Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 7, S. 269-278, 3, 2023
© Telif hakkı IJANSER'e aittir
Araştırma Makalesi

IJANSER
https://as-proceeding.com/index.php/ijanser
ISSN: 2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 7, pp. 269-278, 3, 2023
Copyright © 2023 IJANSER
Research Article

Group key Management in Resource Constraint Environment: Applications and Use Cases

FOUZIA SAMIULLAH [*], SEDAT AKEYLEK [2], MING LEE GAN [3] and Y AUN [4]

[,1,3,4]The Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman, Petaling Jaya, Perak 31900, Malaysia.
[2]Department of Computer Engineering, Ondokuz Mayis University and IAM, METU, Turkey

[*]*(sedat.akleylek@bil.omu.edu.tr) Email of the corresponding author*

(Received: 29 March 2023, Accepted: 15 April 2023)

(2nd International Conference on Engineering, Natural and Social Sciences ICENSOS 2023, April 4 - 6, 2023)

ATIF/REFERENCE: Samiullah, F., Akeylek, S., Gan, M. L. & Aun, Y. (2023). Group key Management in Resource Constraint Environment: Applications and Use Cases. *International Journal of Advanced Natural Sciences and Engineering Researches*, 7(3), 269-278.

Abstract – In today's interconnected world, where several endpoints require data sharing in the most effective and concurrently secure manner, group communication is a crucial mode of communication. Especially in the confined surroundings introduced by the Internet of Things and sensor networks, the ensuing complexity constitutes a significant issue. Group key Management (GKM) is a vital function in schemes for secure group communication. Secure group communication scheme (SCG) should be created for realistic circumstances because they must account for the requirements and limits of real-world applications. This covers elements such as network latency, bandwidth constraints, processing resources available on devices used by end-users, and so on. By creating schemes that are customized to these settings, it is possible to improve performance and usability in the field while preserving robust security assurances against adversary assaults. This paper evaluated various use-cases and their accompanying applications in which group key management is a major concern, as well as emphasizing some of the unresolved issues that must be addressed in a variety of circumstances.

Keywords – Group Key Management, Secure Group Communication, Resource Constrained, Applications, Use Cases.

I. INTRODUCTION

The Internet of Things (IoT) has gained popularity among end users in recent years due to its pervasiveness and variety of applications. Internet of Things (IoT) refers to the interconnection of items (things) that interact across networks utilizing a variety of identification and communication technologies. In addition, an increasing number of IoT applications involving group communication have a significant impact on numerous aspects of our daily life. IoT applications can be found almost everywhere, including industrial control, smart healthcare, smart grid, transportation systems, and logistic [1] s. IoT is a self-configuring, intelligent system that can link to several technologies, such as cloud computing, fog computing, radio frequency identification (RFID), and wireless sensor networks (WSN) [2], to share sensory data and control things with or without human intervention. Owing to the intrinsic promise of this technology, it has already undergone exponential growth across a wide range of use cases and application domains. For the Internet of Things (IoT) to attain its full potential, a network architecture that supports security, privacy, and trust must be deployed, according to the consensus of experts from around the world who continue to investigate its capabilities.

The contribution of the paper are as follows:

- Discuss numerous use cases of resource-constraint environment where group key management is major concern.
- Discuss different applications which require to implement use cases.
- Emphasize a few of the unresolved concerns that must be addressed in a variety of environments.

The remainder of this paper is structured as follows. Section II gives background of this study by discusses the recent studies categories of secure group communication. Section III discuss the Applications and uses cases which required secure group communication schemes and discuss conclusion in Section IV.

