IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 21 June 2023, accepted 13 July 2023, date of publication 24 July 2023, date of current version 31 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3298024

RESEARCH ARTICLE

Group Key Management in Internet of Things: A Systematic Literature Review

FOUZIA SAMIULLAH[1], MING-LEE GAN[1], (Member, IEEE), SEDAT AKLEYLEK[2,3], AND Y. AUN[1]

[1]Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman, Kampar, Perak 31900, Malaysia
[2]Cyber Security and Information Technologies Research and Development Centre, Department of Computer Engineering, Ondokuz Mayis University, 55270 Samsun, Turkey
[3]Chair of Security and Theoretical Computer Science, University of Tartu, 50090 Tartu, Estonia

Corresponding author: Ming-Lee Gan (ganml@utar.edu.my)

This work was supported by the Fundamental Research Grant Scheme, Ministry of Higher Education (MoHE), Malaysia, under Grant FRGS/1/2021/ICT07/UTAR/02/3.

ABSTRACT IoT networks are gaining popularity in terms of group networks built by sensor nodes and other IoT-related devices. The significance of cryptography protocols for secure communication among nodes in such networks cannot be overstated. Effective point-to-point and multicast communication among groups of nodes is of paramount importance. The security of IoT necessitates the concealment of security protocols and keys that are transmitted between nodes. The management of group keys, commonly referred to as Group Key Management (GKM), is an essential component of secure group communication protocols. It is imperative to develop a Secure Group Communication (SCG) scheme that is designed for practical scenarios, taking into consideration the demands and constraints of real-life implementations. In addition, most of the existing GKM schemes are dependent on public-key cryptography which are vulnerable to quantum computers. This SLR evaluates 48 proposals identified in IEEE Xplore, Springer Link, MDPI, ScienceDirect, Scopus, and Hindawi databases between 2013 and 2023. Moreover, we provide a classification of secure group communication schemes. In addition, we conduct a comprehensive performance and security evaluation of the SGC schemes. In addition to other security features, we consider quantum resistance to be one of the security features, and we describe the application and usage area considering a resource-constrained real-world scenario where GKM is the most important issue.

INDEX TERMS Group key management, IoTs, cryptography, Secure group communication, post-quantum.

I. INTRODUCTION

Internet of Things or IoT is influencing our lifestyle from the way we react to the way we behave. IoT devices are progressively assuming a significant role in peoples' daily lives. IoT devices are tangible, network-connected objects with a range of shapes and features. Devices connected through the internet are rapidly increasing. IoT is a giant network of connected devices. IoT is the interconnection of objects (things) that communicate through networks using various identifying and communication technologies. Furthermore, an increasing number of IoT applications involving group communication influence various important areas of our daily lives. Smart factories, remote healthcare [1], smart homes [2], smart mobility, traffic management, and other areas are some examples. In addition to this, new 5G technology significantly speeds up data transfer and enables further scaling of the connectivity process [3]. The deployment of 5G will result in faster broadband speeds and more reliable mobile networks, as well as a faster pace of progress in smart cities, smart vehicles, and smart manufacturing. These advancements open new opportunities for a wide range of applications involving multiple communicating parties.

Moreover, this promising digital transformation will not be released unless consumers can have confidence in the privacy and security of their data [3]. In fast growing IoT devices

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamad Afendee Mohamed.

dealing with sensitive data e.g., monitoring patient health condition [4], safe communication is our main concern. As a result, it is critical that users maintain control over their data and restrict access to it. Unfortunately, in the past, companies developing IoT devices frequently failed to address this need for security and privacy [3]. IoT devices were commonly deployed without due consideration for security. This resulted in 2016's greatest Distributed Denial of Service (DDoS) attack, which was carried out by thousands of hijacked IoT devices transformed into a botnet to bring down major Internet services such as Netflix and Spotify [5]. IoT is a heterogeneous interconnection of smart devices across various application domains. The availability of high-speed Internet connectivity alongside complementary advanced technologies such as Big Data, Cloud Computing, and easily accessible, inexpensive electronic devices equipped with new wireless communications standards are responsible for the explosive growth of the number of Internet-connected "things" These exponentially increasing numbers of connected smart devices also contribute to the Internet's enormous daily data traffic, data storage capacity, and data availability. Therefore, we, the individuals who incorporate IoT into our residences and businesses, should be more concerned about security [3]. As the attack surface is so vast, it is nearly impossible to provide complete security for IoT infrastructure due to its extensive coverage across numerous application domains and large number of heterogeneous devices. Multiple aspects of IoT security have matured, including privacy, authentication, trust, and communications.

It is crucial to boost security by encrypting IoT connection to stop future attacks and better secure users' data. Developers will find it challenging because group communication (also known as n-to-n communication) is more challenging to encrypt than one-to-one communication. In n-to-n communication, messages must be encrypted for a collection of recipients.

GKM represents a fundamental service in secure group communication schemes. On distributed entities the management of secret keys for secure group communication is known as GKM, which shares among all group members. The shared group key is used to sign and encrypt group messages, authenticate group members and messages, and grant access to group resources and traffic [1], [6], [7].

As a result, the vast number of devices in existence generate enormous quantities of data. Enabling these devices to locally process their data by means of identification and authentication enhances their performance, reduces bandwidth consumption, extends battery life, and mitigates security risks associated with attacks, thereby rendering the devices self-sufficient. To attain this objective, it is imperative that the devices possess a secure mechanism that facilitates the generation, distribution, and revocation of cryptographic keys. The cryptographic strength of this group key and the key management protocol determine the strength of an SGC scheme [2], [8]. The development of secure cryptographic protocols capable of ensuring data and communication privacy is a significant step forward in this effort.

Furthermore, Cryptography security mechanisms are classified as Symmetric and Asymmetric in general. Group Key Management schemes can be classified into three categories: symmetric, asymmetric and hybrid [7]. Although asymmetric key mechanisms are the more powerful and serve as a foundation for establishing secure communication channels between multiple parties, they consume more power as well. It is a critical technology for highly interconnected networks and, as such, is critical for the Internet of Things. Previously affects are made to lighter the cryptographic primitives like Elliptical Curve Cryptography (ECC) and Advanced Encryption Systems (AES) [1], [6], [7], [9], [10], [11], [12] by reducing computational time and cost. These protocols are based on hard problems like IF (Integer Factorization) and DL (Discrete Logarithm). It is decided whether the algorithm is more resistant to attacks or not based on how difficult the problem was taken during the formulation.

The existing group key management schemes are designed based on integer factorization (RSA) [9], [13], [14], [15], [16], [17] or discrete logarithms (ECC) [1], [11], [12], [18], [19], which are vulnerable to quantum computer. Both the number of IoT devices and the performance of quantum computers will grow in the coming years. Both technologies put our current crypto strategies to the test. As a result, post-quantum n-to-n communication encryption is an important area of study. In this case, the development of new schemes, as well as the analysis and comparison of existing schemes, is required. The National Institute of Standards and Technology (NIST) published a report on the need for PQC algorithms in 2016, stating that the need for standardizing the new post quantum cryptosystem had been established for the security of digital communications. Many proposals have been submitted to the National Institute of Standards and Technology (NIST) [20].

On 5th of July 2022 first group of winners were announced from the six-years of competition [21].

Certain algorithms, however, may be too inconvenient to use in IoT networks. Cryptography is a critical technology for securing communication in IoT networks. IoT is made up of heterogeneous devices ranging from low to medium power, such as sensors [17], actuators, edge devices, and so on. Dealing with cryptographic techniques in the IoT environment is fraught with difficulties, as it sometimes necessitates lightweight cryptographic solutions. We must be able to integrate new cryptographic schemes with existing protocols like Secure Shell (SSH) or TLS. To do so, designers of post-quantum cryptosystems must consider the following characteristics for IoT use-cases:

- Transfer delay caused by encryption and decryption at both ends of the communication line, assuming several devices from large and fast servers to slow and memory limited IoT devices.

- ➢ Limit the size of public keys and signatures for ultra-low latency.
- ➢ A network architecture that enables cryptanalysis and the detection of vulnerabilities in a dense IoT network.
- ➢ Integration with the existing infrastructure is flawless.

Motivation and Contributions:

- The SLR revealed a significant research gap in the investigation of SGC protocols for IoTs, particularly in the context of scenario specific SGC schemes, as evidenced by the limited existing literature identified in Table 2.
- The key contribution of this research lies in the identification of critical factors for secure group communication in resource-constrained networks. This includes examining the consequences of recent cryptographic developments, particularly in the context of post-quantum cryptography and the new NIST quantum resistance protocol.
- Through the investigation and comparison of 48 different secure group communication schemes with a focus on IoT scenarios, this research article provides valuable insights into effective approaches for managing group keys in resource-constrained networks.
- Our study contributes by providing valuable insights into the challenges and unresolved issues surrounding GKM in a variety of use cases and applications applicable to IoT scenarios, considering into factor the opportunities arising from post-quantum security.
- By identifying and discussing these open issues, our research aims to guide researchers in developing effective solutions for SGC in diverse situations, leveraging developments made in the field of post-quantum cryptography.

The remainders of the paper are organized in the following manner. Section II provides contextual information for this study by examining the various classifications of secure group communication. Section III presents a comparison between the current study and the previous one. Section IV explores the three stages of Systematic Literature Review (SLR), namely Planning, Conducting, and Reporting. Furthermore, Section V highlights existing challenges associated to group key management that are being addressed by researchers in the field of Internet of Things (IoT). Subsequently, the various schemes placed forward by distinguished researchers are presented in Section VI. Section VII provides a detailed account of the various applications and use cases, while Section VIII presents an extensive evaluation of the conclusions drawn from the study.

II. BACKGROUND

In this section, we provide the necessary context for secure group communication by describing the requirements of SGC and then defining GKM to gain a deeper understanding of the subject.

A. SECURE GROUP COMMUNICATION

The requirements of secure group communication can be divided into two categories: security requirements and efficiency requirements (as shown in **FIGURE 1.**)

i Security Requirements:

a) Authentication: Before giving nodes access to the group, an SGC scheme must authenticate their identities. Furthermore, in group communication, a member can be designated as the sender, the receiver, or both. To protect against identity-related attacks, members should be authenticated. Authentication can be accomplished using a group key, a pairwise key, or a certificate [28].

b) Integrity: It refers to correctness and consistency of group messages. Messages should be forwarded without modification and tempering. To achieve this hashing, digital signatures can used with strong encryption keys [29].

c) Confidentiality: It is a set of rules that limit access and define some restrictions on data. Group messages sent to a group should be limited to that group; only authorized groups can be able to access that data. This can be achieved by different encryption techniques [19].

d) Rekeying: It refers to the process of updating the session key. Long-term key had more chance to compromise frequently. Every change in membership necessitates rekeying of associated keys. The group key should be revoked immediately if a member's membership changes. Otherwise, until the group key is updated, the revoked nodes can continue to use the group communication. To reduce the amount of data encrypted with the same keys we modify the encryption key. The different techniques for key update provide options for managing the lifecycle of encryption keys in group communication scenarios. (As shown by Table: 1)

e) Group Independence: A node keeps a per-group profile that includes security parameters like the group controller address and group key. Because a node may be a member of more than one group, security parameters must be independent so that a compromised group does not have an impact on the other groups.

f) Quantum Resistant: The emergence of quantum computing may render various classical cryptography primitives susceptible to security breaches. Consequently, it is imperative to devise protocols that exhibit resistance against quantum attacks and guarantee enduring security.

ii Efficiency Requirements

a) Scalability: Secure group communication schemes which provide efficiency and security for small groups should be maintained if the group size becomes larger. Most importantly, membership management algorithms must be efficient in a way that group controller can manage multiple requests simultaneously

TABLE 1. Definitions of different key update strategies.

Key update types	Definitions
Periodic	It is a key update strategy in which encryption keys are updated at regular intervals. Important changes occur on a predetermined schedule, such as hourly, daily, weekly, or any other regular interval. This method ensures that keys are routinely updated, minimizing the risk of long-term compromises, and preserving the security of group communication.
Probabilistic	It is a strategy in which key updates occur at random according to a probability distribution. Keys are updated at random intervals, adding an aspect of unpredictability, rather than according to a predetermined schedule or trigger. This approach adds an additional layer of security, making it difficult for potential attackers to predict when critical updates will be implemented.
On-demand	It is a strategy in which significant changes occur in response to specific requests or triggers from group members or the system. When a member requests a new key, identifies a security issue, or certain predefined conditions are met, key updates may be initiated. This method allows for greater flexibility in key management, as updates are implemented on an as-needed basis rather than according to a predetermined schedule.
Session wise	It is a strategy in which encryption keys are updated at the start of each group session or communication session. A session is a distinct period or phase of group communication. This method guarantees that each session begins with a new set of keys, thereby reducing the potential impact of key compromises or assaults on subsequent sessions.
At membership change	It is a key update strategy in GKM that requires updating encryption keys when group membership changes. When members join or leave a group, or when the number of members changes this strategy triggers important updates.

TABLE 2. Related surveys.

