are at the receiver end) (Wang et al., 2014).

4 PRESENT (Singh et al., 2017) works very well with low power devices.

4.3 Sending data from class 1 to class 1

Sending data from a class 1 device to other devices of the same class OR the device of some higher class can be encrypted using the following techniques:

1 Elliptic-curve Diffie Hellman (ECDH) (Yao et al., 2015). It has a very small key size, very less memory requirement.

The shared secret is generated by:

$$K_{A,B} = S_A \cdot P_B = S_B \cdot P_A = S_A \cdot S_B \cdot G$$

where (S_A, P_A), (S_B, P_B) are key pairs used to generate it.

2 RC5 (Singh et al., 2017) vulnerable to differential attack, small key size.

3 Key-policy attribute-based encryption (KP-ABE) (Yao et al., 2015).

4.4 Sending data from class 1 to class 2

It follows the same encryption techniques as that used for

- Sending data from class 1 to class 1 and the data encryption-decryption diagram is also the same.

4.5 Sending data from class 1 to class 3

It follows the same encryption techniques as that used for

- Sending data from class 1 to class 1 and the data encryption-decryption diagram is also the same.

4.6 Sending data from class 2 to class 3

It follows the same encryption techniques as that used for

- Sending data from class 2 to class 2 and the data encryption-decryption diagram is also the same.

4.7 Sending data from class 1 to class 3 via class 2

It follows the same encryption techniques as that used for

- Sending data from class 1 to class 1 and sending data from class 2 to class 2 and the data encryption decryption diagram is given below.

In this case, the data sent by class 1 device is encrypted using the techniques mentioned in the section 'sending data from class 1 to class 1'. On receiving data the class 2 device further encrypts it using the techniques discussed in the section 'sending data from class 2 to class 2'.

The class 3 device first decrypts the encryption used by the class 2 device and then decrypts the encryption used by class 1 device.

5 Applications

For IoT devices to work such solutions are required because they need to communicate with each other to transfer the data. And usually, the data travels via one or more devices(nodes) present in between to reach its destination. So, it is essential that the data remains encrypted at all points and not just after a particular point in the route. In the other approaches described in the related work section, they only present how to add encryption between two devices (heterogeneous or homogeneous). They do not consider devices of varying capacities connected and sending data from source to destination with other devices acting as nodes in between, whereas these nodes are also actively collecting and sending data to the destination.

So our approach not only covers the latter scenario but it also covers the scenario where various heterogeneous devices are present in between which are also actively collecting and sending data to the destination.

Some applications to utilise such solutions are as follows:

- Car sensors – These sensors keep track of car speed, mileage, fuel efficiency, fuel left, car location, ignition status, transmission details, etc. and they send this data for analysis and to display it to the user on the dashboard or an application. So, when they send data, its usually by using external (users mobile phone) cellular connectivity or by another inbuilt module for cellular connectivity.
- Emergency response system – These systems keep track of particular things (e.g., the CO_2 levels in a factory) and usually send data using cellular connectivity or Wi-Fi.
- Smart things hub – This hub has a collection of various kinds of sensors, e.g., sensors controlling lights, locks, speakers, cameras, etc. All these sensors collect data and then send it to the cloud. Usually the user mobile application and dashboard access this data from the cloud.