II. RECENT STUDIES

Nayana Hegde and S. Manvi [3] proposed a secure group key management approach for dynamic vehicular cloud computing. The approach enables users to efficiently join or leave groups without activating new protocols, which would considerably improve VCC and save communication time, hence increasing reaction times for VCC applications like distributed storage systems and urban traffic control. SHOUYI ZHANG et al [4], offers a GKM protocol for safe cloud-based file sharing. The protocol combines a combination of encryption and verification techniques to thwart network and collusion attacks from cloud service providers and group members. R. Velumadhava Rao et al [5], presents an effective hierarchical-based group key technique for cloud-based data security. The proposed system relies on the Key Distribution Server (KDS) and the logical key hierarchy protocol to ensure scalability, making it more suitable than traditional security frameworks for group sharing scenarios. Zhihao Wang et al [6] presents a secure and efficient blockchain-based key management solution for smart grids. As demonstrated by a performance analysis and comparison, the suggested approach delivers stronger security features, reduced authentication delay, and less computing cost than conventional schemes. Haowen Tan and Ilyong Chung [7] provides a novel, realistic WBAN system paradigm with group message broadcasting and a secure, efficient protocol for group key management. The suggested approach makes use of the Chinese remainder theorem for batch key updating between healthcare centres (HC) and personal controllers (PC), as well as coded cooperative data exchange to optimize transmission passes and computation burden. Thomas Ewer et al [8], evaluates GKM protocols for LDACS control channel communication security. The proposed algorithms can be implemented utilizing GKM to enable safe communication between the various entities involved in digitally regulating aircraft movement.

III. APPLICATIONS AND USE CASES

This section discusses applications and use cases which required SGC schemes. Due to its widespread use and variety of applications, the Internet of Things (IoT) has become popular with consumers. Industrial control, smart healthcare, smart grid, transportation, and logistics use the Internet of Things. IoT is a self-configuring, intelligent system that can link to cloud computing, fog computing, RFID, and WSN to share sensory data and control things without human interaction. This technology has grown exponentially in many use cases and application domains due to its inherent potential. For IoT to realize its full potential, a network architecture that enables security, privacy, and trust must be established.

A. Smart Grid Networks:

A smart grid network is an enhanced power system that employs current communication and information technologies to enhance the efficacy, dependability, economics, and sustainability of electricity production, transmission, and distribution. It facilitates a two-way flow of energy and data between utilities (power plants), users (homes/buildings), distributed generation sources such as solar panels etc., electric vehicle charging stations etc.

The components of smart grid networks consist o f:

- **Advanced Metering Infrastructure (AMI)** for real-time energy consumption monitoring and control.
- **Distribution Automation** to enhance power distribution system dependability, efficiency, and adaptability
- **Renewable Energy Sources**, such as solar panels or wind turbines, that can produce electricity on a small-scale basis locally.
- **Electric Vehicle Charging Stations** that enable effective charging of electric vehicles and provide demand response services.
- **Energy Storage Devices**, such as batteries or flywheels, that store excess energy generated by renewable sources during periods of low demand so that it can be used when it is required.

Smart Grids' Advanced Metering Infrastructure (AMI) requires group key management. In smart grids, key management is one of the most critical open concerns [9]. This needs the construction of a secure and speedy procedure for verifying the access of numerous intelligent gateways and terminal devices.

1) Blockchain technology:

The blockchain provides Distributed Architecture, Security, and Privacy. It could resolve issues such as a single point of failure in centralized architecture [10]. Peer-to-Peer networks no longer require third-party verification when utilizing the most prevalent technology. Transactions are validated by members of the network. To maintain data integrity, network participants add new blocks of transactions to a ledger. Chien-Ming Chen et al [10] address the single point of failure issue by proposing a blockchain-based authenticated group key management protocol for the Internet of Things (IoT).

