Journal of Engineering Sciences

Vol 12, Issue 06, JUNE /2021
ISSN NO:0377-9254

Secure IoT Environments with Dynamic Access Control in using Cluster Significant Controlling Decentralized Insubstantial

SUBHASHINI CHILAKALA, SINDHU POTHURAJU, SWATHI BADIREDDY, M.N MALLIKARJUNA REDDY, Dr.G RAJESH CHANDRA
DEPT OF CSE
SVR ENGINEERING COLLEGE, NANDYAL

ABSTRACT

Rapid growth of Internet of Things (IoT) devices dealing with sensitive data has led to the emergence of new access control technologies in order to maintain this data safe from unauthorized use. In particular, a dynamic IoT environment, characterized by a high signaling overhead caused by subscribers' mobility, presents a significant concern to ensure secure data distribution to legitimate subscribers. Hence, for such dynamic environments, group key management (GKM) represents the fundamental mechanism for managing the dissemination of keys for access control and secure data distribution. However, existing access control schemes based on GKM and dedicated to IoT are mainly based on centralized models, which fail to address the scalability challenge introduced by the massive scale of IoT devices and the increased number of subscribers. Besides, none of the existing GKM schemes supports the independence of the members in the same group. They focus only on dependent symmetric group keys per subgroup communication, which is inefficient for subscribers with a highly dynamic behavior. To deal with these challenges, we introduce a novel Decentralized Lightweight Group Key Management architecture for Access Control in the IoT environment (DLGKM-AC). Based on a hierarchical architecture, composed of one Key Distribution Center (KDC) and several Sub Key Distribution Centers (SKDCs), the proposed scheme enhances the management of subscribers' groups and alleviate the rekeying overhead on the KDC. Moreover, a new master token management protocol for managing keys dissemination across a group of subscribers is introduced. This protocol reduces storage, computation, and communication overheads during join/leave events. The proposed approach accommodates a scalable IoT architecture, which mitigates the single point of failure by reducing the load caused by rekeying at the core network. DLGKM-AC guarantees secure group communication by preventing collusion attacks and ensuring backward/forward secrecy. Simulation results and analysis of the proposed scheme show considerable resource gain in terms of storage, computation, and communication overheads.

I. INTRODUCTION:

IoT has been introduced as a universal and ubiquitous paradigm that connects transparently and seamlessly a multitude of digital devices to the Internet [1]. Recently, IoT devices are progressively becoming a large part of people's daily lives. They are widely used in various kinds of applications, such as environmental sensing and industrial monitoring (e.g., smart city, smart hotel, smart office, industry 4.0) [1]. A generic IoT network architecture, as shown in Fig.1, is composed of a set of physical objects (i.e., smart things) that are interconnected to exchange and collect data over the Internet. [2] has predicted that, by 2025, more than 41.6 billion connected IoT devices will be used worldwide. These smart things form a diverse and heterogeneous network of interconnected physical objects with a wide range of functionalities and requirements; one essential feature being data collection.

The vast majority of IoT devices have minimal resources, in terms of computation, communication, and storage, preventing them from efficiently performing cryptographic operations, thus rising more security challenges. Indeed, large scale IoT deployments still face serious security issues that still need to be addressed, such as authentication, privacy preservation, and data integrity [3][4]. In order to safeguard IoT data from tampering and

unauthorized access, an appropriate scheme for access control is more crucial than ever. To ensure this, GKM is one promising approach, which would be used to provide access control to data streams for legitimate users only [4]. In other words, it consists of creating a group key that will be shared between a device's group and its current subscribers, such that the device can encrypt its data, and only the subscribers can decrypt it. This mechanism is suitable for IoT environments as it does not require a trusted third entity. This can be achieved through a publish subscribe messaging model, such as MQTT [5]. member's group can intermittently join and leave the system (e.g., reservation IoT systems), safeguarding IoT data from unauthorized access represents a primordial security issue. Therefore, enforcing access control is reduced to solving the GKM problem.

Moreover, in order to guarantee backward and forward secrecy, the shared keys need to be changed whenever a new member joins or an existing one leaves its group [6]. To efficiently reduce the overhead keys management, resulting mainly from rekeying, GKM is extensively studied in theliterature [12]. Most of the existing GKM schemes are not suitable for IoT applications. Indeed, existing GKM for IoT applications are designed to manage communication within a single group, and the GKM schemes introduced for access control in the IoT environment are mostly based on a centralized access management architecture. Consequently, they are not suitable for a scalable and dynamic IoT environment comprising multiple groups. In fact, many users can subscribe to numerous services offered by different IoT devices and change their interest frequently over time.