	[22]	[23]	[8]	[24]	[25]	[26]	[27]	This study
SLR	No	No	No	No	No	No	No	Yes
Discuss GKM schemes in IoT settings	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Quantum Resistant SGC schemes	No	No	Yes	No	No	No	No	Yes
Discuss Scenario specific SGC schemes	No	No	No	No	No	No	No	Yes
Storage cost	Yes	Yes	Yes	No	No	No	Yes	Yes
Communication cost	Yes	Yes	Yes	No	No	No	Yes	Yes
Computational cost	Yes	Yes	Yes	No	No	No	Yes	Yes
Anti-Collision	Yes	Yes	No	No	No	No	No	Yes
Forward / Backward Secrecy	Yes	Yes	No	No	No	No	Yes	Yes
Message Confidentiality	Yes	No	No	No	No	No	Yes	Yes
Member Authentication	Yes	Yes	No	No	No	No	Yes	Yes
Message Integrity	Yes	Yes	No	No	No	No	Yes	Yes
Group Independence	No	No	No	No	No	No	Yes	Yes
Instant Rekey	No	No	No	No	No	No	Yes	Yes

e.g., user joins or leaves activity. Delivery of the group key to large groups must be in reasonable amount of time with reasonable amount of delay, low computational and communication cost [22].

b) Flexibility: Secure group communication schemes should work well in different types of environments. Support dynamic behavior. Allow adding and removing user at any time [22].

c) Low Storage, Communication, computation cost: Secure group communication schemes should be efficient in respect to storage, communication, and computational cost. IoT devices are recourse constraints which make us focus on these specific limitations. Memory to store keys is limited so the number of keys used to protect group communication must be low. Computational cost must not be very heavy as sensors inherently have low power CPU. Component's message exchange rate must be low. In fact, to avoid sensor node energy, drain and thus failure, the SGC scheme must not impose a high communication cost.

B. TOPIC CONCEPTUAL MODEL

The topic conceptualization provides detailed information on the subject under consideration. To gain a "broader understanding of what is known about a topic," thinking about the topic conceptualization is required. [32] TABLE 3. exhibits the working definitions of GKM proposed by various authors.

III. RELATED WORK

GKM in the context of the IoT poses several challenges that researchers have been addressing. One major challenge is the need for highly secure group communication in IoT settings. Multiple studies [8], [22], [23], [24], [25], [26], [27] have been conducted to investigate the various aspects of GKM schemes in IoT environments. Comparing GKM or SGC schemes in terms of security and efficacy, existing research identifies several relevant factors. However, usually, these factors emerge spontaneously, without a systematic comparison of every considered scheme about each factor in depth. In the survey by Piccoli [26], Torraco [25], and

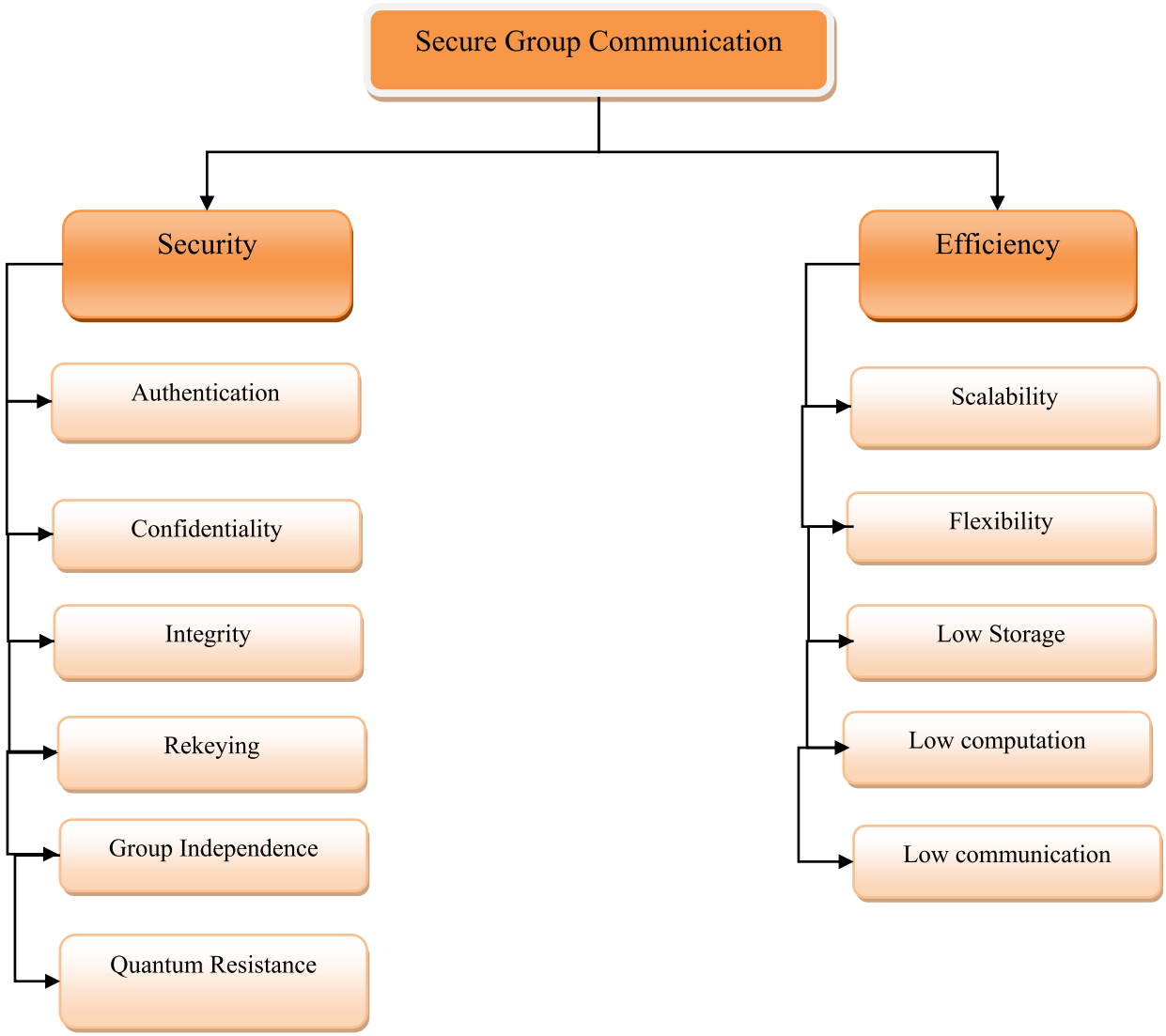

FIGURE 1. Secure group communication reqluirements.

Cheikhrouhou [24], the primary focus is on GKM schemes in IoT contexts. While the specific aspects covered are not explicitly stated, it can be inferred that this study provides an in-depth evaluation of the efficacy and suitability of GKM mechanisms for IoT deployments. Torraco [25] summarize multicast group communication use cases and security requirement, but the use cases are not explicitly related to real-world scenarios.

Prantl's [8] considers factors like Quantum Resistance and SGC schemes, among others by benchmarking pre and post quantum group encryption schemes in IoT settings. The significance of SGC in IoT contexts is highlighted, and the ramifications and difficulties of quantum resistant GKM schemes are investigated. In addition, existing studies either discuss general schemes [25] or concentrate on a particular form of GKM [1], [33]. Piccoli [26] only examine centralized and decentralized schemes, whereas Hanna [23] divides protocols into network independent and network dependent categories. In comparison to our work, Table. 2 provides an overview of the factors used or mentioned by previous studies when evaluating GKM or SGC schemes. In contrast to previous research, our survey examines these factors for each scheme in depth and provides a systematic and exhaustive comparison.

We compare the efficiency of the schemes using the indices storage costs, communication costs, computation costs, key update frequency, and types of employed cryptography. Moreover, we evaluate the security of the schemes in terms of forward and backward secrecy, anti-collision, instant rekeying, message integrity, message confidentiality, member authentication, group independence, and quantum resistance. Only [22] and [27] explicitly address the critical issue of scheme suitability for IoT group Communication.

As compare to [27] 1) This study not only done the systematic comparison of the schemes but also done a SLR adhered to Kitchenham's guidelines [33] 2) Consider not

TABLE 3. An overview of the selected definitions of group key management.

Definitions of GKM	Source
"The management of secret keys on distributed entities is called GKM"	[30]
"The GKM is the core of secure communication. Its main role is to establish secure links between the members of a group."	[7]
"GKM enables secure access to relevant information, such as group keys in order to grant confidentiality, integrity as well as sender- and group-authentication."	[6]
"GKM involves the handling, revocation, updating and distribution of cryptographic keys to members of various groups in a communication network"	[11]
"GKM represents the fundamental mechanism for managing the dissemination of keys for access control and secure data distribution."	[1]
"GKM is one of the fundamentals in securing group communications. A group key essentially is a secret key shared by all members of a group so that all group communication packages are encrypted before they are being transmitted using this group key."	[31]

only 12 but 13 aspects 3) consider quantum resistant security feature, in addition to other security features. 4) Specifically mention the application and usage area considering the real-world resource constraint scenario where GKM is the major concern.

IV. RESEARCH METHODOLOGY

The SLR method was used to examine studies published between 2013-2023. SLR is divided into three phases: ''Planning'', ''Conducting'', and ''Reporting reviews. This methodological study strictly adhered to Kitchenham's guidelines [33] for a systematic literature review. The SLR design is made up of a series of steps, as shown in FIGURE: 2. The guidelines for systematic literature review are divided into three phases, as shown in FIGURE: 4

A. PHASE 1: PLANNING THE REVIEW

The research questions for this study have been developed in accordance with the current study's aims and objectives.

1) RESEARCH QUESTIONS FORMULATION

RQ 1: What existing issues in IoT researchers trying to solve related to GKM? Describe GKM primitives.

RQ 2: Define and Explain different GKM schemes proposed for resource constrained IoT networks.

RQ 3: What is the application/usage areas?

The aim of these RQs is to obtain insight into the existing challenges associated with IoT-related GKM that researchers are addressing. RQ1 focuses on identifying the specific challenges being addressed, such as key distribution, scalability, constrained environments, and security. RQ2 aims to explore the different GKM schemes proposed for resource constrained IoT networks, highlighting their characteristics and approaches. RQ3 broadens the scope by examining the application areas where GKM is relevant, showcasing the practical importance and impact of effective group key management in various domains.

2) SEARCH STRATEGY

A predefined electronic search space was created to look for relevant studies. For the literature search, the electronic databases ScienceDirect, Hindawi, MDPI, Springer Link, IEEE Xplore, Google Scholar, and Scopus were used. To gather relevant literature for this investigation, the inclusion and exclusion criteria for the studies were determined. After screening, the dismissals were detected, and mutual agreements among the authors were erased. The retrieved publications were then evaluated to assess and improve the study's quality [34].

a: SEARCH KEYWORDS

To cover the broader scope of this study, the relevant keywords are pre-defined. To reduce the search for irrelevant studies, Boolean operators such as ''AND'' and ''OR'' were used. Table 4: described the search string employed in the study:

b: DATA SOURCES

To begin the Systematic Literature Review, the authors began by searching for related studies using limited search strings and keywords. A comprehensive search of electronic databases was carried out. To find relevant literature for this systematic review, most popular scientific databases were searched. The mentioned keywords in Table 4 are those against which we get relevant results from different databases. The Figure. 2 includes data sources as well as the number of studies extracted from each data source (ScienceDirect, Hindawi, MDPI, Scopus, Google Scholar, and IEEE Xplore).

B. PHASE 2: CONDUCTING REVIEW

Selecting studies, inclusion and exclusion criteria, and quality assessment are all part of the review phase.

1) PAPER SELECTION

The screening studies were conducted in accordance with the PRISMA framework and the emerging researcher author consensus. To enhance the quality of existing studies, research was selected according to a predetermined set of rules. The article screening procedure commenced with a verification system and the identification of relevant studies, followed by the elimination of duplicate studies from multiple data sources. Before conducting a comprehensive review of the text, an abstract and introduction-based screening was conducted. Then, studies were evaluated according to the inclusion and exclusion criteria. Finally, a full-text analysis of 48 possible articles was conducted and observed. The sequential selection process is depicted in figures. The

TABLE 4. Search keywords.

Databases	Search strings
IEEE Xplore	"(Group key management OR GKM) AND (iot OR internet of things)" OR "(Group key management OR GKM) AND (internet of things OR iot) AND post quantum" OR "(Group key exchange OR GKE)AND (iot OR internet of things)" OR "(Group key exchange OR GKE) AND (internet of things OR iot) AND post quantum" OR "(Group key distribution OR GKD)AND (iot OR internet of things)" OR "(Group key distribution OR GKD) AND (internet of things OR iot)".
***Springer Link*:**	"Group key Exchange AND (IoT OR Internet of things)" OR "Group key Management AND (IoT OR Internet of things)" OR "Group key Establishment AND (IoT OR Internet of things)".
MDPI:	"Group key Establishment AND internet of things AND Quantum Safe" OR "Group key Agreement AND internet of things" OR "Group key Agreement AND internet of things".
ScienceDirect:	"Group key management AND Internet of things" OR "Group key agreement AND Internet of things" OR "Group key distribution AND Internet of things".
Hindawi:	"Group key management AND Internet of things" OR "Group key agreement AND Internet of things" OR "Group key distribution AND Internet of things" OR "Group key Establishment AND internet of things".
Scopus:	TITLE-ABS-KEY (group AND key AND exchange AND (iot OR internet AND of AND things)) , ABS ((group AND key AND management OR gkm) AND (iot OR internet AND of AND things)) , ABS ((group AND key AND distribution OR gkd) AND (iot OR internet AND of AND things)).
Google Scholar:	allintitle: (Group key management OR GKM) OR (iot OR internet of things), allintitle: (Group key exchange OR GKE) AND (iot OR internet of things).