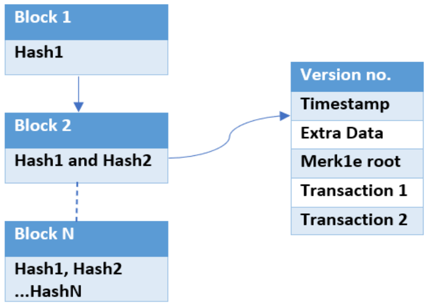

FIGURE 1. Block Structure

For smart grids, blockchain-based solutions have the potential to be effective. Blockchain technology can provide a secure, decentralized platform for handling smart grid network transactions and data. Smart grid networks can reach a higher level of security and privacy protection by utilizing the features of blockchain technology, such as decentralization, tamper-resistance, and transparency. However, the effectiveness of a blockchain-based solution for smart grids is contingent on several aspects, including the system's design, the scalability of the blockchain network, and the computing burden of the employed blockchain algorithms. Zhihao Wang et al [6]proposed a blockchain-based group key management system that is efficient and secure for smart grids. It includes five-tier architecture of the smart grid based on blockchain as shown in figure 2.

- **Management Layer:**

It dispatches the power system and includes energy and distribution management network control centers. The management layer dispatching center may schedule and trade and transmit power availability and order information to other smart grid layers.

- **Power Layer:**

It involves power generation, transmission, and distribution. The power layer manages electricity flow and distributes it to end-users effectively and reliably. All power, perceptual, and user layer entities are controlled by the dispatching center in the management layer.

- **Perceptual Layer:**

It sends data from smart meters and power plant sensors to the management layer for analysis and decision-making.

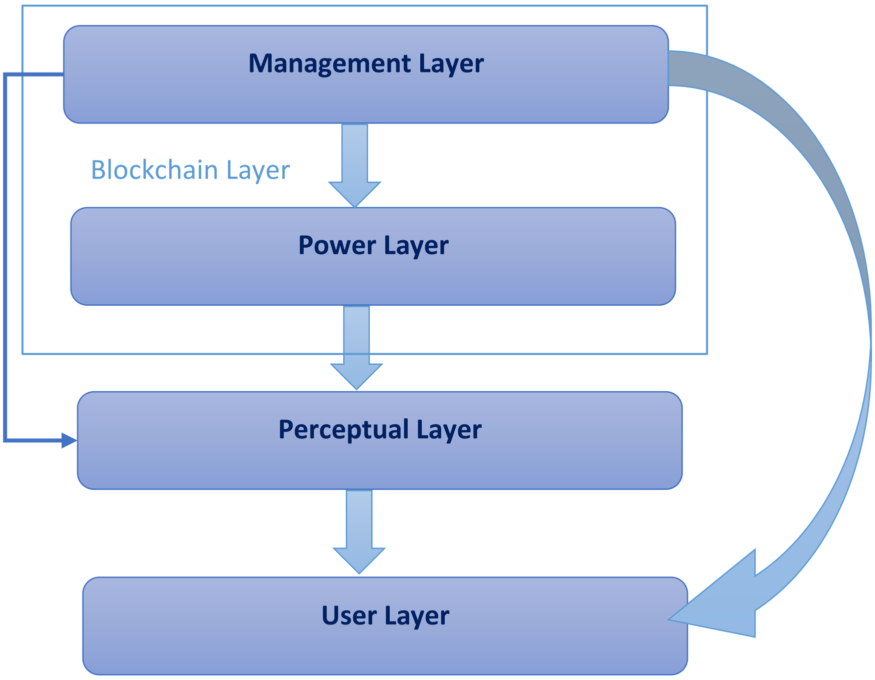

Fıgure 2: The Blockchain-Based Five-Tier Design Of The Smart Grid.

- **User Layer:**

It's where smart grid users interact. Smart meters, home automation, and electric cars comprise this layer. The management layer uses energy use and demand data from the user layer to optimize energy resource distribution.

- **Blockchain Layer:**

It monitors the dispatching center and prevents system parameter tampering by recording key distribution and system parameters. It verifies the key distribution process and prevents the intelligent gateway from interacting with the blockchain.

2) Wireless sensor networks (WSNs):

WSNs are a prominent Internet of Things backbone technology (IoTs). Secure group communications in wireless sensor networks (WSNs) convey weather, traffic, medical, and other data [2]. WSN data differs from digital communication data. IoT-enabled wireless sensor networks use multicasting for message delivery rather than device-to-device communication [11].