Figure 2 Sending data from class 1 to class 3 via class

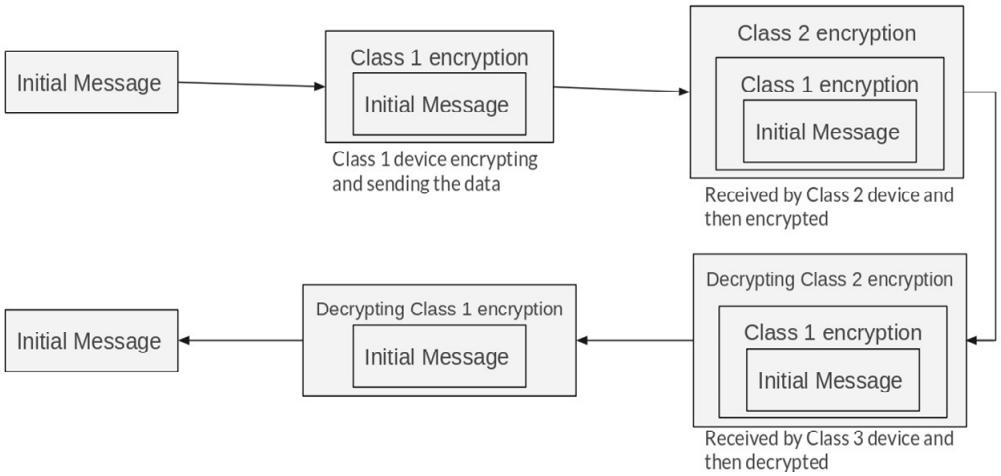


Table 8 Summary of encryption techniques for devices of different classes

-	*Class 1*		*Class 2*		*Class 3*	
Class 1	1	Elliptic-curve Diffie-Hellman (ECDH)	1	Elliptic-curve Diffie-Hellman (ECDH)	1	Elliptic-curve Diffie-Hellman (ECDH)
	2	RC5	2	RC5	2	RC5
	3	Key-policy attribute-based encryption (KP-ABE)	3	Key-policy attribute-based encryption (KP-ABE)	3	Key-policy attribute-based encryption (KP-ABE)
Class 2	1	Elliptic-curve Diffie-Hellman (ECDH)	1	AES-128 with key sharing mechanism	1	AES-128 with key sharing mechanism
	2	RC5	2	ABE (attribute-based encryption on RSA key)	2	ABE (attribute-based encryption on RSA key)
	3	Key-policy attribute-based encryption (KP-ABE)	3	HEIGHT	3	HEIGHT
			4	PRESENT	4	PRESENT
Class 3	1	Elliptic-curve Diffie-Hellman (ECDH)	1	AES-128 with key sharing mechanism	1	Public key infrastructure (PKI) using digital certificates
	2	RC5	2	ABE (attribute-based encryption on RSA key)	2	RSA with key sharing mechanism
	3	Key-policy attribute-based encryption (KP-ABE)	3	HEIGHT	3	Key management protocol (with implicit certificates)
			4	PRESENT	4	DTLS using public certificates

6 Conclusions

For the devices in class 1 if the data transfer rate/throughput for a device is very high, then RC5 proved to be an efficient technique in the scenario. Whereas for the devices sending less amount of data, ECDH can be used to transmit it securely. For the class 2 devices if they need to send a large amount of data in short intervals, then AES proved to be the best technique for the purpose. Whereas if the amount of data to be transmitted is less then PRESENT can be used for the purpose. Similarly for the devices belonging to class 3, if the amount of data to be transmitted is considerable then RSA can be used for the purpose as it is very fast in encryption/decryption and is efficient and secure. Whereas if the amount of data to be transmitted is less than PKI, KMP (with implicit certificates) or DTLS (using public certificates) can be used to ensure secure transmission of data.

7 Future scope

The work on the following can be done in the future:

- Middleware can be used for performing the functions of encryption and decryption when connected to class 1 devices.
- Adding more suitable encryption techniques for interaction between different classes.
- Reduction of overhead time for the whole process using encryption.
- Secure, efficient, and robust key sharing mechanism can be used.

References

Alaba, F.A., Othman, M., Hashem, I.A.T. and Alotaibi, F. (2017) 'Internet of things security: a survey', *Journal of Network and Computer Applications*, Vol. 88, pp.10–28.

Atat, R., Liu, L., Wu, J., Li, G., Ye, C. and Yang, Y. (2018) 'Big data meet cyber-physical systems: a panoramic survey', *IEEE Access*, Vol. 6, pp.73603–73636.

Chakrabarty, S. and Engels, D.W. (2016) 'A secure IoT architecture for smart cities', in *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp.812–813, IEEE.

Conti, M., Dehghantanha, A., Franke, K. and Watson, S. (2018) 'Internet of things security and forensics: challenges and opportunities', *Future Generation Computer Systems*, January, Vol. 78, Part 2, pp.544–546.

Deogirikar, J. and Vidhate, A. (2017) 'Security attacks in IoT: a survey', in *2017 International Conference on ISMAC (IoT in Social, Mobile, Analytics and Cloud)*, IEEE, pp.32–37.

Doukas, C., Maglogiannis, I., Koufi, V., Malamateniou, F. and Vassilacopoulos, G. (2012) 'Enabling data protection through PKI encryption in IoT m-health devices', in *2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE)*, IEEE, pp.25–29.