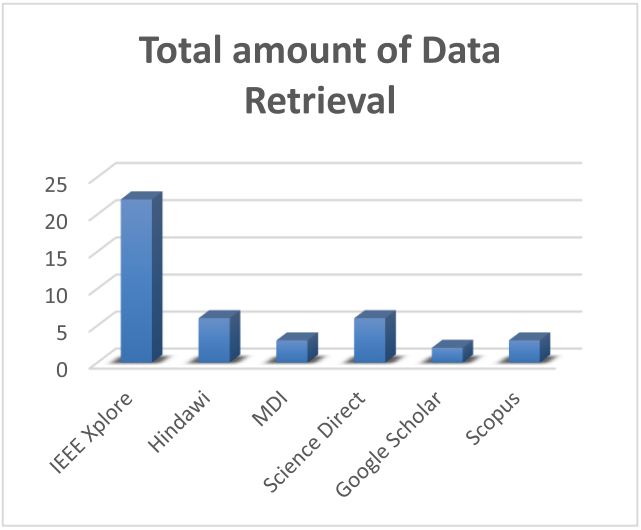

FIGURE 2. Data source publication venues.

PRISMA flowchart displays the total number of studies examined at each research stage (as shown in FIGURE. 3).

2) INCULSION CRITERIA

To select primary studies, authors devised and strictly followed inclusion and exclusion criteria. The following are the finalized inclusion criteria for the current study:

1: Studies must be published in a scholarly journal or presented at a conference.

2: Studies written exclusively in the English language.

3: Publication must occur between 2013 and 2023.

4: Studies focused on Group key management in internet of things.

5: The primary goal of the study should have been to investigate and explore group key exchange within IoT constraint network.

3) EXCLUSION CRITERIA

We have also developed exclusion criteria to narrow the scope.

1: Keynotes, non-conference presentations, lab reports, tutorial summaries, newspaper articles, online blogs, book chapters, short paper summaries and abstracts.

2: Studies that are irrelevant or out of scope.

3: Repetitive/duplicated literature discovered from specified data sources.

4: Studies that are not conducted in English.

5: Search strings against which we don't find any result.

6. Any schemes that do not adequately define a GKM or fall into none of three categories: centralized, decentralized and distributed.

5: Papers that do not meet the quality assessment criterion.

4) QUALITY ASSESSMENT

The selected studies were evaluated using the procedure recommended by York University's Centre for Reviews and Dissemination (CDR) Database of Abstracts of Reviews of Effects (DARE) [35].

The criteria are based on three questions. Each question is score as: - (0,0.5, 1), "0" score indicates that study doesn't includes the favorable outcomes, "0.5" score indicates that study partially answers the question. "1" score indicates that study includes favorable outcomes. Each paper is assessed against quality assessment question. Table 5 shows the total scores for all selected studies.

QA-1: Is the study focused on GKM schemes for resource constraint IoT network?

QA-2: Is the given framework provide solution for rekeying overhead reduction?

QA-3: Is the result findings in the study is shows relatability with their proposed work?

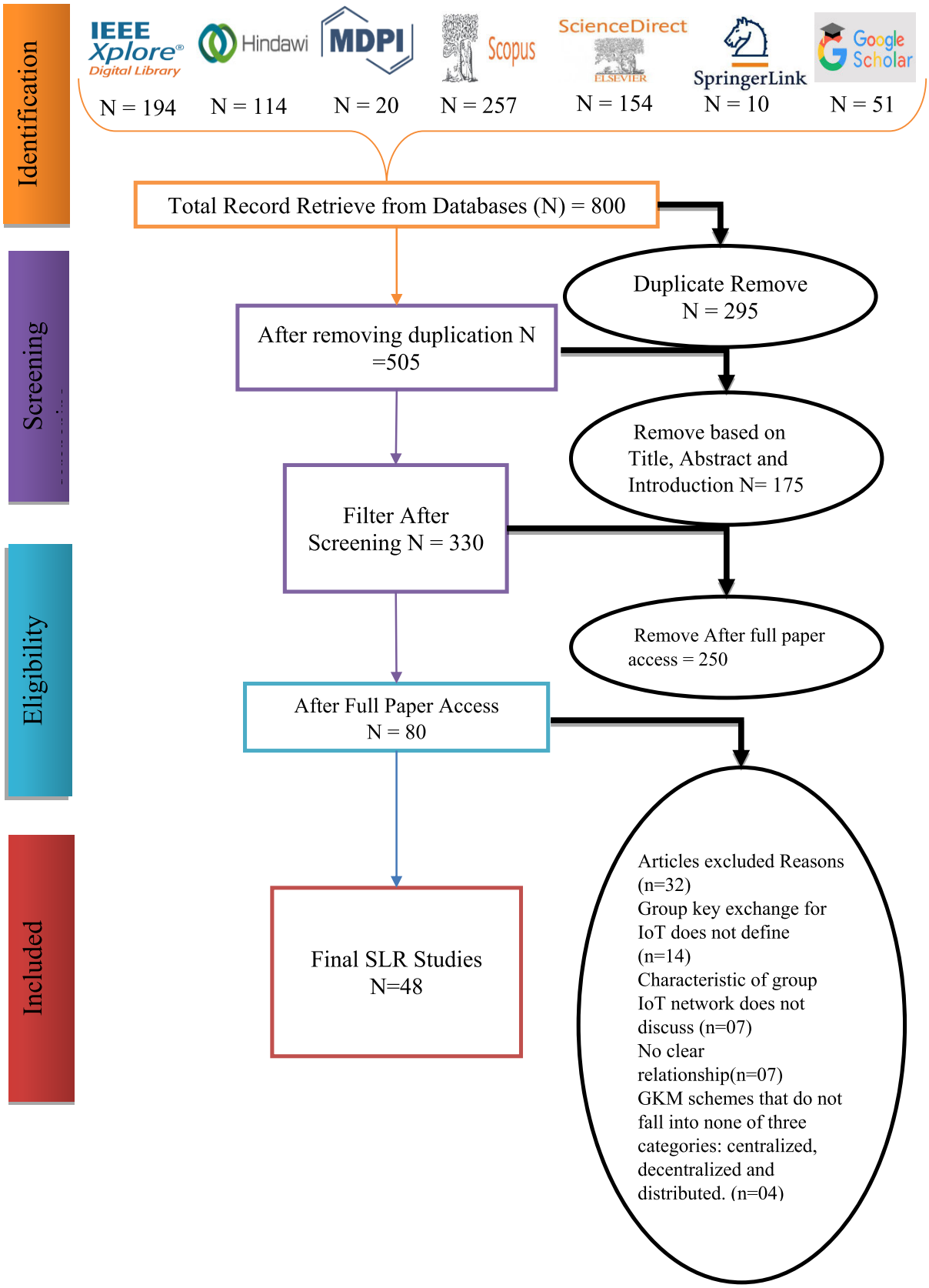

FIGURE 3. Process for study selection in accordance with PRISMA guidelines.

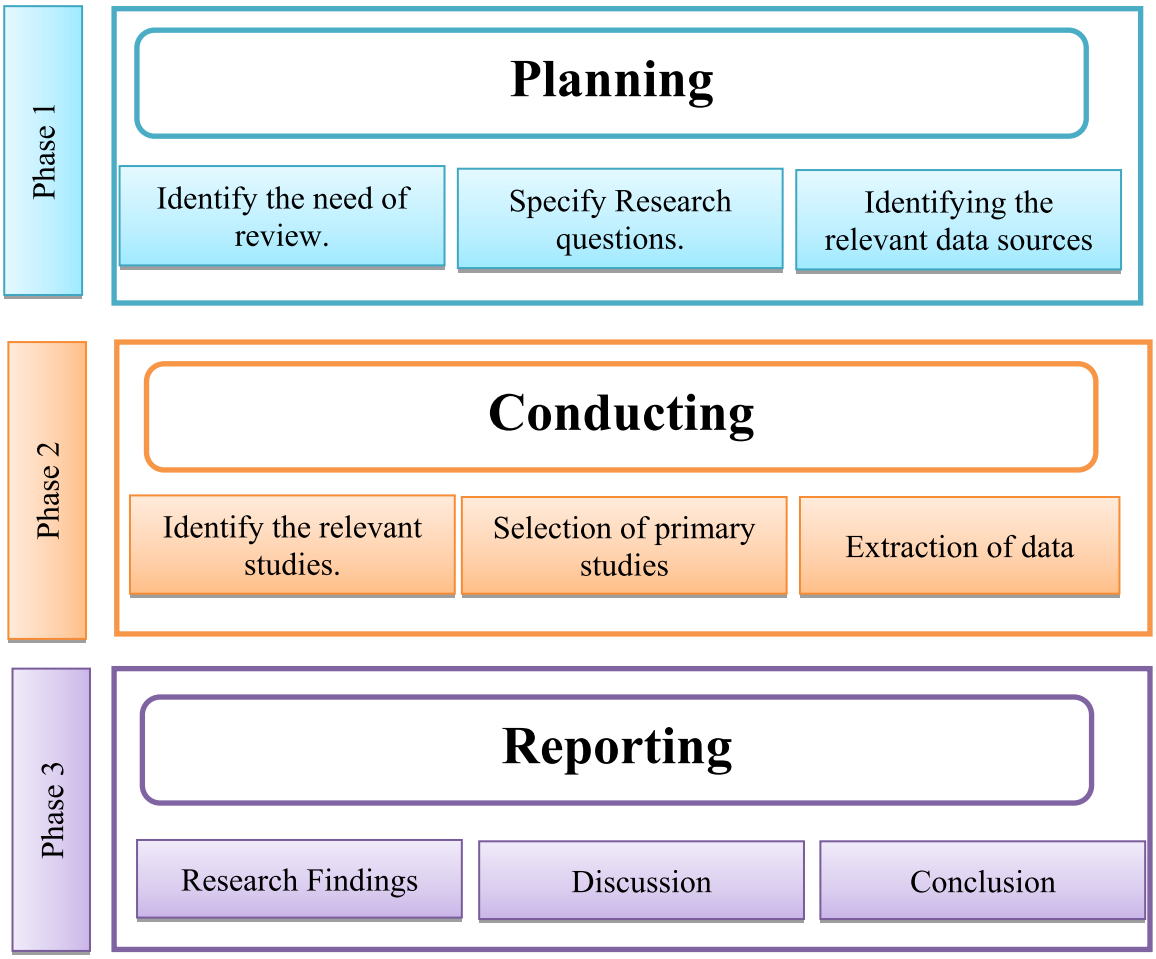

FIGURE 4. Systematic literature review procedure.

C. PHASE 3: REPORTING REVIEW

The reporting review phase includes data extraction, authentication process, and reporting the review, which is described below:

1) DATA EXTRACTION

To obtain the necessary information, the studies extracted for this literature review were meticulously examined, and it was determined that the obtained data reflected a consensus among all studies. In the context of this study, the characteristics obtained are the article's title, the researcher's name, the year of publication, the publisher and type of study, the application of the analysis, methodology, and the sector and security approach discussed. Data were collected, including the conclusion of the authors.

2) AUTHENTICATION PROCESS

To confirm the correct selection procedure and avoid inaccuracies in data extraction, research selection, and article ''classification,'' the recommendations of Kitchenham were adhered to with great care. Uncertainty regarding the ''Validation Process'', particularly regarding ''research selection,'' ''incorrect data extraction,'' ''incorrect classification,'' ''research method,'' and ''Author Bias.'' As a result, authors in the current study followed Kitchenham's recommendations. To avoid conflicts, the authors took part in the classification and carefully discussed the studies. The classification results were reached with the author's mutual agreement and based on recommendations.

V. EXISTING ISSUES IN GKM W.R.T IoT

This section refers to our RQ 1:'' What existing issues in IoT researchers trying to solve related to group key management? Describe primitives of GKM.''

Researchers are working to create an architecture that is not only secure but also capable of preventing attacks even if attackers gain access to the system. The WSN is a critical component of the IoT. Sensors are typically limited in memory, battery capacity, and computation power. As a result, it is more efficient to send multicast messages to a group of devices rather than sending unicast messages to individual devices in multiple copies, which consumes more energy. The establishment of a secure group key is a critical feature for providing message integrity, authentication, and confidentiality [19]. New IoT use cases that rely on multicast group communication raise the need for security to protect

TABLE 5. Quality assessment.