Smart grid systems require these sensors to monitor temperature, humidity, air quality, and more [12]. Generally, sensors lack memory, battery life, and processing capability. Consequently, sending multicast messages to a group of devices is more efficient than sending multiple copies of a unicast message to a device. A key establishment and distribution strategy that protects the communication's integrity, authenticity, and confidentiality is necessary to secure multicast group communication messages.

In general, the sensor nodes of a wireless sensor network share data for analysis. This exchange of information can be categorized as unicast, broadcast, or multicast.

B. E-Health care Management Systems:

The expanding use of the Internet of Things (IoT) presents the healthcare system with various potential (HCS) [13]. IoT applications in healthcare include remote monitoring, enhanced and intelligent sensors, and equipment integration. IoT can be utilized to monitor patient health, authenticate patients, and collect data. E-health is a healthcare system that uses electronic communication and information technology to provide remote healthcare services. These systems can be utilized at any time and in any location for patient monitoring, and wireless networks are utilized continuously to monitor patients' symptoms and recovery progress. In such applications, ensuring the confidentiality, integrity, and validity of patients' health records is essential.

A. *Wireless Mobile Environment (WME):*

A wireless mobile environment (WME) is a network that allows for secure communication between various nodes by employing wireless communication technologies like cellular networks or Wi-Fi. WME [14] in e-health systems is meant to ensure safe data exchange between various monitoring nodes. It is crucial that patients' health records remain private, intact, and legitimate while being monitored remotely across wireless networks. GKMPs provide authentication and data confidentiality to secure channels.

Arun Mailerum et al [13] suggests a breakthrough master-key management method to secure healthcare data. The [13] authors also note that as more users join a multicast group, existing protocols and schemes struggle to efficiently manage keys without compromising performance or security. Telemedicine solutions must ensure secure patient-provider communication and data accuracy with minimal delays. Finally, future research may compare cryptographic methods to find the most secure healthcare communication in resource-constrained wireless mobile circumstances. Healthcare Key Management (HCKM) is another approach [14]. This strategy decreases group members' rekeying overhead while maintaining forward and backward secrecy and strong encryption management in e-health systems. Better authentication, encryption, and dynamic group changes like user handoffs and node evictions are needed.

B. *Wireless body area networks (WBANs):*

As an integral part of the emerging IoT, wireless body area networks (WBANs) provide promising new avenues for e-healthcare systems of the future by monitoring users' vital physiological and behavioral data in real time using wearable sensors [15] [16] [7]. These essential bodily parameters are collected and broadcast externally to a WLAN, the internet, or a centralized database using this short-range wireless networked device that can be implanted in, on, or around the body.

Between the medical center (HC) and patient controller (PC), group key management takes place. In a WBAN, the PC oversees keeping in touch with sensors, while the HC oversees disseminating critical notifications to different patient groups. For both parties to be able to encrypt and decrypt data communicated over a network, group key management necessitates the exchange of messages carrying secret keys [16] [7]. The majority of the proposed group key agreement schemes in recent years only produce one group's secret key. More and more conversations in the IoT E-HCS are involving more than one person or organisation, and users can hold many conversations at once. Because of this, the computational cost and security flaws of the conventional public-key based, one-at-a-time group key establishment procedures are quite high.

The Haowen tan et al [7], proposed a protocol for group key management between the host controller (HC) and the personal controller (PC) makes use of the Chinese remainder theorem (CRT) and allows for batch key update. CRT reduces the number of calculations needed for encryption and decryption, making the process faster. It's also ideal for low-power, resource-constrained WBAN systems due to the reduced volume of keys that must be stored on both ends. The concept of coded cooperative data exchange (CCDE) motivates the suggested sensor association approach [7]. CCDE is a strategy for optimizing the transmission of data between several nodes in a network. According to Haowen tan et al [15] ,the healthcare facility (HC), biological sensors, and the user's smartphone as personal controller are the three most important parts of the WBANs system.

