Secure Key-distribution in IoT Cloud Networks

Soumya Ranjan Moharana, Vijay Kumar Jha, Anurag Satpathy
Department of Computer Science and Engineering
Birla Institute of Technology, Mesra, India
{soumya.moharana92, anurag.satpathy}@gmail.com,
vkjha@bitmesra.ac.in

Sourav Kanti Addya, Ashok Kumar Turuk, Banshidhar Majhi
National Institute of Technology, Rourkela, India.
{kanti.sourav, akturuk, bmnitr}@gmail.com

***Abstract*—Internet of Things (IoT) cloud networks is itself a pervasive idea where all the physical objects are connected over the internet and are allocated with special self-identifying ability to discover other potential objects to transmit data over the internet. The most important shortcoming of IoT cloud networks which needs immediate addressing is the issue of IoT nodes when used within a virtual network of a cloud system. The IoT nodes often communicate over a virtual network and this communication needs to be monitored and managed by the cloud service provider (CSP). This CSP needs to make sure that no IoT node with malicious intent can thrive in such a network. In this paper we propose a framework for the security over virtual network for IoT nodes in a cloud system. Firstly, we propose a secure key management protocol between the CSP and the user group having the IoT nodes using a balanced incomplete block design (BIBD) model. Secondly, we device a lightweight cryptographic technique involving a key exchange protocol to establish a secure end-to-end communication between the IoT nodes. Finally we measure the efficiency and resiliency of the distribution using different metrics.**

***Index Terms*—Internet of Things, Cloud Computing, BIBD, Lightweight cryptography, communication channel**

I. Introduction

The era of cloud computing has brought with it several new methodologies to use the smart devices and objects in our day to day life paving its way towards the Internet of Things (IoT) cloud networks. This enables the use of embedded technology which in turn helps it to easily interact and share information with the external environment by the help of internet. Despite all the positive influence that the IoT cloud network has garnered since its arrival, one cannot simply rule out the risks that accompany this technology which turns out to be a hindrance in its adoption. Security issues in IoT cloud networks are especially concerned with the communication security and end-user privacy protection. In this scenario there is always a possibility that a non-malicious user may share the same network as a malicious user. The traffic generated by a malicious user can cause a degradation in the performance of other sensors and can also cause erroneous billings when it comes to other nodes in the virtual network [1]–[3].

The cloud service provider (CSP) plays an important role in monitoring and controlling the traffic generated by various IoT nodes. There are various issues that make traffic management a headache for the CSP such as confidential information of a usergroup is not to be shared with the CSP and the CSP has to support IoT nodes mobility which makes traffic management a very cumbersome task [2].

The basic idea behind the work is to establish a secure communication between the cloud service provider and the IoT nodes that are placed within different user groups in different virtual networks. There exist a communication between the cloud service provider and the user groups over a public chan-nel. The user groups are thus assigned tasks among themselves by the CSP. There can also be an instance where the IoT nodes placed in one user group would like to communicate with different IoT nodes placed in other user group in different virtual network; this particular communication among the CSPs and user groups may be intercepted while they are being transmitted over a public channel.

Thus the proposed architecture provides a key management policy of the IoT nodes using BIBD (Balanced Incomplete Block Design) approach where the key is distributed from a key pool by the CSP to the different user groups over an secure communication channel [4]. The distributed valid keys are further taken into consideration for a lightweight cryptographic encryption and decryption in order to establish a secure end-to-end communication among the IoT nodes in their respective usergroups [5].

The remainder of the paper is organized as follows: Section II outlines related work. Section III discusses certain preliminaries about the concepts used. Section IV describes the distribution model along with the problem definition and its constraints. Section V outlines the results of the simulation. Finally, section VI concludes and provides future work for the paper.

II. Related Work

Many existing works on cloud computing have given emphasis on different issues which is encountered on a regular basis. These issues can be further grouped into storage security issues, and process and memory security issue. Furthermore many works on IoT nodes in cloud system has been imple-mented which basically is concerned about the inconsistencies and overhead issues.