Study (S)	Quality Assessment			Total Score
	QA-1	QA-2	QA-3	
Study-1 [36]	1	1	1	3
Study-2 [13]	1	0.5	1	2.5
Study-3 [37]	1	0.5	1	2.5
Study-4 [38]	0.5	1	1	2.5
Study-5 [1]	1	1	1	3
Study-6 [17]	1	0	1	2
Study-7 [9]	1	0.5	1	2.5
Study-8 [14]	1	0	1	2
Study-9 [28]	1	0	1	2
Study-10 [31]	1	0.5	1	2.5
Study-11 [39]	1	0	1	2
Study-12 [18]	1	0.5	1	2.5
Study-13 [29]	1	1	1	3
Study-14 [40]	1	0	1	2
Study-15 [10]	1	0	1	2
Study-16 [41]	1	1	1	2
Study-17 [42]	1	1	1	3
Study-18 [12]	1	1	1	3
Study-19 [6]	1	0.5	1	2.5
Study-20 [19]	1	0	1	2
Study-21 [43]	0.5	1	1	2.5
Study-22 [44]	1	1	1	3
Study-23 [16]	1	1	1	3
Study-24 [15]	1	0	1	2
Study-25 [45]	1	0	1	2
Study-26 [46]	1	1	1	3
Study-27 [47]	1	1	1	3
Study-28 [4]	1	0	1	2
Study-29 [24]	1	1	1	3
Study-30 [48]	0.5	1	1	2.5
Study-31 [25]	1	0.5	1	2.5
Study-32 [49]	0.5	0.5	1	2
Study-33 [23]	1	1	1	3
Study-34 [26]	1	1	1	3
Study-35 [51]	0.5	0	1	1.5
Study-36 [8]	1	0	1	2
Study-37 [52]	0.5	0	1	1.5
Study-38 [53]	0.5	0	1	1.5
Study-39 [27]	1	1	1	3
Study-40 [54]	1	0.5	1	2.5
Study-41 [55]	1	0.5	1	2.5
Study-42 [56]	1	0.5	1	2.5
Study-43 [57]	1	1	1	3
Study-44 [58]	1	1	1	3
Study-45 [59]	1	1	1	3
Study-46 [60]	1	1	1	3
Study-47 [63]	1	0	1	2
Study-48 [62]	1	1	1	3

many devices. Providing dedicated multicast security for constrained IoT environments is critical to the success of IoT services. The efficiency of multicast group communication can be increased. This makes configuring and managing multiple devices at the same time much easier. When a source sends information to a group of recipients in a multicast session, there are numerous challenges such as group privacy and key administration. Security in charge of the session is Group controller (GC) manages authentication, authorization, and access control. Key server (KS) manages the required key material. IP multicast transmission model good at scalability. But the model lacks security measures of access control and protect group communication. Because any receiver can request data without directly contacting the sender which makes sender enable to enforce any access control to manage membership. When IP multicast application is used in IoT use cases, it makes it more difficult to enable access control due to the broadcasting nature of network. Access control is the most crucial security issue in GKM. To get control encryption is needed and to encrypt group communication a shared secret key is used to multiple distributed entities, called group key or TEK. Privacy depends on the safety of group keys. The management of key in group communication is different than managing the key in 1 to 1 communication scenario. The encryption key may be generated through protocol negotiation, such as the Diffie-Hellman key exchange protocol, or it may be generated by one party and then transmitted to the other. The connection is automatically severed, and the encryption key is discarded when one side of a communication disconnects, so key does not need to be updated. But In GKM our main challenge is to assure that all authorized groups have updated keys, as there are multiple receivers. The group communication remains active when a member leaves, and no one can force the departing member to forget the key. So, to prevent ex-members from accessing future communication keys, it must be updated. When a new user joins the group, the group key must also be updated.

Before joining the group, a new member may record the encrypted group communication. To decrypt the stored data, the user joins the group temporarily to obtain the group key. Additionally, data-encryption keys should be regularly replaced. Encrypting a large amount of data with the same key is frowned upon by cryptographers because the data is vulnerable to cryptanalysis attacks. Now GKM includes generate, distribute and update of group key. Resource constraint property of IoT makes GKM a challenge to achieve.

Major problem of group key management in IoT devices are as follows:

A. GROUP KEY MANAGEMENT PRIMITIVES

GKM primitive focuses on two things: Primitive requirements and procedures (as shown in figure. 5).

Most significant group key management scheme which is consider as compatible should has following primitive requirements. They are classified into five types:

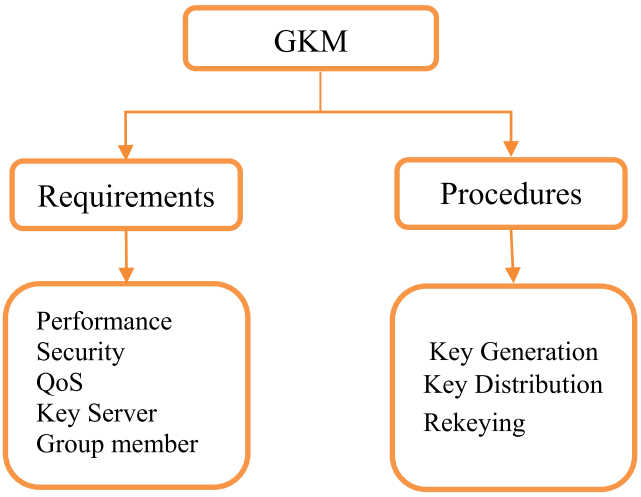

FIGURE 5. GKM primitives.

Performance, Security, QoS (Quality of service), Key management server, and Group Members.

1) PERFORMANCE REQUIREMENT

Robustness: In GKM protocols should have the ability to handle dynamic group size.

1-Affects-N phenomena: Multiple group members are affected when a single membership status changes throughout the join/leave procedure. It decreases network communication iterations.

Availability of services: The operation of key management structures throughout the entire multicast session is unaffected by the failure of a single node.

2) SECURITY REQUIREMENTS

Forward Secrecy: If a member of a group leaves the group, the member should not be able to obtain any future group key or decode any group message after leaving the group.

Backward secrecy: preventing a new member from decrypting group communication that it has received before joining the group.

3) QoS (QUALITY OF SERVICE)

When multicast services are used, there is minimal packet delay and high packet delivery during communication. The packet delivery ratio is calculated using jitters. It plays an important role in key management, minimizing key changes in key management because it affects packet delivery delays.

4) KEY MANAGEMENT SERVER

The re-keying of the group should not be influenced by the large number of messages, it applies to changes in dynamic groups, and it should not be limited by group size.

The amount of time required to encrypt and decrypt the keys to be used should all be considered for the efficient operation of key management protocols.

5) GROUP MEMBERS

To access the memory quickly and work frequently for the key server, there should be a minimum number of keys required for communication.

B. GROUP KEY MANAGEMENT PROCEDURES

The GKM protocol specifies how the group key is generated, distributed, and updated. The most important part of group key management is ensuring the secure and reliable delivery of keying materials to all legitimate members [22]. To do this, efficient key distribution, generation and updating processes must be implemented. Each of these processes must be considered when designing a key management algorithm in resource-constrained network.

1) KEY GENERATION

Creating all the other keys along with the group key refers to key production phase and assists the key allocation controller in distributing the group key to all genuine receivers.

2) KEY DISTRIBUTION

Key allocation refers to the reliable, efficient, and secure distribution of keying materials to group members. Because group members in wireless networks may be geographically dispersed or move from one location to another, the most important task in group key management is ensuring that the group key is delivered to all legitimate members.

3) RE-KEYING

The re-keying process is done to guarantee forward and backward secrecy. Group key and other keys updates. Updated keys sent to the group members. Reducing re-keying costs is more important. Key rekeying is the costliest process out of the three, because it requires the most amount of computation and communication overhead, meaning it requires more time, energy, and resources to generate and distribute the new key.

Since an IoT network can connect a vast number of devices with varying functions, each device may communicate with an undetermined number of other devices. Some messages should be sent to multiple devices simultaneously.

When it is necessary to send messages to multiple recipients, group communication can be used in the network to improve efficiency and communication performance. A group key is distributed among group members to ensure secure group communication [9]. Group key refers to the shared encryption key. It is the key upon which the security of group communication relies entirely. Symmetric encryption algorithms are used for encryption of messages within the multicast group member nodes, but the keys used for these encryption processes play a vital role in group key exchange processes. Group key management mechanism has been employed in several works (architecture of multicast centralized).

TABLE 6. Notation used in Tables 7,10,13.

Notations - Description	Notations – Description
N – Total number of users	n- Total number of members in group.
M - total number of devices	m- Maximum number of sensors
K - key size	k – number of keys
E – Encryption operation	s_k- symmetric key
D – Decryption operation	p – modulus
p_k- public key	t, h- univariate polynomial
g_k- group key	l- number of classes of sensors H- hash operation

In summary, this section provides an overview of the current problems and obstacles in the field of IoT group key management. It also examines the fundamental components of GKM and elucidates the essential processes involved in this area. The study offers valuable insights pertaining to the optimal management of group keys in IoT environments that are limited in terms of resources. Specifically, it investigates aspects such as performance, security, QoS, key management server, and group member requirements, all of which are crucial for ensuring effective group key management. This section serves to address RQ 1 by providing a comprehensive outline of the pertinent concerns and identifying the fundamental components of GKM.

VI. GROUP KEY MANAGEMENT SCHEMES FOR IoT NETWORKS

This section refers to research question 2: ''What type of GKM schemes are proposed for resource constrained IoT networks?''

An IoT network's group key management should be efficient and highly scalable. Because of the limitations of IoT devices, any operation performed by the devices should not exhaust the device's resources. Because traditional protocols are insufficient for resource constrained IoT devices, we require faster and lightweight protocols for secure group communications. As a result, group key management should be implemented effectively. The GKM schemes should use the least amount of memory in each device and distribute the group key with the least amount of communication overhead. An IoT network, on the other hand, is often dynamic and has many members. To deal with these circumstances, group key management should be highly scalable. Multicast communication reduces terminal bandwidth, energy consumption, and processing overhead. Secure message delivery within a multicast group can be obtained by establishing a group key among the authorized members [19]. The SCG schemes are classified in three categories: centralized, decentralized and distributed (as shown in FIGURE. 9)

A. CENTRALIZED GKM SCHEMES

This section discusses the performance and security of centralized SGC schemes. The supplementary materials provide a more comprehensive explanation of the functionality of the schemes under consideration. The comparison is presented in three tables. The notation used in these tables is detailed in Table 6. Tables 7 and 8 provide a summary of the performance of centralized schemes. Figure 6 illustrates a comparison of Centralized (GKM) schemes, highlighting the differences in storage, communication, and computation costs. The graph shows the performance characteristics of various GKM schemes and enables a comprehensive evaluation of their viability and effectiveness. The performance characteristics of the given schemes within the given categories are described and compared using asymptotic notation. By assigning low, medium, and high complexities to storage, communication, and computational costs, the notation provides a framework for comparing the scalability and efficiency of each approach. This notation emphasizes the scaling behavior of the costs relative to the input parameters. The asymptotic notation enables a concise and standardized representation of the complexities, thereby facilitating the evaluation and selection of GKM schemes for secure group communication in resource-constrained scenarios within the given category. Tables 7 and 8 illustrate how various schemes achieve varying levels of performance and employ diverse methods. The security aspects of centralized GKM schemes are summarized in Table 9. Some schemes are significantly more efficient than others, but they may pose unacceptable security risks to the group to achieve such results.

In centralized schemes, the group is managed by a centralized trusted entity known as the Group Controller (GC). This includes managing members joining and leaving as well as the renewal of the group key. The GC is the only entity that has control over all components of an SGC scheme [22]. This centralized approach aims to reduce computational costs and storage requirements for group members [61]. The efficiency of symmetric key encryption and the high security of key selection and generation are advantages of centralized schemes [22]. However, the GC is a potential bottleneck and a single point of failure. If the GC of a centralized system fails, the system ceases to function entirely. As the only entity responsible for the entire group, the GC is the primary target of centralized system attacks [22].

XKFS is distinguished by its high storage, communication, and computational costs, which scale linearly with the number of network nodes. Thus, it is better suited for scenarios with fewer nodes and efficient resource management. However, it may not be suitable for networks with numerous users or limited resources.

The CL-EKM scheme is intended to be lightweight and appropriate for dynamic Wireless Sensor Networks (WSN). It facilitates efficient communication for important updates and management when nodes join or leave a cluster, mitigating the effect of compromised nodes.

TABLE 7. Centralized GKM schemes (part 1).

GKM Schemes	Storage Cost	Communication Cost	Computational Cost
XKFS [57]	High: $O(n)$	High: $O(n)$	High: $O(n)$
CL-EKM [58]	Medium: p_k/g_k	High: $O(n)$	High: $O(n)$
KMGC [59]	Medium: p_k/g_k	High: $O(n)$	High: $O(n)$
SBSA [60]	High: $O(n)$	High: $O(n)$	High: $O(n)$
G-IKEv2 [6]	Low: $O(1)$	Medium: E / D	Medium: g_k
LGKMCP [62]	High: $O(n)$	Low: $O(1)$	Low: $O(1)$

TABLE 8. Centralized GKM schemes (part 2).

GKM Schemes	Cryptography type	Key update frequency	Discussion	
XKFS [57]	Hash, XOR, Symmetric	At membership change	Pros: The scheme minimizes key freshness operations and energy consumption.	Cons: network is vulnerable if the head node fails.
CL-EKM [58]	Asymmetric	At membership change	Pros: Supports efficient key revocation for compromised nodes.	Cons: vulnerable to man-in-the-middle attacks if the nodes do not authenticate each other.
KMGC [59]	Asymmetric	At membership change	Pros: reduces the number of keys stored in nodes.	Cons: Due to the specific requirements for its implementation, the scheme may not be suitable for all types of wireless sensor networks.
SBSA [60]	PRG, symmetric	At membership change	Pros: It does not require any special hardware and does not employ any costly cryptographic operations, making it suitable for hardware-constrained networks.	Cons: Key management is required for the broadcast channel and each node to update the session-specific private key.
G-IKEv2 [6]	AES-128 SHA-256 ECC-256	Periodic	Pros: Secure and scalable protocol that can support multiple cryptographic functions, making it highly adaptable to different applications.	Cons: Still in the early stages of development, so there may be some security issues that need to be addressed before it is ready for widespread use.
LGKMCP [62]	Symmetric, XOR	Periodic	Upon comparison with pre-existing schemes, the proposed scheme has demonstrated efficiency in effectively managing offline users.	