C. Intelligent Transportation System:

Connected vehicles, cloud computing, and the Internet of Things (IoT) are just a few examples of the cutting-edge technology that make up an ITS, which aims to improve transportation networks' security and efficiency. Sensors, cameras, and other devices are used in ITS systems to gather data on the traffic situation, which is then evaluated by computers or algorithms to help make better decisions. With increased visibility of possible risks like accidents and severe weather, this helps alleviate traffic congestion and boosts road safety.

Additionally, these systems help drivers save money on petrol by displaying up-to-the-moment data on the most efficient routes to take considering the current traffic situation. It was widely anticipated that the Intelligent Transportation System (ITS) would be fully operational within a decade of the advent of current vehicle and communication technologies.

To improve road safety and traffic flow, ITS incorporates IT into transportation infrastructure. Yet, security in vehicle-to-vehicle communication continues to be a top priority (VCSs). Safe group communication is the key to fixing this problem. That's why it's crucial to implement safe key management methods as part of your network's defenses. Essential to the achievement to the success of ITS are VCC, VANETs, and CAN [17].

1) *Vehicles Ad-hoc Networks (VANETs):*

Intelligent transportation system (ITS) components, such as decision-making agents, use VANETs data to make educated decisions that lessen traffic and cut down on fuel use. To protect data transmissions within a VANET network, it is important to use group key management. When a trusted authority (TA) in a VANET network gives out a group key, users in the network can communicate with one another. Keys that are part of a group can have their versions updated quickly and securely as new nodes join or leave the network.

2) *Vehicular Cloud Computing (VCC):*

Vehicular cloud computing (VCC) is a technology that enables vehicles to pool unused resources like data storage, network access, and processing power and share or rent them with other vehicles. It's an improvement over conventional VANETs, which are hampered by the need for complex computer hardware on board the units themselves (OBUs). VCC makes it possible for a diverse group of drivers to band together as a cloud and pool their available tools and services so that everyone can travel without incident.

As several vehicles form a cloud and need to securely exchange resources and services, VCC requires group key management. Nayana Hegde and S. Manvi [3] offers a dynamic asymmetric group key agreement technique for Vehicular Cloud Computing (VCC) that enables users to share resources and services inside a vehicular cloud in a secure and efficient manner. The technique combines classic authenticated group key agreement, public key encryption, and signing to allow users to join or leave a group without initiating a brand-new key agreement protocol.

An unsolved issue with the proposed method is mentioned in the study [3]. The authors point out that their proposed strategy presupposes that all users in the vehicular cloud are trustworthy and would not work together to undermine the system's safety. Unfortunately, though, there may be malicious individuals that attempt to assault the system. Hence, future studies may concentrate on creating a scheme that can deal with such attacks and guarantee the safety of the vehicular cloud even in the presence of bad users.

3) *Controller Area Networks (CANs)*

CAN is a crucial component of ITS. It enables the various ECUs in a car to talk to one another, allowing for the smooth transfer of information and instructions between them. By removing the need for human intervention in the operation of systems like engine control and transmission control, this makes automobiles more fuel efficient.

Furthermore, CAN can aid in the enhancement of safety measures in contemporary automobiles by offering real-time monitoring capabilities for several components, allowing for the early discovery of potential issues before they escalate.

Since CAN messages are broadcast to multiple receivers, the protocol must allow for the creation and modification of shared encryption keys. Group key exchange protocols provide this purpose. To safely trade cryptographic keys between ECUs via the CAN bus, they can be exchanged in a group setting. The network's nodes (ECUs) can come to an agreement on a shared secret for encrypted data transfer. Establishing secure connections with minimal computational overhead using group extensions of standard key exchange protocols, such as elliptic curve Diffie-Hellman, is possible [17]. This is because these protocols use group-based cryptographic primitives to generate and verify each of the necessary public keys. Transmission of Secret Keys in a Cryptosystem An integral part of designing safe networked systems is making sure that communications can take place over a publicly available channel. The CAN bus has serious vulnerabilities in terms of security due to its

inability to ensure the privacy and security of data and
to restrict who has access to it. All the proposed cryptographic solutions for safeguarding the CAN bus rely on the ECUs sharing a secret key, also known as a group key, for encryption and authentication purposes.