As we all know cloud computing provides on demand services over the Internet using a large amount of virtual storage. In cloud computing the users are not necessarily required to have a setup of costly big-budget computing infrastructure. Though cloud computing has several advantages, but changes

978-1-5090-4929-5©2017 IEEE

TABLE I
SYMBOL TABLE

Symbol	Description
X	Set of IoT nodes
A	Multiset of Non-Empty subsets of IoT nodes
v	No. of points
λ	Pair of distinct points
k	Block size
b	Total blocks possible
r	Replication no. of BIBD
n	Total number of user groups
α	Key for IoT node A
β	Key for IoT node B
M	Private Key of IoT node A
C	Private Key of IoT node B
$P K_A$	Public Key of IoT node A
$P K_B$	Public Key of IoT node B
SK_A	Shared Secret Key of IoT node A
SK_B	Shared Secret Key of IoT node B

to local computing has brought forward many security issues and challenges for both the consumer and provider. Singh proposes a work that tells about the basic of cloud computing, security issues related to the cloud environment and also focusses on various research issues related to cloud security [1]. Jeong in his survey work [6] presented a complete overview of the security issues relating to cloud computing suggesting a 3-tier security architecture. In his work Zhang suggested different algorithms and analysed them systematically to tackle the security issues in a cloud environment by studying close to 150 articles also hereby discussing various other methods [7]. Varadharajan in [8] used a flexible security as a service as a part of the security services that a CSP can provide to an individual.

Since the migration of IoT into cloud system, works in [9] suggests a specific solution for supporting IoT in cloud. [3] provides a detailed information regarding the existing IoT cloud service providers as well as discusses various pros and cons in a very concrete manner. Works in [10] discusses the importance of cloud computing, autonomous control, artificial intelligence with regard to IoT as well as sheds some light upon the need of synchronization of the Internet, wireless sensors and actuators for successfully implementing new tech-nologies in IoT cloud networks. Whenever IoT cloud network is mentioned a new type of distributed system consisting of smart objects, sensors and actuators come into mind. Thus [11] suggests a lightweight alternative for hypervisor-based approach that can be implemented on devices to enhance the IoT cloud service provisioning. [12] suggests an approach for implementing virtualization framework using SicthSense cloud platform to get satisfactory evaluation results on metrics such as maximum availability and probability of failure on demand.

On the security front for IoT devices in cloud, work [13] suggests an architecture and unique security and privacy requirements for next gen mobile technologies on cloud based IoT by identifying and addressing the issues of secure packet forwarding and privacy preservation. [14] focusses on 20 different security considerations for IoT nodes in regard to cloud tenants, end-users and CSPs working across a range of prolific IoT technologies. End-to-End security and key establishment schemes as well as their limitations have been discussed in [15]. [16] suggests the use of cryptosystems such as RSA, ECC, ECDH to provide security for lo power devices with the help of small key sizes. [17] basically implements various methodologies using cryptosystems for a secure end-to-end communication of resource constrained IoT nodes in healthcare systems.

However these works do not in any way suggest how to minimize the influence of the IoT nodes traffic in a cloud network and how to distribute the secure key from the CSP to the different user-groups. Our proposed architecture is mainly concerned for the external traffic that is present assuming that the internal traffic communication among the sensors within a user-group is secure. Thus the main distribution of secure keys from the CSP to the user-groups IoT nodes is our main concern.

III. PRELIMINARIES

A BIBD (Balanced Incomplete Block Design) is an incomplete block design where all pairs of treatments occur together within a block an equal number of times λ. These applications come from many areas including experimental design, finite testing, software testing, cryptography, and algebraic geometry. Let v, k, and λ be positive integers such that $v > k <= 2$. A (v, k, λ) balanced incomplete block design is a design (X, A) such that the following properties are satisfied :

i. $|X| = v$,
ii. Each block contains exactly k points, and
iii. Every pair of distinct points is contained in exactly λ block.

Where, X is a set of elements called points, and A is a collection (i.e. multi-set) of non-empty subsets of X called blocks. Item number iii mentioned above is the balance property of the BIBD. It is thus called incomplete because $k < v$, and hence all its block are incomplete. Generally, a BIBD is an arrangement of v distinct objects into b blocks such that each block contains exactly r different blocks, and every pair of distinct object occurs together in exactly λ blocks. The design thus can be expressed as (v, k, λ), or equivalently (v, b, r, k, λ), where: $λ(v − 1) = r(k − 1)$ and $b.k = v.r$. Following is an example of (7, 3, 1) BIBD: v = Number of set of elements called points. k = Each block contains exactly k points. λ = Every pair of distinct point is contained in exactly λ blocks [18].