Thus, maintaining an efficient GKM in a dynamic IoT environment remains a challenging issue due to the rekeying process that affects all members in the same group for joining/leaving events. Therefore, all members should update their shared group access keys. Hence, an efficient group key mechanism should be introduced to reduce the rekeying dependence of members in the same group, and thus reducing overhead. To solve the rekeying dependence, minimize resulting overhead and achieve scalable access management for dynamic IoT environment, this work introduces a new Decentralized Lightweight Group Key Management Architecture for Access Control named DLGKM-AC. We consider in our use-case, in the context of the European project PARFAIT [28], an extensive reservation system for franchise hotels. In this scenario, key cards and smartphones might be interchangeably used to give access permissions for guests in different rooms. They can also be used to control the usage of various facilities according to room classes' and purchased services. When a guest checks out, and the room becomes vacant, the devices should stop sending the room's information and receiving information from other devices. The main idea of DLGKM-AC is to create an efficient and flexible mechanism to secure distribution of contents to eligible subscribers.

A hierarchical scheme comprising a central Key Distribution Center (KDC) and several Sub Key Distribution Centers (SKDCs) to manage groups of subscribers and to mitigate the single point of failure issue is introduced. Key management tasks in DLGKM-AC are offloaded to several SKDCs, which allow enhancing the system's performances in terms of computation and communication by reducing the overhead caused by membership changes (join/leave). The KDC manages device groups, while each SKDC manages user groups, which provides scalability for our DLGKM-AC. Furthermore, DLGKM-AC introduces a new key management mechanism that allows reducing the rekeying dependence of users in the same group. DLGKM-AC is a scalable and flexible access management protocol that is based on the GKM mechanism. It improves the computation capability, the storage capacity, and the communication overhead.

The main contributions and novelties of this paper are summarized as follows: - Presenting a new lightweight decentralized keys distribution architecture to ensure forwarding valuable and sensitive information to legitimate users in a scalable and secure manner, - Designing a rekeying mechanism suitable for multiple groups of IoT devices and various users' groups whenever memberships change, which ensures a flexible access management system, - Presenting a master token management algorithm that creates and updates a master token and multiple slave tokens for handling user groups, which achieves the independence of user during the rekeying process, - Ensuring security requirements, backward and forward secrecy even

with changes in users and devices membership, and resisting to the collusion attack, - Minimizing computational and storage overheads for users and IoT devices, and also communication overhead for the overall system, which is proved through extensive analytical study and simulation work.

The remainder of this paper is structured as follows: First, related work is described in Section II. Then, we discuss the necessary background related to our scheme in Section III before presenting the overall system architecture, attacker model and different system requirements in Section IV. The proposed DLGKM-AC for IoT is introduced in Section V. Security and performance analysis in terms of storage, communication and computation overheads are summarized in Section VI. Finally, conclusions and future works are given in Section VII.

II. EXISTING SYSTEM:

- The dynamic nature of group communications makes safeguarding data from unauthorized access a significant challenge. The larger problem of access control is reduced to GKM, where a group key is shared by the group members to define the access permissions. Table I summarizes and classifies existing GKM solutions based on different attributes and criteria as follow: (i) *Environment* of its application, such as wired Internet [6], wireless sensor networks (WSN) [7][9][11], ad hoc networks [8], wireless body area networks (WBAN) [10] and IoT environment [13][14]. *(ii) Network model* that could be centralized, decentralized or distributed. *(iii)*the used *Cryptography types*, and essential security services *(iv) backward secrecy and (v) forward secrecy*, where shared keys need to be updated whenever a new member joins, or an existing one leaves its group. *(vi) Key independence* to ensure the independence of keys from each other. (vii) *Vulnerability to collusion attack* (collaboration of adversaries to compromise a communication) for which rekeying is important to maintain security. However, this process may cause a lot of key management overhead and leads to *(viii) Single point of failure*, especially in a (ix) *Scalable* environment that supports (x) *Multiple group services* and composed of (xi) *Dynamic publishers* and dynamic subscribers. Hence, ensuring (xii) *Subscribers' independence* makes subscribers of one group independent from the entire group in the rekeying process of the group key after a join/leave event in the group.
- Authors in [12] surveyed numerous key distribution schemes over wireless networks and classified them into centralized, decentralized, and distributed schemes. Centralized schemes use only one server known as the key distribution server (KDC) for creating and distributing encryption keys. Distributed schemes do not have a specific KDC; they rather generate group key either in a collaborative manner between the group members or by one member. Moreover, each member must keep track of the other members to make robust communication. Besides, membership change events (join/leave) cause a high processing and communication overheads [25], which may lead to a congestion problem in a dynamic IoT environment. In contrast, decentralized schemes divide the system into several subgroups, thus, reducing the load on the KDC and offering a solution to scalability issues. Furthermore, a subgroup manager is responsible for keeping track of the group's members, which may reduce computation and storage overhead on members. The distribution of encryption keys in the different mentioned GKM architectures is further ensured by using two main cryptographic types (symmetric and asymmetric). Two fundamental and efficient GKM schemes were proposed: The Logical Key Hierarchy (LKH) [15] and the One-way Function Tree (OFT) [16] based on symmetric keys (traffic key and encryption key) to distribute the updated encryption keys. In contrast to LKH, all the OFT implementations suffer from collusion attacks and increase devices' computational overhead for obtaining group keys. Hence,