TABLE 9. Comparison of centralized GKM scheme in terms of security features.

GKM Schemes	Forward/ Backward Secrecy	Anti-Collision	Message Confidentiality	Member Authentication	Message Integrity	Group Independence	Instant Rekey	Quantum Resistance
XKFS [57]	✓/✓	X	✓	✓	✓	✓	✓	X
CL-EKM [58]	✓/✓	✓	✓	✓	✓	✓	✓	X
KMGC [59]	✓/✓	X	✓	✓	✓	✓	✓	X
SBSA [60]	✓/✓	✓	✓	✓	✓	✓	✓	X
G-IKEv2 [6]	✓/✓	X	✓	✓	✓	✓	✓	X
LGKMCP [62]	✓/✓	✓	✓	✓	✓	X	✓	X

TABLE 10. Decentralized GKM schemes (part 1).

GKM Schemes	Storage Cost	Communication Cost	Computational Cost
DBGK [36]	Medium: $O(k * K)$	Low: $O(logk)$	Low: $O(logk)$
DLGKM-AC [1]	Device: Low: $O(log_2 n * s_k)$ User: Medium: $O(m * s_k)$	Low: $O(logk)$	Low: $O(logk + M)$
ABP-MAGKE [28]	Low: $(t + h)log_2 p$	Low: $compute\ n\ hash\ outputs.$ $(2 <= n < N)$	Low: $2h - 1$
SCBA [4]	Smartphone: $O(M + m)$ Sensor: $O(m)$	Low: $O(M)$	Smartphone: $O(M)$ Sensor: $O(1)$
DCSGS [13]	High: $O(N * M)$	High: $O(N * M)$	High: $O(N * M)$
LT-SMM [42]	High: $O(n)$	High: $O(n)$	High: $O(n)$

TABLE 11. Decentralized GKM schemes (part 2).

GKM Schemes	Cryptography type	Key update frequency	Discussion	
DBGK [36]	Hash	On-demand	Pros: Rekeying does not rely on the estimated departure time of objects. Instead, a mechanism based on demand is utilized.	Cons: 1-affects-n problem because rekeying only affects active members with valid tickets in each area.
DLGKM-AC [1]	ECC, AES	Membership change	Pros: It supports a scalable IoT architecture, which reduces the load caused by rekeying at the core network, reducing the single point of failure.	Cons: It is not appropriate for applications requiring a high level of security.
ABP-MAGKE [28]	Hash, XOR, Symmetric	Session wise	noninteractive, can speed up the communication process significantly.	
SCBA [4]	ECC	Membership change	Pros: Provides secure authentication and GKM for WBANs, as well as resistance to a variety of attacks.	Cons: Limited by the smartphone's computational power and storage capacity, which may be an issue for some applications.
DCSGS [13]	Asymmetric (roughly same as RSA)	Periodic	When the number of servers (n) in a multi-server environment increase, it is discovered that this scheme is the most efficient when compared to the others.	
LT-SMM [42]	Hash	Membership change	Pros: Offers a secure mobility management scheme that enables secure group communication and efficient group deployment.	Cons: Maintaining the logical tree structure requires a significant amount of computational power and memory, which can be quite costly.

TABLE 12. Comparison of decentralized GKM scheme in terms of security feature.

GKM Schemes	Forward/ Backward Secrecy	Anti-Collision	Message Confidentiality	Message Authentication	Message Integrity	Group Independence	Instant Rekey	Quantum Resistance
DBGK [36]	✓/✓	✓	✓	✓	✓	✓	✓	X
DLGKM-AC [1]	✓/✓	✓	✓	✓	✓	✓	✓	X
ABP-MAGKE [28]	✓/✓	✓	✓	✓	✓	✓	✓	X
SCBA [4]	✓/✓	✓	✓	✓	✓	✓	✓	X
DCSGS [13]	✓/✓	✓	✓	✓	✓	✓	✓	X
LT-SMM [42]	✓/✓	✓	✓	✓	✓	✓	✓	X

TABLE 13. Distributed GKM schemes (part 1).

GKM Schemes	Storage Cost	Communication Cost	Computational Cost
FMPMAKE [14]	High: $O(n)$	High: $O(n)$	High: $O(n)$
GROUPIT [12]	Medium: $O(log_2 m * k)$	Medium: $O(logm * k)$	Medium: $O(E * D * k * log_2(m * k))$
GKA [54]	High: $O(n)$	High: $O(n)$	High: $O(n)$
GKMSFC [47]	Low: $O(k)$	High: $O(n)$	High: $O(n)$
ITSKM [45]	Low: $O(M * K)$	Low: $O(K * k)$	Low: $O(M)$
GKMCA [46]	Low: $O(1)$	Low: $O(K)$	Low: $O(K)$
GKPS [17]	Medium: $(l - 1)\, t$	Low: $(l - 1)$	Medium: $(l-1)(t-1)$ multiplications in Z_N
MIPUF [31]	Low: $O(1)$	High: $O(NlogN)$	High: $O(N)$
SGKES [41]	High: $O(nK)$	High: $O(n)$	High: $O(n)$
GKAT [63]	Medium: $O(E + D)$	Low: $O(H)$	Low: $O(p + H)$

CL-EKM has moderate storage costs but high communication and computation costs, making it more suitable for networks with a moderate number of nodes.

The KMGC plan prioritizes scalability, work efficiency, and the reduction of communication time. Combining master-key and ECC techniques, KMGC reduces the number of keys stored in nodes, increases scalability, and decreases the risk of Denial of Service (DoS) attacks. Additionally, it reduces the amount of energy and time required for crucial negotiations, thereby improving the overall network's effectiveness. As a result of its high communication and computational costs, it may be limited to large-scale deployments.

TABLE 14. Distributed GKM schemes (part 2).

GKM Schemes	Crypto type	Key update frequency	Discussion	
FMPMAKE [14]	Hash	Membership change	Pros: The scheme is secure, with the group key being secure even if m sensors are captured.	Cons: Malicious users may attempt to manipulate the authentication responses or the group key, making the scheme vulnerable. To reduce these risks, the scheme should be used in conjunction with other security measures such as encryption and access control.
GROUPIT [12]	AES-256, ECC-224, SHA-256	Membership change	Pros: Our method is more scalable to the expanding IoT environment in terms of both growth rate and overhead.	Cons: Don't support subscriber independence. No scalability, no forward secrecy
GKA [54]	attribute-based encryption	Periodic	Pros: Ensures that each terminal in the group has a unique key and the same set of attributes, preventing unauthorized access.	Cons: Because each terminal must generate and exchange its own key, GKA can be computationally expensive.
GKMSFC [47]	ECC	Periodic	Pros: Reduce cost, rekeying message overhead, and the dependence on reliable channels.	Cons: Difficult to implement due to the bilinear pair calculations, which include scalar multiplications, exponential modules, and pairing calculations.
ITSKM [45]	Symmetric, Asymmetric	Periodic	Pros: Computational complexity is minimized by combining the physical layer key exchange technique (PLKE) with the cryptographic secret sharing approach.	Cons: It is not appropriate for high-constrained IoT D2D communication because the protocol was designed for low-constrained IoT D2D communication.
GKMCA [46]	Symmetric, Asymmetric	Periodic	Pros: Provides control over load balancing among key servers and overcomes key server failover.	Cons: It necessitates a secure and dependable communication channel between the context-aware security server and the key server cluster.
GKPS [17]	Polynomial, RSA	Probabilistic	Pros: One distinguishing feature of proposed GKPS is that it significantly improves the security of polynomial-based schemes.	Cons: Although the scheme provides probabilistic k-secure security, after capturing a certain number of sensors, the security can still be compromised.
MIPUF [31]	Hash, AES	Membership change	The scheme's security and overhead analysis show that this scheme is not only secure against multiple attack methods, but also low power.	
SGKES [41]	XOR, symmetric	Membership change	Pros: Fast communication due to the use of symmetric keys.	Cons: For some applications, the frequency of key updates may be excessive. - The possibility of denial-of-service (DOS) and reply attack vulnerabilities.
GKAT [63]	Diffie–Hellman problem	Membership change	The results of the performance analysis indicate that the proposed scheme exhibits better efficiency in terms of both computational complexity and computational time when compared to the literature that has been referenced.	

TABLE 15. Comparison of distributed GKM scheme in terms of security features.

GKM Schemes	Forward/ Backward Secrecy	Anti-Collision	Message Confidentiality	Member Authentication	Message Integrity	Group Independence	Instant Rekey	Quantum Resistance
FMPMAKE [14]	✓/✓	✓	✓	✓	✓	✓	✓	X
GROUPIT [12]	✓/✓	✓	✓	✓	✓	✓	✓	X
GKA [54]	✓/✓	✓	✓	✓	✓	✓	✓	X
GKMSFC [47]	✓/✓	✓	✓	✓	✓	✓	✓	X
ITSKM [45]	✓/✓	✓	✓	✓	✓	✓	✓	X
GKMCA [46]	✓/✓	✓	✓	✓	✓	✓	✓	X
GKPS [17]	✓/✓	✓	✓	✓	✓	✓	✓	X
MIPUF [31]	✓/✓	✓	✓	✓	✓	✓	✓	X
SGKES [41]	✓/✓	✓	✓	✓	✓	✓	✓	X
GKAT [63]	x/x	✓	✓	✓	✓	✓	X	X

The SBSA scheme provides a group key establishment protocol and a special key management protocol for secure one-to-many communication in hardware-restricted networks. SBSA guarantees security and effectiveness, but comes with high storage, communication, and computational costs. Even with a comparatively large number of users, it is ideally suited for situations requiring secure communication.

LGKMCP scheme efficiently manages offline users and variations in group membership. While it incurs high storage costs, its communication and computation costs are low. LGKMCP achieves a balance between storage costs and

group administration effectiveness, making it suitable for situations requiring effective group management.

In summary, selecting a centralized GKM scheme includes the consideration of storage, communication, and computational costs, as well as the scheme's suitability for resource-constrained environments and a large amount of users. XKFS is better suited for scenarios with fewer nodes, whereas CL-EKM, KMGC, SBSA, and LGKMCP can accommodate a greater number of members with variable cost and efficiency tradeoffs. Researchers should evaluate these schemes based on their specific network requirements, considering factors such as scalability, efficiency, security, and resource constraints, to choose the most appropriate GKM scheme.

B. DECENTRALIZED GKM SCHEMES

In this section, we discuss the efficiency and safety of decentralized SGC schemes. The supplementary material provides a more comprehensive explanation of the functionality of the schemes under consideration. Table 6 describes the notation employed in these tables. Tables 10 and 11 illustrate how various schemes achieve varying levels of performance and employ a variety of techniques. Table 12 outlines the security features of decentralized GKM schemes. Figure 7 illustrates a comparison of decentralized (GKM) schemes, highlighting the differences in storage, communication, and computation costs.

Some tasks in decentralized architectures are performed by a central unit, while others require collaboration. These decentralized protocols aim for efficiency as well as fault tolerance [22]. The division of group management among SGC is a very common approach in decentralized schemes. The goal of using SGC schemes is to reduce the problem of concentrating all workloads on a single entity [61]. Another approach is to allocate group key generation to a group controller while group key distribution is done collaboratively by all group members [22].

DBGK and DLGKM-AC are decentralized GKM schemes designed for IoT environments with limited resources. They manage group membership efficiently and assure secure multicast communication. DBGK reduces the rekeying burden caused by dynamic and mobile group membership while preserving both backward and forward secrecy. DLGKM-AC reduces the Key Distribution Center's (KDC) rekeying burden and offers a scalable IoT architecture that improves overall efficiency.

ABP-MAGKE and LT-SMM provide lightweight and efficient protocols for secure group communication in WSNs with limited resources. ABP-MAGKE concentrates on membership authentication and pairwise shared key distribution, whereas LT-SMM deals with frequent membership changes. Both protocols have minimal communication and computational costs, which reduces the rekeying burden in WSNs.

SCBA is a decentralized GKM scheme designed specifically for WBANs that ensures secure and efficient communication in medical environments with continuous physiological monitoring. SCBA addresses the need for minimal communication and computational costs, but its specific approach to rekeying is not specified.

DCSGS is a decentralized GKM scheme that is suited for large-scale networks that require secure group communication. It may incur additional storage, communication, and computational costs. In contrast to other schemes, the scheme does not expressly address rekeying overhead.

When evaluating these schemes, researchers must consider specific requirements such as resource limitations, dynamic group membership, secure communication, and rekeying overhead. DBGK and DLGKM-AC are well-suited for resource-constrained IoT environments, whereas ABP-MAGKE and LT-SMM are well-suited for resource-constrained WSNs. SCBA addresses the needs of WBANs, whereas DCSGS focuses on large-scale networks that necessitate secure group communication.

C. DISTRIBUTED GKM SCHEMES

In this section, we discuss the efficiency and safety of distributed SGC schemes. The supplementary material provides a more comprehensive explanation of the functionality of the schemes under consideration. Table 6 describes the notation employed in these tables. Tables 13 and 14 illustrate how various schemes achieve varying levels of performance and employ various methods. Table 15 provides a summary of the security features of distributed GKM schemes. Figure 8 illustrates a comparison of distributed (GKM) schemes, highlighting the differences in storage, communication, and computation costs.