A. Evaluation of efficiency

A few metrics can be used to calculate the efficiency of the key distribution [18]. They are:

i. **Scalability**:The network should support post-deployment. User groups can be added after the system is set up and running.
ii. **Resiliency**: Resistance against malicious activities e.g. compromised key. The key may be compromised fully or

978-1-5090-4929-5©2017 IEEE

partially. The resiliency of a network can be determined in two different ways:

a. *E(nodes)*: This can be calculated as:

$$E(nodes) = \frac{Number\ of\ links\ compromised}{Total\ number\ of\ communication\ links} \quad (1)$$

b. V (nodes): This can be calculated as:

$$V(nodes) = \frac{Number\ of\ nodes\ compromised}{Total\ number\ of\ nodes} \quad (2)$$

IV. Proposed Architecture

The proposed architecture provides a very simple and efficient way of communication between the CSP and the user groups as well as among different user groups. The CSP contains a key pool i.e., $\{1, 2, 3, \cdots, n\}$. The CSP uses a BIBD approach to generate the total valid unique keys. Using the BIBD approach the generated keys from the key pool is distributed among the user groups over a secure communication channel. A key generated is in fact a composition of many subkeys. A key is represented as $k = \{k_1, k_2, \cdots, k_n\}$. By using such a key '$k$' we can establish secure communication with 'n' different user groups in the cloud. This architecture has been explained in Figure 1. Every user group has a gateway node that keeps track of all the external and internal communication using a routing table. All the external traffic has to pass through the gateway node of the respective group. The classification of the traffic as internal, external is done by the IoT gateway node of the respective group. This can be easily done by examining the destination IP of the packets. If the destination IP is of any IoT node that belongs to the same group then the traffic can be easily deemed as internal, for all other cases the traffic is external. The security for an intra-group communication is left to the user groups.

A. Security Concerns

The concerns related to security issues in IoT nodes in such environment are:

i. IoT devices lack an user interface (UI) which makes them more vulnerable towards different IoT viruses i.e., there can be no knowledge beforehand whether or not the IoT devices are being attacked by any attackers or not.

ii. TCP/UDP sockets are required to configure the IoT devices in order to gain access to a network. The issue here is the use of same access strategy across all devices making it to share a common password across all other devices within a network. Thus it makes life difficult on the part of consumers to remember various passwords which results in leaving the password set to default, using any brute force technique the attacker can get an easy access to the network.

iii. IoT devices do not support any firewalls or diagnostic tools because of their limiting computational capability.

iv. One key mistake manufacturers make is they're pushing their devices to connect directly to the internet over Wi-Fi. The right thing to do would be to use a simpler protocol like ZigBee within the premise and then have an aggregated feed through a secure gateway.

B. Traffic Types

The entire traffic generated in the model can be classified into two categories:

i. **Internal Traffic:** The traffic generated due to the commu-nication or exchange of information between IoT nodes of the same user group.

ii. **External Traffic:** The traffic generated due the communication or exchange of information between IoT nodes of different user groups.

C. Motivating Example

Let us say there are three user clouds/ user groups namely G_1,G_2,G_3. The key size $KSZ > 1$ is represented as $1 > KSZ <= |n|$. Let the key size KSZ here is 2. The key array generated here for the respective groups are (1, 2), (1, 3), (2, 3). These keys are distributed distributed to their respective groups over an secure channel. For instance the key array available with G_1 enables it to establish secure communication with G_2 and G_3 using keys 1 and 2 respectively.

D. Security Module

This is the security module which will be used for the work. Using the BIBD model the key management is efficiently done among the user groups making it difficult for any attacker to get to know the secret keys. It thus becomes evident that the IoT gateway nodes in figure:1 takes care of the internal traffic or the communication that takes place within the user groups. Further proceedings will show how the secret keys are used in an end-to-end secure communication among the IoT nodes.