D. Smart Home Management System:

The Internet of Things enables real-time data flow analysis, which improves the efficiency and reliability of communication systems. Connecting all appliances in a smart home, for example, can save electricity through efficient monitoring. IoT improves daily life by making better use of available resources in the home. The concept of smart homes is to connect appliances using the Internet of Things architecture (IoT). The primary applications of smart homes can be classified, but are not limited to, the four categories listed below [18].

1. Household control: It is the most basic function that a household. host can use to control smart devices as a central or remote controller.
2. Surveillance and Security: Smart home systems can physically protect the home with surveillance devices and smart door locks.
3. Digital entertainment: To provide a better entertainment experience, the entertainment system can connect all the devices into a single Graphical User Interface (GUI).
4. Optimization of living conditions: Based on sensor data such as temperature, humidity, and air quality, the smart home system can optimize living conditions.

The enormous application potential of smart homes has drawn the attention of academia and industry. However, another factor that must be considered for smart home improvement is security [19]. Smart home systems are vulnerable to a variety of attacks due to their wireless communication environment and distributed network structure, such as Denial of Service (DoS) attacks, black hole attacks, Sybil attacks, and so on.

Two features of smart home sensors and devices should be considered to protect the smart home. Firstly, most sensors and devices have limited power and computation. Although such a design allows for the optimization of the system's power consumption, it means that such nodes cannot perform large-scale computations. Secondly, the smart home system is not designed with central authentication in mind. Home routers can connect to all smart devices or nodes; however, the home router is not trustworthy enough for authentication. This case raises the hard problem of key management in the smart home.

Qiao Liu et al [18], propose a novel secure group data exchange protocol in smart homes with physical layer approaches which retains the benefit of key sharing needles and lightweight computation. Gagandeep Kaur and Er. Kamaljit Singh Saini, provide a solution to secure network communication between motes in smart homes using IoT by utilizing Hierarchical Group Key Management Scheme [20]. Smart home energy management systems are a fast-growing smart home important field that is part of the smart grid program. Insufficient security is a major concern in smart home energy management systems. Because most security protocols commonly used for computer network and internet security are computationally expensive for wireless sensor nodes used in smart home applications, they cannot be implemented in smart home energy management systems. The establishment of the initial session key between the wireless nodes and the control center is the major issue in the security of smart home energy management systems.