Granjal, J., Monteiro, E. and Silva, J.S. (2015) 'Security for the internet of things: a survey of existing protocols and open research issues', *IEEE Communications Surveys & Tutorials*, Vol. 17, No. 3, pp.1294–1312.

Guo, J., Chen, R. and Tsai, J.J. (2017) 'A survey of trust computation models for service management in internet of things systems', *Computer Communications*, Vol. 97, pp.1–14.

Haroon, A., Shah, M.A., Asim, Y., Naeem, W., Kamran, M. and Javaid, Q. (2016) 'Constraints in the IoT: the world in 2020 and beyond', *Constraints*, Vol. 7, No. 11, pp.252–271.

Hossain, K., Rahman, M. and Roy, S. (2019) 'IoT data compression and optimization techniques in cloud storage: current prospects and future directions', *International Journal of Cloud Applications and Computing*, Vol. 9, No. 2, pp.43–59.

Jiang, F., Fu, Y., Gupta, B.B., Lou, F., Rho, S., Meng, F. and Tian, Z. (2018) 'Deep learning based multi-channel intelligent attack detection for data security', *IEEE transactions on Sustainable Computing*, Vol. 5, No. 2, pp.204–212.

Jing, Q., Vasilakos, A.V., Wan, J., Lu, J. and Qiu, D. (2014) 'Security of the internet of things: perspectives and challenges', *Wireless Networks*, Vol. 20, No. 8, pp.2481–2501.

Khan, M.A. and Salah, K. (2018) 'IoT security: review, blockchain solutions, and open challenges', *Future Generation Computer Systems*, Vol. 82, pp.395–411.

Panwar, M. and Kumar, A. (2015) 'Security for IoT: an effective DTLS with public certificates', in *2015 International Conference on Advances in Computer Engineering and Applications*, IEEE, pp.163–166.

Sciancalepore, S., Capossele, A., Piro, G., Boggia, G. and Bianchi, G. (2015) 'Key management protocol with implicit certificates for IoT systems', in *Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems*, ACM, pp.37–42.

Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A. (2015) 'Security, privacy and trust in internet of things: the road ahead', *Computer Networks*, Vol. 76, pp.146–164.

Singh, N. and Vardhan, M. (2019) 'Distributed ledger technology based property transaction system with support for IoT devices', *International Journal of Cloud Applications and Computing*, Vol. 9, No. 2, pp.60–78.

Singh, S., Sharma, P.K., Moon, S.Y. and Park, J.H. (2017) 'Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions', *Journal of Ambient Intelligence and Humanized Computing*, pp.1–18.

Suo, H., Wan, J., Zou, C. and Liu, J. (2012) 'Security in the internet of things: a review', in *2012 International Conference on Computer Science and Electronics Engineering*, IEEE, Vol. 3, pp.648–651.

Tewari, A. and Gupta, B.B. (2018) 'Security, privacy and trust of different layers in internet-of-things (IoTs) framework', *Future Generation Computer Systems*, Vol. 108, pp.909–920.

Tsai, K-L., Huang, Y-L., Leu, F-Y., You, I., Huang, Y.L. and Tsai, C-H. (2018) 'AES-128 based secure low power communication for LoRaWAN IoT environments', *IEEE Access*, Vol. 6, pp.45325–45334.

Wang, X., Zhang, J., Schooler, E.M. and Ion, M. (2014) 'Performance evaluation of attribute-based encryption: toward data privacy in the IoT', in *2014 IEEE International Conference on Communications (ICC)*, IEEE, pp.725–730.

Wu, J., Guo, S., Huang, H., Liu, W. and Xiang, Y. (2018) 'Information and communications technologies for sustainable development goals: state-of-the-art, needs and perspectives', *IEEE Communications Surveys & Tutorials*, Vol. 20, No. 3, pp.2389–2406.

Wu, J., Guo, S., Li, J. and Zeng, D. (2016) 'Big data meet green challenges: big data toward green applications', *IEEE Systems Journal*, Vol. 10, No. 3, pp.888–900.

Yan, Z., Zhang, P. and Vasilakos, A.V. (2014) 'A survey on trust management for internet of things', *Journal of Network and Computer Applications*, Vol. 42, pp.120–134.

Yao, X., Chen, Z. and Tian, Y. (2015) 'A lightweight attribute-based encryption scheme for the internet of things', *Future Generation Computer Systems*, Vol. 49, pp.104–112.