It is very important to form an efficient method for a secure end-to-end communication or transmission of data from one IoT node to others. It thus requires efficient key distribution scheme which will enable the nodes to interact with each other. Since the IoT nodes being used are low power devices and have limited resources, making them vulnerable to inconsistencies and overhead issues. The main motivation of the security module is to clearly ensure secrecy and integrity of messages that are communicated among IoT nodes as well as the messages that are being exchanged among the nodes. As IoT nodes are low power devices they have intrinsically restricted resources in regard to the processing power, memory, communication bandwidth, and energy. While providing security constraints in IoT nodes one must keep in mind to use cryptographic methods that do not affect the performance of the IoT nodes in cloud networks. In many cases the IoT nodes act differently as a client and as a server opposite to the wireless sensor nodes. This implies that providing security becomes a cumbersome task involving only the two members present at the ends in the pairwise key exchange phenomenon having an access to a mutually agreed upon shared secret key. On the basis of mutual authentication, these two nodes should

978-1-5090-4929-5©2017 IEEE

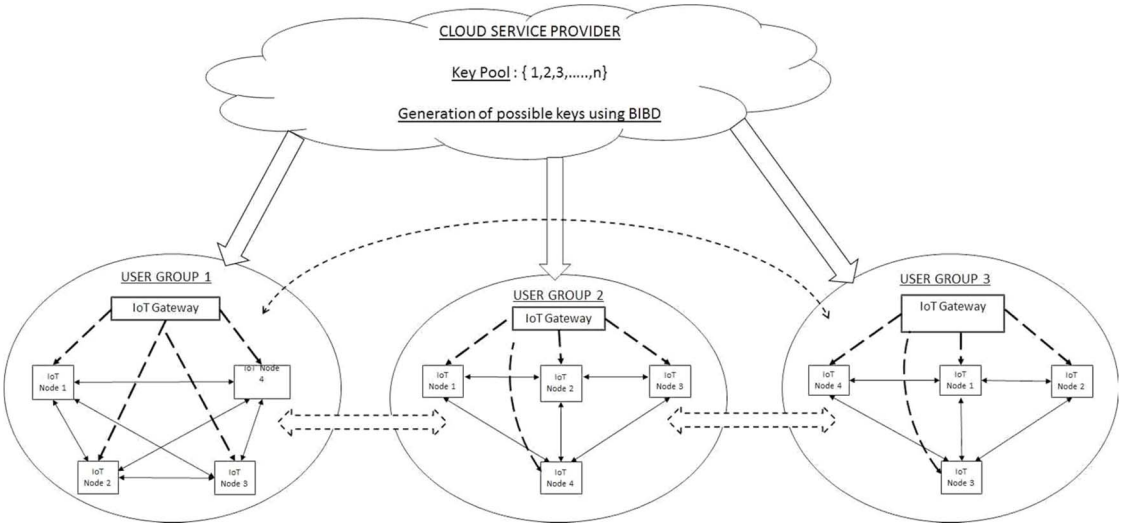

Fig. 1. **Proposed Model**

Algorithm 1: Diffie-Hellman Key Exchange for IoT nodes in cloud networks

1 Two numbers (keys) α and β are selected from the valid key pool formed from the BIBD procedure for IoT Nodes A and B which is made known to both of them.
2 IoT Node A picks up a secret number '*M*' (random number) which is regarded as its private key/value such that $M < \alpha$; IoT node A then calculates its public key $PK_A = \alpha^M \bmod \beta$ and sends it to IoT node B.
3 IoT Node B picks up a secret number '*C*' (random number) which is its own private key/value such that $C < \alpha$; IoT node B calculates its public key $PK_B = \alpha^C \bmod \beta$ and sends it to IoT node A.
4 Upon receiving their respective public keys PK_A and PK_B from each other both the IoT nodes calculate their shared key i.e., $SK_A = PK_B^M \bmod \beta$ and $SK_B = PK_A^C \bmod \beta$.
5 Thus the shared secret key $SK = SK_A = SK_B$ is found and it is known to the communicating IoT nodes only.

also authenticate each other and link the generated shared key among themselves.