OFT is far from ideal in an IoT environment, where the communicating devices may have limited computational power.

- Additionally, [20] [21] schemes provided fine-grained access control Attribute-Based Encryption (ABE) to manage keys' update. However, ABE is a cumbersome mechanism that relies on asymmetric cryptography, which is unsuitable for running on resource-constrained IoT devices [22]. Besides, asymmetric encryption mechanisms are also used in key management schemes [23] [24]. Specifically, Porambage et al. [7] proposed a group key establishment protocol for multicast communication by using the Elliptic Curve Cryptographic (ECC) operations. Even though, the latter are known to be suitable for resource-constrained devices; their protocol does not efficiently manage the rekeying process. Furthermore, all previous mentioned schemes are designed for single multicast groups, but users may subscribe to multiple services. To ensure many multicast groups, Park et al. [11] accommodate various services' groups. Their scheme addressed rekeying in the wireless mobile environment, which is based on a centralized architecture and a LKH mechanism to manage multiple communications. Likewise, Mapoka et al. [17] proposed using a distribution list of the session key and key update slot for each subgroup. This list is centrally managed by a node called the area key distributor. The proposed protocol alleviates the 1- affect-n phenomenon and transmission overhead of the core network, but it does not ensure the forward secrecy. Hence, Zhong et al. [18] proposed another protocol called area based multiple GKM that securely provides services when users migrate to different wireless networks, which ensures forward secrecy. Nonetheless, its high overhead, due to revocation events, makes it unsuitable for dynamic IoT environments.

Disadvantages

- There are no dynamic group communication lack of group key management.
- Less security due to the key distribution server (KDC) for creating and distributing low encryption keys .

III. PROPOSED SYSTEM:

In this paper, we propose a decentralized group key management scheme where the numbers of users and devices change frequently. Before presenting the solution, we introduce the overall system, the attacker model and the system requirements. The architecture of the proposed network model, shown in Fig.2, illustrates a typical three-tier scheme used for a smart hotel for our use case scenario. The entire system considers three essential layers: publishers, subscribers and group key manager. The *publisher layer* contains IoT devices, such as smart door locks or IP cameras, collecting and sending data to subscribers. These constrained IoT devices have limited computation, storage and energy resources.

 The *subscriber layer* is composed of a set of users that want to get access to data of the publisher layer. A user can be a device owner with legitimate, full and permanent control or a guest user with only limited access. A user communicates and receives data from IoT devices via his/her smartphone.