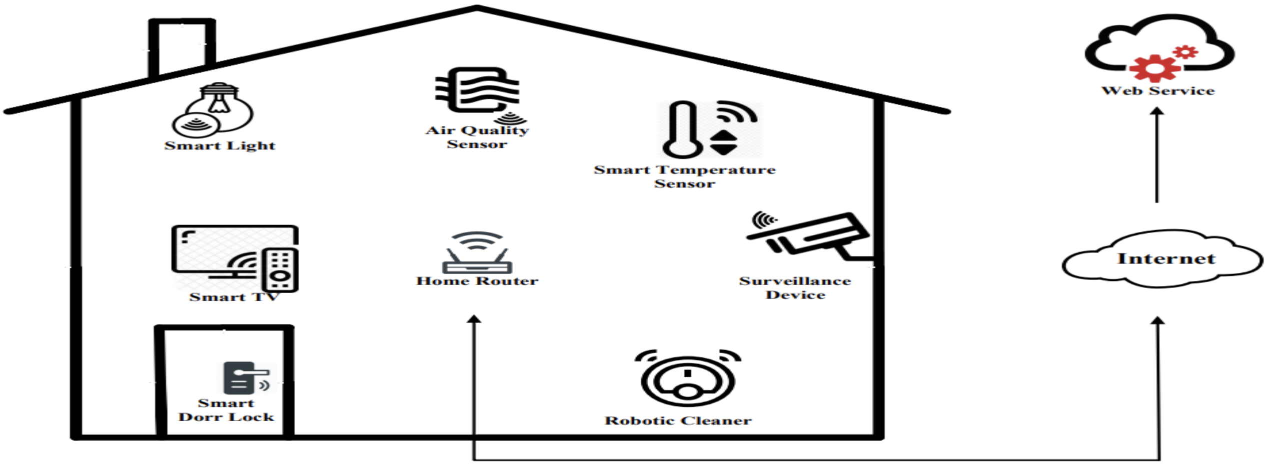

Figure 3. Smart Homes

E. Smart Hotel Management System:

IoT-connected devices are used in smart hotels to improve the guest experience and streamline the hotel management system for staff and administrators. There are numerous opportunities to use automation solutions to improve smart hotel rooms in the hospitality industry. Hotel owners and operators benefit from increased efficiency, cost savings, and guest satisfaction, while guests enjoy greater convenience and comfort. Yi-Hsuan Kung and Hsu-Chun Hsiao [21] propose a GroupIT scheme considering the hotel scenario. A hotel uses key cards to control guest access permissions in different rooms as well as the use of various facilities based on room class. When a guest checks in or out, or when new equipment is installed in some facilities, the hotel control center must update the shared keys between users and devices. When a guest checks out and the room becomes vacant, the devices inside the room should cease sending and receiving information from other devices.

Interoperability, along with personal data security and privacy, are the two most significant constraints to the growth of the Internet of Things (IoT) market. Interoperability increases the complexity and cost of service production processes. A lack of security and trust in privacy protection creates a barrier between service providers and consumers. The PARFAIT project, which stands for "Personal dAta pRotection FrAmwork for IoT," was proposed to address these challenges. The PARFAIT [22] project will create a platform for protecting personal data in IoT applications that will be tested with two main use-cases: Smart Home and the Smart Hotel. Maissa Dammak et al [23] consider the use-case of an extensive reservation system for franchise hotels in the context of the European project PARFAIT. In this scenario, key cards and smartphones could be used interchangeably to grant access permissions to guests in various rooms. They can also be used to restrict access to various facilities based on room classes and purchased services. When a guest leaves and the room becomes vacant, the devices should stop sending information about the room and receiving information from other devices.

IV. CONCLUSION

In a setting with limited space and resources, ensuring the safety of group conversations can be difficult. The resultant complexity is a serious problem, particularly in the restricted environments brought forth by the Internet of Things and sensor networks. Group key management, abbreviated as GKM, is an essential component of any system designed to ensure the confidentiality of group communications. Because they need to take into consideration the requirements and constraints of real-world applications, secure group communication schemes (SCG) should be developed with real-world scenarios in mind. This encompasses aspects like as the network latency, the limits on the bandwidth, the processing resources that are accessible on devices that are utilised by end-users, and so on. It is feasible to increase performance and usability in the pitch by establishing schemes that are adapted to these parameters. This can be done while still maintaining adequate security assurances against the assaults of adversaries. The purpose of this article was to analyses a range of use-cases and the applications that go along with them in which group key management is a major problem. Also, the paper highlighted some of the unresolved difficulties that need to be handled in several settings.

REFERENCES

[1] "41.6 billion IoT devices will be generating 79.4 zettabytes of data in 2025," 2019.

[2] A. ALBAKRI, "Non-Interactive Group Key Pre-Distribution Scheme (GKPS) for End-to-End Routing in Wireless Sensor Networks," *IEEE Access,* p. 9, 2019.

[3] N. Hegde, "Secure Group Key Management Scheme for Dynamic Vehicular Cloud Computing," *Int. J. Advanced Networking and Applications,* vol. 13, no. 1, pp. 4821-4826, 2021.

[4] S. Zhang, "Group Key Management Protocol for File Sharing on Cloud Storage," *IEEE Access,* vol. 8, pp. 123614 - 123622, 2020.