The main protocol that the paper follows with this security module is to establish shared secret keys in a very secure and efficient way to provide confidentiality and authentication while exchanging data among themselves. Thus a lightweight cryptographic technique involving the Diffie-Hellman (DH) key exchange is used which in turn is not that a complex procedure to implement. This methodology involves selection of two keys in the cryptosystem which in turn establishes a secure connection between two IoT nodes and helps in the communication process over an insecure channel. This DH algorithm uses a public key distribution scheme to se-curely establish a common secret key known to only the two

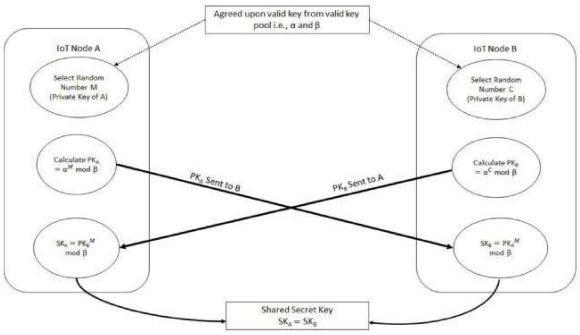

Fig. 2. **Diffie-Hellman Key Establishment Protocol**

communicating IoT nodes. DH key establishment protocol is illustrated below in the Figure 2. In order to implement DH algorithm it is very important on the part of the communicating IoT nodes to agree upon two numbers that are made known to each other from the respective valid key pool generated from the BIBD procedure. After this both the IoT nodes choose their respective secret values *'M'* and *'C'* (random numbers known as respective private keys). Using the secret values we calculate their respective public values to exchange with each other. After the exchange of public values shared secret key can be obtained at both the nodes by using a modular computa-tion given as $SK_A = PK_B^M \bmod \beta$ and $SK_B = PK_A^C \bmod \beta$. On getting the shared secret key encryption of the message takes place that is sent from IoT node A to IoT node B by XORing with the shared secret key. On the receiving end the decryption process is also the same the cipher text is decrypted by XORing with the secret key.

V. Simulation Results and Discussion

The proposed models were implemented using a program-ming model. An in-house simulation is done on a desktop system with Intel (R) Core (TM) i5-2430M processor with

978-1-5090-4929-5©2017 IEEE

TABLE II
RESILIENCY METRIC E(S) FOR USER-GROUPS IN CLOUD NETWORKS

	10%	20%	30%	40%
v=7,k=3,λ=1	0.428	0.428	0.714	0.857
v=10,k=3,λ=1	0.343	0.656	0.75	0.937
v=15,k=3,λ=1	0.407	0.648	0.703	0.944
v=20,k=3,λ=1	0.417	0.656	0.895	0.91

TABLE III
RESILIENCY METRIC V (S) FOR USER-GROUPS IN CLOUD NETWORKS

	10%	20%	30%	40%
v=7,k=3,λ=1	0.142	0.142	0.285	0.428
v=10,k=3,λ=1	0.1	0.2	0.3	0.4
v=15,k=3,λ=1	0.153	0.23	0.307	0.461
v=20,k=3,λ=1	0.133	0.2	0.333	0.428

2.40 GHz and 4 GB memory. The simulation is shown for the generation of unique keys from various cases of key pool sizes such as 7,10,15,...,1000. Now these key groups are divided into a key-chain length of 3 having a unique distinct pair of keys. Since we have considered the test parameters to be small enough to resemble real life scenarios, the key chain length can thus be extended to more than 3 satisfying the required parameters in future use.

In order to proceed with the calculation we must well be aware of the metrics that are needed for key management scheme. One of the most important metrics being the resiliency against node capture, i.e adaptability and sustainability of the nodes when they are compromised by attacker. There are two kinds of resiliency that arises viz., *E(s)* and *V(s)*.

From the given Table II and III ,we have showed the E(S) and V(S) values for the percentage compromise in the unique key pool. Let us assume if V(total keys that are considered) = 7, k(key-chain length) = 3, λ(unique no. of distinct key pair) = 1 gives us the unique E(S),V(S) values for the respective 10%,20%,30%,40% of the compromised unique keys. In order to calculate the E(S) and V(S) we had to first find out the total number of communication links that were possible taking into consideration the datasets. If we consider the above scenario of V=7, k=3 and λ=1, we find that the total communication links possible will be 35. Out of the total communication links we will consider the only 21 communication links from the valid 7 nodes that is possible.