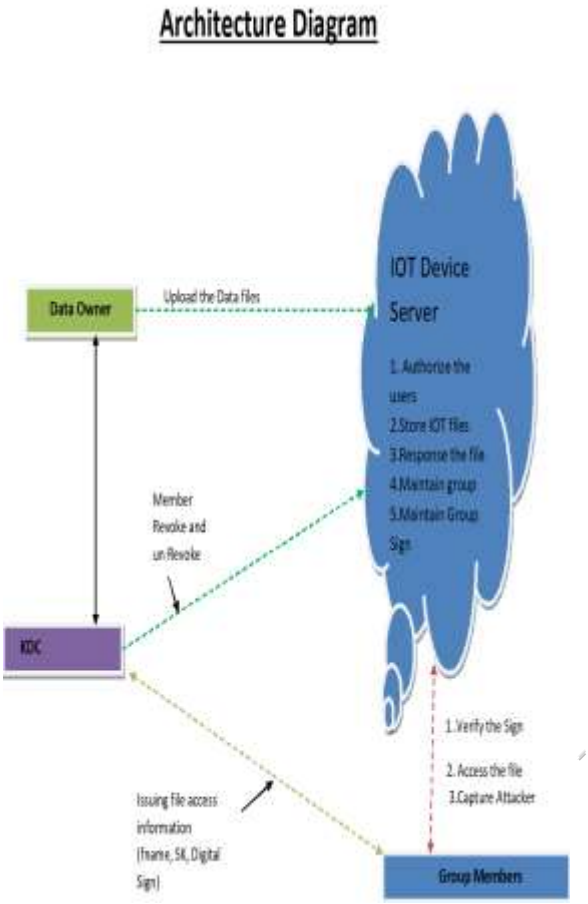
 The *group key manager layer* is responsible for generating the system parameters and managing group members by providing required encryption keys used to control the access to data. The group key manager in our system is considered as a fully trusted third party.

Advantages

- The system is more secure due to introduce a new Decentralized Lightweight Group Key Management Architecture for Access Control named DLGKM-AC.
- DLGKM-AC is to create an efficient and flexible mechanism to secure distribution of contents to eligible subscribers.

Journal of Engineering Sciences
Vol 12, Issue 06, JUNE /2021
ISSN NO:0377-9254

IV. SYSTEM ARCHITECTURE:



V. MODULES:

- **Data Owner(Group Member)**
  In this module, the data owner uploads their data in the IOT server. For the security purpose the data owner encrypts the data file and then store in the IOT. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file.
- **IOT Server**
  The IOT Server manages a IOT to provide data storage service. Data owners encrypt their data files and store them in the IOT for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the IOT and then decrypt them.
- **Data Integrity**
  Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence in general. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.
- **KDC**
  The KDC who is trusted to store verification parameters and offer public query services for these parameters. In our system the Trusted Third Party, view the user data and uploaded to the distributed IOT. In distributed IOT environment each IOT has user data. The Group Manager will perform the revocation and un revocation of the remote user if he is the attacker or malicious user over the IOT data.
- **Data Consumer(End User / Group Member)**

In this module, the user can only access the data file with the encrypted key if the user has the privilege to access the file. For the user level, all the privileges are given by the GM authority and the Data user's are controlled by the GM Authority only. Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges.

VI. SYSTEM SPECIFICATION:

Hardware Requirements:

- System : Pentium IV 3.5 GHz.
- Hard Disk : 40 GB.
- Monitor : 14' Colour Monitor.
- Mouse : Optical Mouse.
- Ram : 1 GB.

Software Requirements:

- Operating system : Windows XP or Windows 7, Windows 8.
- Coding Language: Java – AWT,Swings,Networking
- Data Base : My Sql / MS Access.
- Documentation : MS Office

- IDE : Eclipse Galileo

Development Kit : JDK 1.6

VII. CONCLUSION:

A novel decentralized lightweight group key management for access control in a dynamic IoT environment named DLGKM-AC has been introduced in this paper. A hierarchical architecture is adopted using one KDC, for managing group keys and broadcasting update messages, and several SKDCs, for handling direct communication links between devices and users. Besides, a new master token encryption algorithm has been introduced in order to ensure members' independence in highly dynamic group communication. In DLGKM-AC, mobility is smoothly handled as we provide the backward and the forward secrecy with fewer rekeying operations. Furthermore, our protocol mitigates the 1-affects-n issue. Indeed, users can always get access to data even if one SKDC is affected. Extensive security analysis covering a wide range of desired security properties has also been provided. Additionally, performance analyses shows that our proposed scheme offers better performances by reducing storage, communication, and computation overheads. Finally, adopting a decentralized architecture increases scalability and reduces overhead for resource-constrained devices. As future work, to put it into practice via a proof-of-concept, we are already planning to deploy our architecture in a real-world setting, in the context of the European project PARFAIT [28], by constructing a physical network comprising a set of IoT devices and smart phones as users.

VIII. REFERENCES:

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of
Things for Smart Cities," in IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22-32, Feb. 2014. [2] https://www.helpnetsecurity.com/2019/06/21/connected-iot-devices-forecast/.
[3] M. Dammak, O. R. M. Boudia, M. A. Messous, S. M. Senouci, and C. Gransart, "Token-Based Lightweight Authentication to Secure IoT Networks," 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2019, pp.1-4.