[5] R. V. Rao, "Hierarchical group key management for secure data sharing in a cloud-based environment," *Special Issue:Advanced Algorithms for IoT Cloud computing and Cyber-Enabled Applications (ICAMMAET-ICTPACT2018),* vol. 31, no. 12, 2018.

[6] Z. Wang, "A Lightweight Certificateless Group Key Agreement Method without Pairing Based on Blockchain for Smart Grid," *MDPI,* vol. 14, no. 4, 2022.

[7] H. Tan, "A Secure and Efficient Group Key Management Protocol with Cooperative Sensor Association in WBANs," *MDPI sensors,* vol. 18, no. 11, p. 3930, 2018, ; https://doi.org/10.3390/s18113930.

[8] T. Ewert, "Group Key Distribution Procedures for the L-Band Digital Aeronautical Communications System (LDACS)," in *2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC),* San Antonio, TX, USA, 2021.

[9] Z. Wang, "A Lightweight Certificateless Group Key Agreement Method without Pairing Based on Blockchain for Smart Grid," *Future Internet 2022 ; https://doi.org/10.3390/fi14040119,* vol. 14, no. 4, p. 119, 2022.

[10] C. Chen, "A secure blockchain-based group key agreement protocol for IoT," *SpringerLink,* vol. 77, p. 9046–9068, 2021.

[11] Q. CHENG, "Fast Multivariate-Polynomial-Based Membership Authentication and Key Establishment for Secure Group Communications in WSN," *IEEE ACCESS,* Vols. 8, 2020, no. April 29, 2020, p. 7, 2020.

[12] H. Nicanfar, "Password-authenticated cluster-based group key agreement for smart grid communication," *https://doi.org/10.1002/sec.726,* vol. 7, no. 1, pp. 221-233, 2014.

[13] A. M. Perumal, "Architectural framework of a group key management system for enhancing e-healthcare data security," *IET,* Vols. 7 ,https://doi.org/10.1049/htl.2018.5114, no. 1, pp. 1-12, 2019 .

[14] S. Iqbal, "Real-time-based E-health systems: design and implementation of a lightweight key management protocol for securing sensitive information of patients," *SpringerLink,* vol. 9, p. pages93–111, 2019.

[15] H. TAN, "Secure Authentication and Group Key Distribution Scheme for WBANs Based on Smartphone ECG Sensor," *IEEE Access,* vol. 7, no. 2019, p. 16, 2019.

[16] A. Rivero-García, "Patients' Data Management System Protected by Identity-Based Authentication and Key Exchange," *MDPI sensors,* vol. doi: 10.3390/s17040733, no. 4, 2017.

[17] A. Musuroi, "Fast and Efficient Group Key Exchange in Controller Area Networks (CAN)," *IEEE Transactions on Vehicular Technology,* vol. 70, no. 9, pp. 9385 - 9399, 2021.

[18] Q. Liu, "Novel Secure Group Data Exchange Protocol in Smart Home with Physical Layer Network Coding," *Sensors* , vol. 20, no. 4, p. 1138, 2020.

[19] E. Fernandes, "Security Analysis of Emerging Smart Home Applications," in *In Proceedings of the IEEE Symposium on Security and Privacy*, San Jose, CA, USA, 2016.

[20] G. K. a. E. K. S. Saini, "Securing Network Communication Between Motes Using Hierarchical Group Key Management Scheme Using Threshold Cryptography in Smart Home Using Internet of Things," in *Springer Singapore*, Singapore, 06 July 2017.

[21] Y.-H. Kung, "GROUPIT: Lightweight Group Key Management for Dynamic IoT Environments," *IEEE INTERNET OF THINGS JOURNAL,* Vols. VOL. 5, NO. 6, no. DECEMBER 2018, p. 11, 2018.

[22] [Online]. Available: PARFAIT. [Online]. Available: http://www.itea3-parfait.com/.

[23] M. Dammak, “Decentralized Lightweight Group Key Management for Dynamic Access Control in IoT Environments,” *IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT*, Vols. VOL. 17, NO. 3, no. SEPTEMBER 2020, p. 16, 2020.