A. Security Analysis: Key Exchange Protocol

Assuming that the communication protocol among the IoT nodes is done through trusted devices, the possibility of Denial of Service (DoS) attacks from any compromised IoT nodes is avoided by implementing the used key establishment protocol. The protocol also provides with the confidentiality factor for the exchanged data between different IoT nodes involved. Since resource-constrained IoT nodes are involved in lightweight cryptography i.e, no use of large asymmetric encryption there by minimising the overheads of key establishment to very low hence making it more secure and efficient.

B. Security Analysis: Resisting against MITM Attack

Since there is encryption of the keys using the private keys of the IoT nodes, it becomes difficult for man-in-the-middle (MITM) and eavesdropping attacks to determine any confidential information since the use of DH key exchange ensure discrete logarithm problem which makes it near to impossible to get the private keys from the encrypted public keys. Thus forward secrecy is maintained.

VI. CONCLUSION

In this paper, we addressed the issue of secure key-distribution in IoT cloud networks thereby reducing the infection between the usergroups within a IoT cloud network as well as managing the traffic for communication among the usergroups and IoT nodes present inside them. Using a BIBD approach the key management has been efficiently done among the usergroups. On the security analysis part, we have used Diffie-Hellman algorithm for features like less power consumption, lightweight and robust nature which is a very novel approach for IoT nodes. Thus security analysis and performance evaluation prove to be one of the major improvements as well as the resiliency of the IoT nodes against well known attacks.

Moreover, the security protocol implemented is lightweight in nature taking into energy consumption of IoT nodes into account thereby enabling this methodology to be employed upon different IoT gadgets and applications. We also intend to show the full communication among the different IoT nodes within a cloud network in our future work. We also intend to implement and extend this protocol on actual hardware and find out its resiliency and efficiency to different security threats.

REFERENCES

[1] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88 – 115, 2017.

[2] J. S. Yang and H. K. Choi, "Ip based security architecture of virtual network in cloud computing system," in *2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2012, pp. 709–715.

[3] P. P. Ray, "A survey of iot cloud platforms," *Future Computing and Informatics Journal*, pp. –, 2017.

[4] J. Lee and D. R. Stinson, *Deterministic Key Predistribution Schemes for Distributed Sensor Networks*. Springer Berlin Heidelberg, 2005, pp. 294–307.

[5] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," *IEEE Des. Test*, vol. 24, no. 6, pp. 522–533, Nov. 2007.

[6] S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200 – 222, 2016.

[7] J. Zhang, H. Huang, and X. Wang, "Resource provision algorithms in cloud computing: A survey," *Journal of Network and Computer Applications*, vol. 64, pp. 23 – 42, 2016.

[8] V. Varadharajan and U. Tupakula, "Security as a service model for cloud environment," *IEEE Transactions on Network and Service Management*, vol. 11, no. 1, pp. 60–75, 2014.

978-1-5090-4929-5©2017 IEEE

[9] A. Iera, G. Morabito, and L. Atzori, "The internet of things moves into the cloud," in *2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW)*, 2016, pp. 191–191.

[10] H. N. Saha, A. Mandal, and A. Sinha, "Recent trends in the internet of things," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, 2017, pp. 1–4.

[11] A. Celesti, D. Mulfari, M. Fazio, M. Villari, and A. Puliafito, "Exploring container virtualization in iot clouds," in *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2016, pp. 1–6.

[12] K. S. Dar, A. Taherkordi, and F. Eliassen, "Enhancing dependability of cloud-based iot services through virtualization," in *2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2016, pp. 106–116.

[13] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based iot: Challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, 2017.

[14] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty security considerations for cloud-supported internet of things," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 269–284, 2016.

[15] Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Lightweight collaborative key establishment scheme for the internet of things," *Computer Networks*, vol. 64, pp. 273 – 295, 2014.

[16] T. K. Goyal and V. Sahula, "Lightweight security algorithm for low power iot devices," in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2016, pp. 1725–1729.

[17] M. A. Iqbal and M. Bayoumi, "Secure end-to-end key establishment protocol for resource-constrained healthcare sensors in the context of iot," in *2016 International Conference on High Performance Computing Simulation (HPCS)*, 2016, pp. 523–530.

[18] D. R. Stinson, *Combinatorial Designs: Constructions and Analysis*. SpringerVerlag, 2003.

978-1-5090-4929-5©2017 IEEE