[4] Panagiotis I. Radoglou Grammatikis, Panagiotis G. Sarigiannidis, Ioannis D. Moscholios, Securing the Internet of Things: Challenges, threats, and solutions, Internet of Things, Volume 5, 2019. [5] A. Banks and R. Gupta, "MQTT version 3.1. 1," OASIS standard, 2014.
[6] AlMajed, H.N.; AlMogren, A.S. Simple and Effective Secure Group Communications in Dynamic Wireless Sensor Networks. Sensors 2019, 19,
[7] P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila, and B.Stiller, "Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for IoT applications," IEEE Access, vol. 3, pp. 1503–1511, 2015. [8] A. Mehdizadeh, F. Hashim, and M. Othman, "Lightweight decentralized multicast–unicast key management method in wireless ipv6 networks," Journal of Network and Computer Applications, vol. 42, 2014. [9] Zhu, B.; Susilo, W.; Qin, J.; Guo, F.; Zhao, Z.; Ma, J. A Secure and Efficient Data Sharing and Searching Scheme in Wireless Sensor Networks. Sensors,
2019, 19, 2583. [10] Tan, H.; Chung, I. A Secure and Efficient Group Key Management Protocol with Cooperative Sensor Association in WBANs. Sensors 2018, 18, 3930 [11] M.-H. Park, Y.-H. Park, H.-Y. Jeong and S.-W. Seo, "Key management for multiple multicast groups in wireless networks," IEEE Transactions on Mobile
Computing, vol. 12, no. 9, pp. 1712–1723, 2013. [12] Cheikhrouhou O. Secure Group Communication in Wireless Sensor Networks: A survey. Journal of Network and Computer Applications. [13] Y. Kung and H. Hsiao, "GroupIt: Lightweight Group Key Management for
Dynamic IoT Environments," in IEEE Internet of Things Journal, vol. 5, no. 6, pp. 5155-5165, Dec. 2018. [14] M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, "A decentralized batchbased group key management protocol for mobile internet of things (dbgk)," 2015 IEEE International Conference on Computer and InformationTechnology. [15] H. Harney and E. Harder, "Logical key hierarchy protocol," Internet draft, Tech. Rep., 1999. [16] D. Balenson, D. McGrew, and A. Sherman, "Key management for large

dynamic groups: One-way function trees and amortized initialization,"
[17] T. T. Mapoka, S. J. Shepherd and R. A. Abd-Alhameed, "A New Multiple Service Key Management Scheme for Secure Wireless Mobile Multicast," in IEEE Transactions on Mobile Computing, vol. 14, no. 8, pp. 1545-1559, 1 Aug. 2015. [18] Zhong, H., Luo, W., and Cui, J. (2017) Multiple multicast group key management for the Internet of People. Concurrency Computat.: Pract. Exper. 29:e3817, doi: 10.1002/cpe.3817.
[19] I.-C. Tsai, C.-M. Yu, H. Yokota, and S.-Y. Kuo, "Key management in internet of things via kronecker product," in Dependable Computing (PRDC), 2017 IEEE 22nd Pacific Rim International Symposium on. IEEE, 2017.
[20] W. Ding et al., "An Extended Framework of Privacy-Preserving Computation with Flexible Access Control," in IEEE Transactions on Network and Service Management. TNSM.2019.
[21] M. Nabeel, N. Shang and E. Bertino, "Privacy Preserving Policy-Based Content Sharing in Public Clouds," in IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 11, pp. 2602-2614, Nov. 2013.
[22] X. Wang, J. Zhang, E. M. Schooler, and M. Ion, "Performance Evaluation of Attribute-Based Encryption: Toward Data Privacy in the IoT," in IEEE ICC, 2014.
[23] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia, and G. Bianchi, "Key management protocol with implicit certificates for iot systems," in Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems. ACM, 2015, pp. 37–42.
[24] Y. Tseng, C. Fan and C. Wu, "FGAC-NDN: Fine-Grained Access Control for Named Data Networks," in IEEE Transactions on Network and Service Management, vol. 16, no. 1, pp. 143-152, March 2019.
[25] Karuturi, N. N., Gopalakrishnan, R., Srinivasan, R., & Rangan, C. P. (2008). Foundations of Group Key Management-Framework, Security Model and a Generic Construction. IACR Cryptology EPrint.