In distributed SGC schemes, group members collaborate to manage the group without the assistance of a central authority. Distributed schemes have the benefit of fault tolerance because no single entity is responsible for distributing and generating keys [22]. However, this comes with increased computational costs for group members and other drawbacks, such as increased energy consumption for the devices [22].

For WSNs with limited resources, FMPMAKE, GKPS, and GKAT provide solutions. FMPMAKE emphasizes efficient membership authentication and key establishment, whereas GKPS emphasizes efficient key distribution and secure communication. GKAT, on the other hand, focuses on securing group communication in WSNs with mobile decline, thereby providing increased resistance to node capture attacks. GKAT stands out among these schemes when mobile sinks are present, as it addresses the unique challenges posed by node capture attacks.

In IoTs environments that are dynamic, GROUPIT, GKMSFC, and SGKES offer solutions. GROUPIT accommodates varying memberships and device counts, efficiently managing key updates and ensuring secure communication with IoT devices with limited resources. GKMSFC reduces communication costs and message overhead for fog computing networks. SGKES prioritizes the establishment of secure group keys in IoT environments with heterogeneous devices

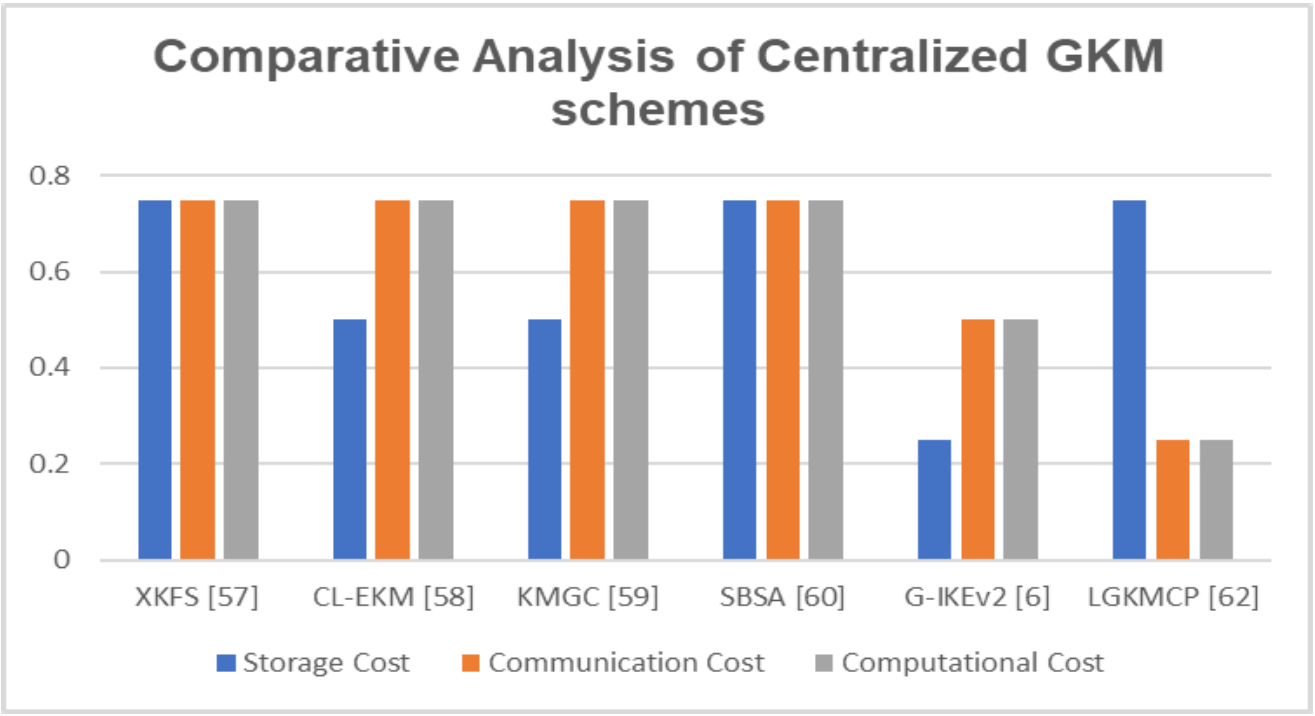

FIGURE 6. Comparative analysis of centralized GKM schemes.

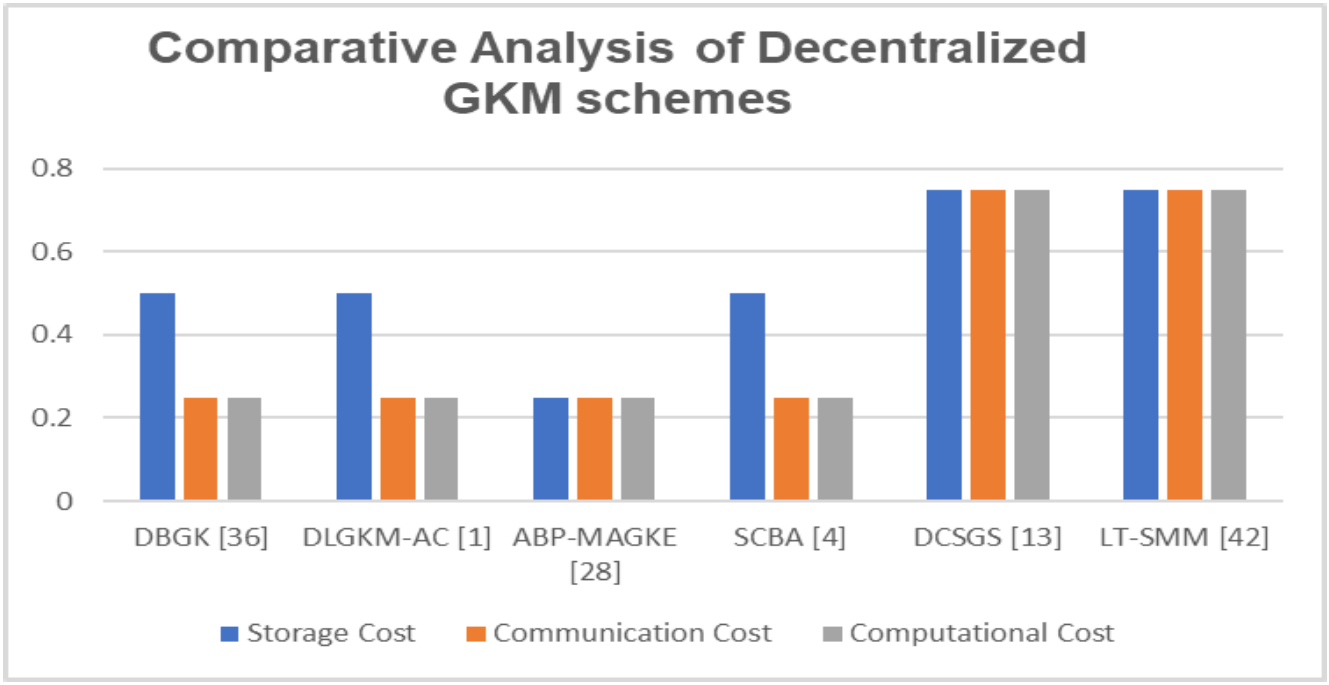

FIGURE 7. Comparative analysis of decentralized GKM schemes.

and dynamic group memberships. GKMSFC stands out in comparison due to its scalability, decreased communication costs, and optimized message overhead. SGKES, on the other hand, offers a specialized solution for IoT environments with heterogeneous devices and dynamic group memberships.

Regarding specific IoTs applications, ITSKM, MIPUF, GKMCA, and GKA stand out. ITSKM addresses group-based communication in low-constrained IoT device-to-device (D2D) networks, specifically in medical assisted living scenarios. MIPUF emphasizes key management in IoT devices that are energy efficient. GKMCA introduces a group key management scheme for clustered IoTs environments, thereby minimizing computational overhead and communication expenses. GKA emphasizes group key

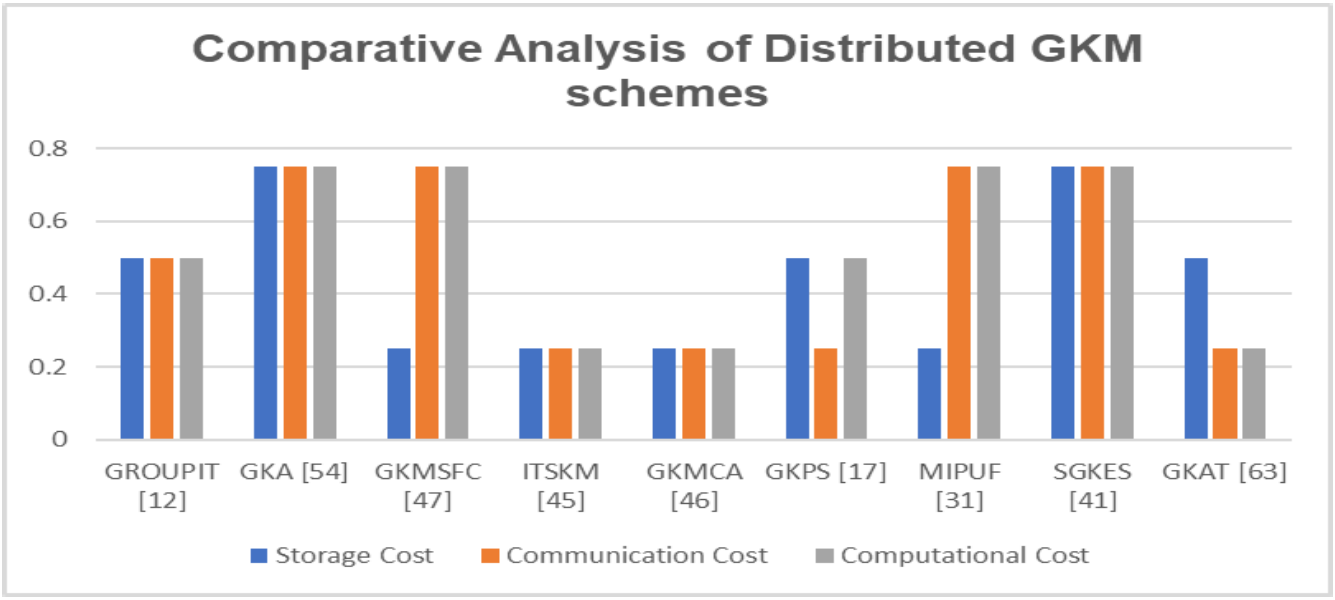

FIGURE 8. Comparative analysis of distributed GKM schemes.

agreement with forward secrecy for the distributed Internet of Things environment. ITSKM stands out among these protocols due to its incorporation of physical layer key exchange, which provides an additional layer of security against unauthorized access.

Comparing the provided GKM schemes reveals that each scheme is tailored to specific environments and applications. GKAT offers enhanced resilience to node capture attacks in scenarios with mobile sinks for resource constrained WSNs. GKMSFC excels in terms of scalability, reduced communication costs, and optimized message overhead in dynamic IoT environments, whereas SGKES provides a specialized solution for heterogeneous devices and dynamic group memberships. ITSKM's incorporation of physical layer key exchange enhances the security and robustness of specific IoT applications. These comparisons emphasize the unique contributions of each scheme to group key management, considering their respective environments' strengths and benefits.

D. SECURITY ANALYSIS OF GKM SCHEMES

In section II: ''Overview of the study'' we defined the security requirements for a secure GKM schemes, now this section presents how the selected secure GKM schemes fulfil the security requirement. Table 8, 11, 14 present the comparison of different centralized, decentralized, and distributed GKM schemes in terms of 8 different security factors.

DBGK [36], DCSGS [13] achieves anti-collision by using a unique identifier for each member of the group, which allows messages sent from different members to be distinguishable and identifiable, also guarantees forward and backward secrecy by preventing collusion attacks from unauthorized users or devices. DLGKM-AC [1] employs a hierarchical architecture comprised of one Key Distribution Centre (KDC) and several Sub Key Distribution Centers (SKDCs), while GROUPIT [12], use a device grouping technique and MIPUF [31] using a novel physically unclonable function (PUF) that allows each device to encrypt its data with a unique key though preventing collisions between devices in different groups. ABP-MAGKE [28],FMPMAKE [14],GKPS [17] done a polynomial calculation to authenticate memberships and establish a secret session key among all communication entities. SCBA [4] employs a certificateless biometric authentication process to achieve anti-collision, message confidentiality, member authentication, message integrity, and group independence. This entails using representative features from electrocardiogram (ECG) records as distinct biometric parameters during the authentication procedure, allowing for efficient identification of participating sensors without any collisions between them.

Next, GKAT [63] includes ciphertext retention, hidden attribute authentication, and multi-policy access. IoT terminals use a key algorithm to produce their public and private keys in the proposed edge-cloud collaborative network architecture. The cloud server also verifies the terminals' private and public keys. Encrypting IoT terminal cryptographic attributes allows the cloud to authenticate them and grant rights for each attribute. The terminal's permissions are used to encrypt FL model parameters and send them to the edge server as sensitive data. The edge server stores the ciphertext's decryption parameters for different FL terminal variants.

By segmenting the shared secret key, GKMSFC [47] achieves anti-collision, message confidentiality, member authentication, message integrity, and group independence. Each segment is then divided into two factors, each with its own production mechanism, allowing for quick key updating

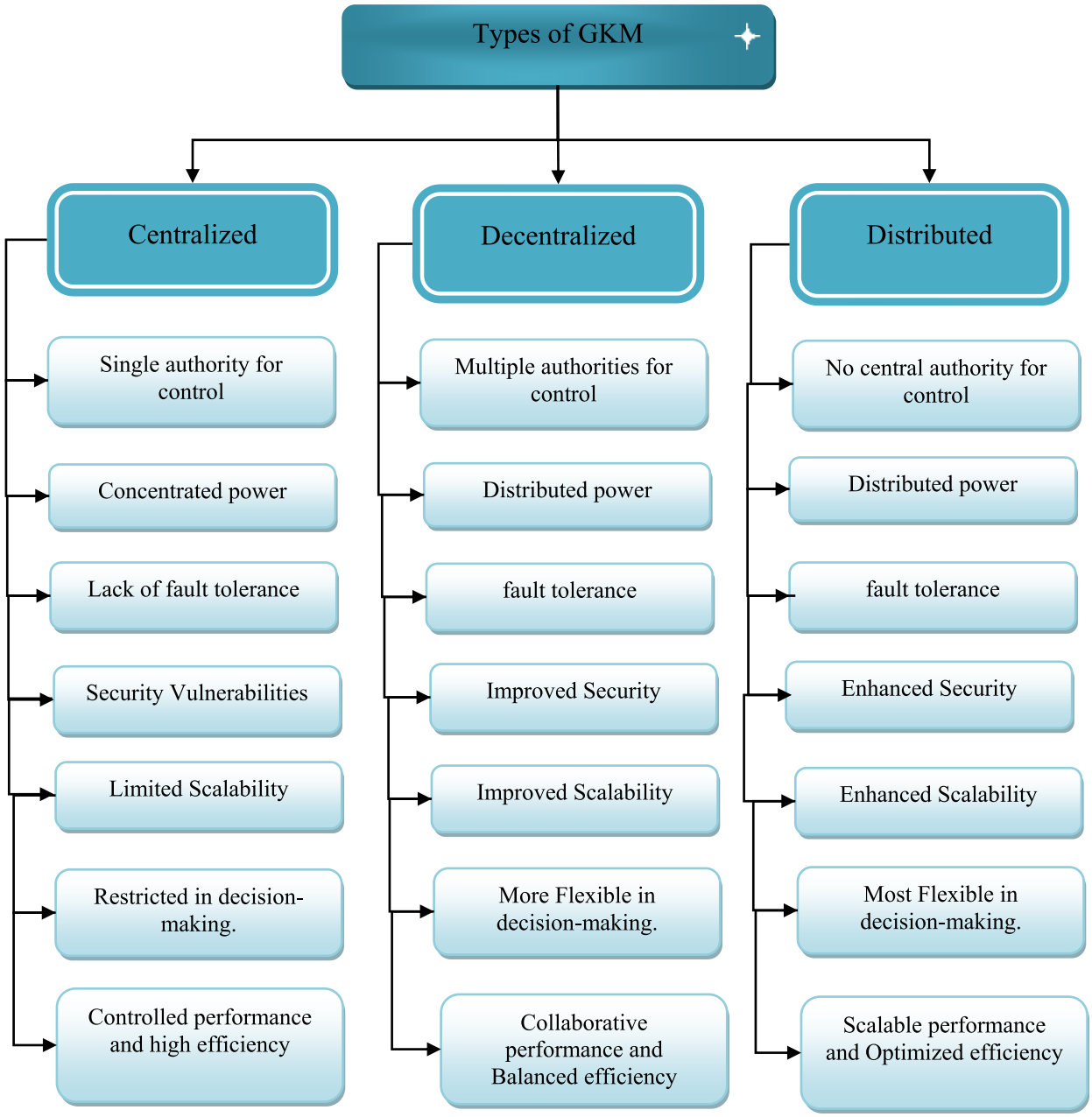

FIGURE 9. Types of GKM schemes.

when a new user joins or leaves the fog node. On the other hand, SBSA [60] achieves all security factors using a special key management mechanism. This involves each node having its own unique session-specific private keys for every broadcast communication session which helps to prevent collisions between different nodes in the network as well as providing secure encryption when sending messages over public networks without compromising user privacy or security.

LGKMCP [62] successfully attains both forward and backward secrecy, thereby guaranteeing the confidentiality of messages. Employing a unique secret key for each user can effectively guarantee both member authentication and message integrity. However, LGKMCP is a centralized key management scheme that relies on the key distribution Centre (KDC) to generate the group key. Consequently, it has no group independence. LGKMCP exhibits a consistent expense for the process of rekeying and upholds a publicly accessible bulletin board to enable instant rekeying.

Further, different schemes maintained their message confidentiality by different techniques, in DLGKM-AC [1] use an efficient key updating process where all keys are completely independent from each other to safeguard data security, while GKPS [17], GROUPIT [12], DCSGS [13], DBGK [36] encryption of all data sent over the network to ensure its privacy. To provide message confidentiality

and integrity ABP-MAGKE [28], FMPMAKE [14] uses user authentication process, which allows only authorized members of the group to access messages sent within it. Member Authentication ensures only legitimate members can join a group communication session and message integrity guarantees that no malicious third party has tampered with any exchanged data or messages in transit between two parties.

However, Message integrity guarantees any changes made to transmitted information will be detected so they cannot go unnoticed, DBGK [36] used a ticket-based system. This entails creating tickets, which are sent to each new joining node and must be validated before being accepted into the network. Furthermore, our protocol relies on an Area Key Management Server (AKMS), which oversees authenticating members within its corresponding area to ensure that only valid nodes can join or leave groups without compromising security and privacy requirements. DLGKM-AC [1] Member authentication is done via master token management protocol which ensures that only authorized users can access the system. Message integrity property is ensured with cryptographic techniques such as digital signatures or message authentication codes for verifying messages sent between devices/users within a group communication session. DCSGS Member Authentication verifies each member of a group before allowing them access and Message Integrity checks for errors or tampering with transmitted information.

Next, Group independence allows for multiple groups with overlapping membership without compromising security. It is achieved in DBGK [36] by generating Traffic Encryption Keys with a one-way function (TEKs). This ensures that the data used as an input cannot be retrieved from the resulting output, implying that disclosing one key does not provide an attacker with any additional information needed to retrieve previous, future, or other keys.

Furthermore, invalidating received tickets when a new member joins or existing members leave helps to ensure the security and privacy of all members within each individual group, DLGKM-AC [1] employs a hierarchical structure comprising a single Key Distribution Centre (KDC) and multiple Sub Key Distribution Centers (SKDCs). During the group communication sessions, the SKDCs oversee the administration of the keys linked to each individual user or device. The division of key management responsibilities among multiple entities serves to prevent any one entity from possessing all session keys, thereby enhancing security measures against unauthorized access to ongoing interactions. FMPMAKE [14], ABP-MAGKE [28] employing k-secure key confidentiality. This means that secure transmissions are possible even in groups of varying sizes, allowing multiple users to join and leave the group without interfering with one another's communications.

Furthermore, Instant Rekey allows users to quickly update their encryption key when needed without having wait all other participants in conversation first, DBGK [36] employing a hierarchical protocol, such as the Logical Key Hierarchy (LKH) [9] or the One-way Function Tree Protocol, which improves on LKH [14]. This approach reduces the number of messages exchanged at the expense of a high computational cost, allowing for quick key updates when member join/leave events or mobility issues within dynamic networks require it. In DCSGS [13] and ABP-MAGKE [28] a distributed key generation protocol is used which enables group members to generate new keys quickly and securely without the need to wait for an external source or administrator, allowing for instant data rekeying in the event of a security breach.

Moreover, all SGC schemes listed in Table 9, 12, 15 employ both symmetric and asymmetric cryptography, which are susceptible to quantum attacks. Symmetric cryptography is influenced by quantum computing. AES and 3DES can be broken by quantum computers. Symmetric cryptography is secure if the key size is raised. For instance, increasing AES's key size from 128 bits to 256 bits can make it safer against quantum attacks. It is essential to observe, however, that this is only a temporary solution, and that post-quantum cryptography should be considered for long-term
security [53].

Finally, forward and backward secrecy properties are guaranteed by preventing collusion attacks against unauthorized users trying to gain access into ongoing communications. SCBA [4] Instant Rekey & Forward/Backward Secrecy properties are enabled through Ciphertext Policy Attribute Based Encryption (CP-ABE) technology which provides dynamic updates when needed ensuring security remains intact even after keys become compromised due revocation etc. DBGK [36] ensure forward secrecy is ensured by invalidating received tickets when a new member joins or an existing one leaves the group, while backward secrecy prevents joining members from accessing communications that occurred before their arrival in the group as well as mobile members not being able decrypt stored messages encrypted with previous traffic encryption keys upon movement from one area another. GKMSFC [47] ensuring both forward and backward security by dividing the shared secret key into segments, which are then split into two factors with their own production mechanism, allowing quick updating when new users join/leave without the need for additional messages from end-users requesting rekeying operations, thereby significantly reducing cost and network load.

This section addresses RQ 2 by investigating various GKM schemes designed for resource-constraint IoT networks. It focuses on the efficiency, scalability, and security features of these schemes. This section examines various GKM schemes, including centralized, decentralized, and distributed approaches, and highlights their respective advantages and disadvantages. In addition, it provides a comparison of these schemes, allowing for a thorough evaluation of their applicability for resource constrained IoT environments.

VII. GROUP KEY MANAGEMENT APPLICATIONS/USAGE AREAS

This section refers to Research question 3: ''What is the application/usage areas?''

The applications and usage areas of these applications in context of SGC schemes are discussed in this section. In recent years, the IoT has gained appeal among end consumers due to its ubiquitous use and range of applications. Applications of the Internet of Things can be found virtually everywhere, including in industrial control, smart healthcare, smart grid, transportation systems, and logistics [62]. IoT is a self-configuring, intelligent system that can connect to a variety of technologies, such as cloud computing, fog computing, radio frequency identification (RFID), and wireless sensor networks (WSN), to share sensory data and control objects with or without human intervention. Due to the inherent promise of this technology, it has already experienced exponential growth in a vast array of use cases across numerous application areas. As experts from across the world continue to examine its capabilities, there is universal consensus that for IoT to reach its full potential, a network architecture that supports security, privacy, and trust must be implemented.

A. INTELLIGENT TRANSPORTATION SYSTEM

An intelligent transportation system (ITS) is a collection of advanced technologies, such as connected vehicles, cloud computing, and the IoT, used to enhance the safety and efficiency of transport networks. ITS systems collect data about traffic conditions using sensors, cameras, and other devices, which can then be analyzed by computers or algorithms for improved decision-making. This reduces traffic congestion on roads and improves road safety by increasing visibility of potential hazards such as accidents and bad weather. In addition, these systems assist in optimizing fuel efficiency by providing real-time information regarding optimal routes based on current traffic conditions. As modern vehicles and communication technologies advanced rapidly, people began to believe that the Intelligent Transportation System (ITS) would be implemented within a decade.

ITS integrates information technology into transportation infrastructure to enhance road safety and traffic flow. Nonetheless, security remains a primary concern for vehicular communication systems (VCSs). With secure group broadcast, this issue can be resolved. Therefore, secure key management schemes are an indispensable network security measure. CAN [63], VANETs and Block chain technology [64] plays an important role in ITS.

1) CONTROLLER AREA NETWORKS (CANs)

ITS utilizes CAN as an essential technology. It allows separate electronic control units (ECUs) within a vehicle to interact with each other, facilitating the interchange of data and directives. This enables automobiles to be more fuel-efficient by letting systems such as engine control and transmission control operate in concert without human intervention. In addition, CAN can contribute to the improvement of safety features in modern automobiles by providing real-time monitoring capabilities for several components, thereby allowing for the early detection of possible problems before they become severe.

CAN messages are multicast, the protocol must support the generation and updating of group keys. For this purpose, group key exchange protocols are needed. Group key exchange is utilized to exchange cryptographic keys between electronic control units on the CAN bus in a secure manner. Multiple nodes (ECUs) within a network can share and agree upon a common secret, which can then be used for secure communication. Using group extensions of standard key exchange protocols, such as elliptic curve Diffie-Hellman, it is possible to establish secure connections with minimal computational overhead, while still providing robust security guarantees against malicious attackers [63]. Cryptographic key distribution between devices Communicating over a publicly accessible medium is a critical component of secure networked system design. The major security flaws of the CAN bus are a lack of confidentiality and integrity, as well as a lack of access control. For encryption and authentication purposes, all proposed cryptographic methods for protecting the CAN bus require that ECUs share a secret key, also known as a group key.

2) VEHICLES AD-HOC NETWORKS (VANETs)

ITS components such as decision-making agents use VANETs data to make intelligent decisions regarding how to reduce traffic and minimize fuel consumption. Group key management is necessary for securing VANET network communications. In the VANET network, group communication occurs when a trusted authority (TA) distributes a group key to all network members. Group keys aid in updating user information when new nodes join or leave the network by distributing updated versions of these keys efficiently without compromising security.

3) BLOCKCHAIN TECHNOLOGY

Blockchain offers Distributed Architecture, Security, and Privacy. It could solve problems like a single point of failure in centralized architecture. The most popular technology eliminates the need for third-party authentication on Peer-to-Peer networks. Active network members validate transactions. Network participants update a ledger with new blocks of transactions to ensure data integrity. In [65], authors address the single point of failure challenge by proposing a blockchain based authenticated group key management protocol for IoT.

Blockchain technology is also essential for Intelligent Transport Systems (ITS) because it provides a secure and dependable method for transmitting encrypted data across network nodes [64]. By spreading keys across heterogeneous domains in a secure manner, this ensures that only authorized

users can access information stored on the blockchain and provides greater security than old, centralized techniques. In Intelligent Transportation System's Vehicular Communication Systems (VCS), group key exchange is required (ITS). This sort of safe key management ensures that only authorized users may access information stored on the chain and provides greater security than previous centralized techniques by spreading keys across diverse domains in a secure fashion. In [64] the suggested framework makes use of blockchain technology to simplify distributed key management and dynamic transaction collecting periods to shorten transfer time during vehicle handoff, making it an appropriate alternative for ITS applications.

The study [64] identifies an unresolved issue that has not yet been addressed. The authors remark that security remains a primary concern in Vehicular Communication Systems (VCS) and present their framework as a potential solution to this problem. However, they recognize that there are further potential solutions for safe key management inside heterogeneous networks that have not been researched or implemented.

B. E-HEALTH CARE MANAGEMENT SYSTEMS

The widespread use of the IoT creates numerous opportunities for the Electric-health care system (E-HCS). In e- healthcare, IoT applications range from remote monitoring to advanced and intelligent sensors to equipment integration. IoT can be used to track patient health, authentication, and data collection.

1) WIRELESS BODY AREA NETWORKS (WBANs)

Wireless body area networks (WBANs), as one of the critical components in the emerging IoT, are capable of monitoring vital physiological and behavioral information of users via wearable sensors, offers great opportunities for the next-generation e-health care systems [4], [66], [67]. This short-range wireless networked device can be placed in, on, or around the body to collect and monitor vital body parameters, which are then transmitted externally to a WLAN, the internet, or a centralized database for processing.

Group key management occurs between the healthcare facility (HC) and the individual controller (PC). The HC is responsible for disseminating important notifications to various patient groups, whereas the PC maintains communication with sensors in a WBAN. During group key management, both parties exchange messages containing secret keys required to encrypt and decrypt network-sent data [66], [67]. Even though many group key agreement schemes have been proposed in recent years, most of these protocols generate a single group's secret key. In the IoT E-HCS, however, more and more communications involve multiple groups, and users can communicate simultaneously with multiple groups. Consequently, traditional one-at-a-time group key establishment protocols based on public keys have a high computational cost and security vulnerabilities.

The Chinese remainder theorem (CRT) is utilized in [67] the proposed protocol for group key management between the host controller (HC) and the personal controller (PC), which also supports batch key update. CRT expedites encryption and decryption by lowering the number of calculations required to encrypt or decrypt data. Additionally, it minimizes storage needs because fewer keys must be saved on both sides, making it more suitable for resource constrained WBAN systems with restricted power capabilities. The motivation for this [67] proposed sensor association approach is coded cooperative data exchange (CCDE). CCDE is a method for enhancing the efficiency of data flow between numerous network nodes. The authors of [4] assume that the three essential components of the WBANs system are the healthcare center (HC), biological sensors, and the user's smartphone as personal controller.

The [4] study identifies a problem with group key management that has not yet been resolved. This is the restricted power capability of conventional WBAN sensors, particularly implanted ones. These constraints hinder their widespread applications in medical settings and make it difficult for healthcare facilities to safely distribute important notifications to diverse patient groups. To address this issue, the authors propose a novel practical WBAN system model with group message broadcasting and a secure and efficient group key management protocol with cooperative sensor association; however, this does not yet address all aspects of the issue.

2) WIRELESS MOBILE ENVIRONMENT (WME)

In e-health systems, WME is utilized to offer secure communication between nodes for patient monitoring. Since wireless networks are used to monitor patients' illnesses and recovery progress, it is crucial that the confidentiality, integrity, and validity of their health records remain protected. Group key exchange is carried out in a mobile wireless environment. This sort of network employs wireless communication technologies, such as cellular networks or Wi-Fi, to facilitate secure communication between nodes for e-health applications. Group key management protocols (GKMPs) are used to create secure channels by providing authentication and data secrecy.

Existing key management protocols cannot securely route these applications due to the resource constraints of wireless mobile environments. Therefore, a novel and improved key management scheme was proposed that aims to provide an efficient solution that minimizes rekeying overhead while ensuring forward and backward secrecy, computational cost, and strong encryption management [68].

This [68] research study proposes a revolutionary master-key management technique for managing keys that enhances the security of healthcare information. The [68] authors also mention some open problem, as additional users join a multicast group, it becomes increasingly challenging for existing protocols and schemes to efficiently

manage keys without compromising performance or security. Providing safe communication between healthcare practitioners and patients, as well as assuring data accuracy with minimal delays, is an additional difficulty when employing telemedicine technologies. Lastly, future study might focus on comparing different cryptographic algorithms to identify which offers the most secure form of healthcare communication in resource-constrained wireless mobile situations. Another paper [69] proposes the Healthcare Key Management (HCKM) framework as a solution. This method offers a safe and privacy-preserving key management approach for e-health systems that minimizes the rekeying overhead of group members while ensuring forward and backward secrecy and strong encryption management. There is a need for more efficient authentication and encryption mechanisms, as well as improved methods for handling dynamic group changes such as user handoffs and node evictions.

In [13] authors describe a use case named as Scenario 2: of central hospital providing a free medical treatment to a specific group of patients. They describe that there scheme can be employed in this scenario to fulfil secure group communication. Figure: 11 refers to dynamic group key distribution model.

C. SMART GRID MANAGEMENT SYSTEM

Utilizing information technology, SMART Grids are altering the conventional services offered by existing electrical grid networks. It maximizes the use of information technology to achieve system efficiency and dependability. In addition to power generation and transmission utilities, smart grids include appliances, meters, sensing devices, and information gateways that function in near real-time [70].

The key components of smart grid technology are as follows:

- *Supervisory Control and Data Acquisition System (SCADA):* This is a system which is used to monitor and control electrical flow. It ensures that electricity is distributed in an efficient and reliable way. It is an essential component of smart grid networks since it assists in the collection and analysis of real-time data from remote places to optimize industrial processes [71].
- *Advanced Metering Infrastructure (AMI):* This is the system that collects, measures, and analyses energy usage data from networks with smart meters.
- *Communication Networks:* These networks allow bidirectional communication between various grid components, including power plants, substations, and consumers. Depending on bandwidth requirements, they could be optical fibers or Ethernet passive optical network.
- *Software & Hardware Components:* These include software applications that manage client accounts, billing systems, etc., as well as hardware components such as routers and switches that enable the safe transfer of data across several nodes in the grid.

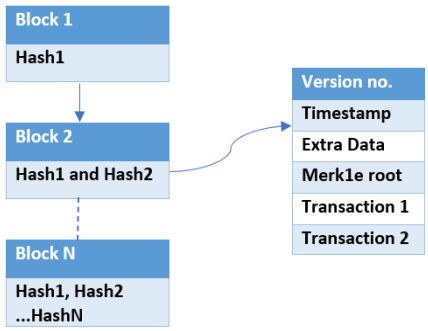

FIGURE 10. Block structure.

GKM is required in AMI and SCADA [74] systems of Smart Grids. Key management is one of the most pressing open issues in smart grids [72]. This necessitates the development of a secure and fast mechanism for access verification of many intelligent gateways and terminal devices. In different research author highlights.

- ➢ Developing efficient authentication mechanisms for secure communication between various grid components, including SMGWs, consumer consuming/generating devices, etc. [70].
- ➢ Designing lightweight security techniques for Smart Grids' wireless sensors with limited resources [70].
- ➢ Investigating new approaches, such as PUF-based KMS, that have not been thoroughly addressed in the literature [70].
- ➢ Construct a GKM protocol that can handle collusion assaults, in which a newly added member attacks in collaboration with an eliminated member [71].
- ➢ Construct a protocol that can handle the dynamic nature of SCADA systems, in which new members can join or leave at any time [71].
- ➢ How to protect the secrecy, integrity, and authentication of multicast communications while employing publish-subscribe topologies.
- ➢ How to efficiently distribute GKs in large clusters with numerous nodes and subgroups, update, or revoke keys safely, and maintain security and performance [73].
- ➢ Data privacy and protection against malicious assaults, such as man-in-the-middle and replay attacks, continue to present obstacles [74].

1) WIRELESS SENSOR NETWORKS (WSNs)

WSNs are networks of small devices that use radio waves or other communication technologies to share environmental data. These sensors monitor temperature, humidity, air quality, and more, making them essential to smart grid systems [73]. WSN data is distinct from most data transmitted in digital communication applications. In [29] WSN gateways are connected to brokers that provide multicast communications through UDP, allowing us to use MQTT for their strategy and evaluate its effectiveness on a testbed comprised of Raspberry PIs and Wi-Fi dongles representing distributed IEDs connected to the server serving as the control center.

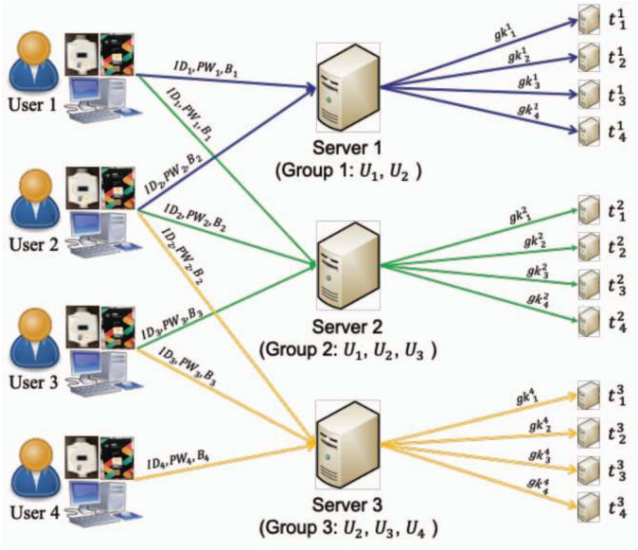

FIGURE 11. Dynamic group key distribution.

Typically, sensors are lacks in memory, battery, and computation power [74]. Therefore, it is more efficient to send multicast messages to a group of devices than to send multiple copies of a unicast message to a device. To secure multicast group communication messages, an efficient key establishment and distribution scheme that preserves the communication's integrity, authenticity, and confidentiality is necessary. The sensor nodes within a wireless sensor network typically exchange data for analysis. This communication exchange is capable of being unicast, broadcast, or multicast (as shown in FIGURE. 12).

• Unicast Communication:

This type of information transfer is useful when 1-to-1 transmission is required. This is a very common type of data transfer over a network.

• Broadcast Communication: Broadcast transmission involves the transmission of data from one or more senders to all receivers within the same network or between networks. This type of transmission is useful for network management packets, such as ARP (Address Resolution Protocol) and RIP (Routing Information Protocol), in which the data must be visible to all devices.

• Broadcast Communication: Multicasting involves multiple senders and multiple receivers for data transfer [47]. Multicast enables servers to simulate and route single copies of data streams to hosts that request them. Multicasting is associated with lower transfer speed utilization in the system for applications such as information replication, task of assignments and sending of orders to a specific group of sensors, inquiries to many sensors, etc.

D. AIR TRAFFIC MANAGEMENT

ATM is the system that controls air traffic in controlled airspace. Monitoring and managing aircraft movements, guaranteeing their safe separation while optimizing their flight paths for efficient travel. The International Civil Aviation Organization (ICAO) establishes global standards for ATM systems, with each nation implementing these standards in accordance with local needs and legislation [75]. The primary elements of an ATM system are communication, navigation, and surveillance technology, as well as operational procedures that ensure flight safety, such as route planning and conflict resolution tactics.

The main components of ATM are [76]:

• Communication technologies:

It allows air traffic controllers and pilots to communicate with one another. This comprises voice radio in addition to data link systems like the LDACS. It is an air/ground communications system that enables the modernization of ATM. It satisfies special requirements for the L-band environment and ATM applications, making it suitable for use in the modernization of air traffic management systems [75].

• Navigation technologies: It provides information regarding an aircraft's position relative to other objects or geographical characteristics. Included are GPS navigation devices and instrument landing system beacons for precise airport approaches.

• Surveillance technologies: It enables ground control operators to monitor an aircraft's location relative to its flight plan path or designated airspace boundaries using radar tracking or Automatic Dependent Surveillance – Broadcast technology (ADS–B).

1) L-BAND DIGITAL AERONAUTICAL COMMUNICATION SYSTEM (LDACS)

Due to the rising amount of air traffic, the current aeronautical communication technologies have reached their limits. To digitalize formerly analogue systems and prepare them for future demands, a process of modernization is undergoing [75]. As part of this transition, the LDACS was developed to replace legacy analogue voice communications to provide secure communication channels for critical infrastructures by implementing Mutual Authentication and Key Establishment protocols as well as Group Key Management procedures that permit authorized users within an LDACS cell or network to access data securely.

GKM is essential since it aids in securing LDACS control channel communications. GKM entails the use of cryptographic mechanisms, such as Mutual Authentication and Key Establishment procedures, to safeguard the data being communicated across a network or among a group of users against unauthorized access [77]. By employing these security measures, LDACS can provide robust cybersecurity when deployed in key infrastructures such as the aviation and aeronautics industries. In [77] this study, author investigate GKM techniques for LDACS control channels and how they promote secure communication within these networks. However, the application of security mechanisms such as GKM approaches on a group-by-group basis, which could provide further protection against hostile actors and illegal access attempts, has not yet been studied. In addition, it investigates

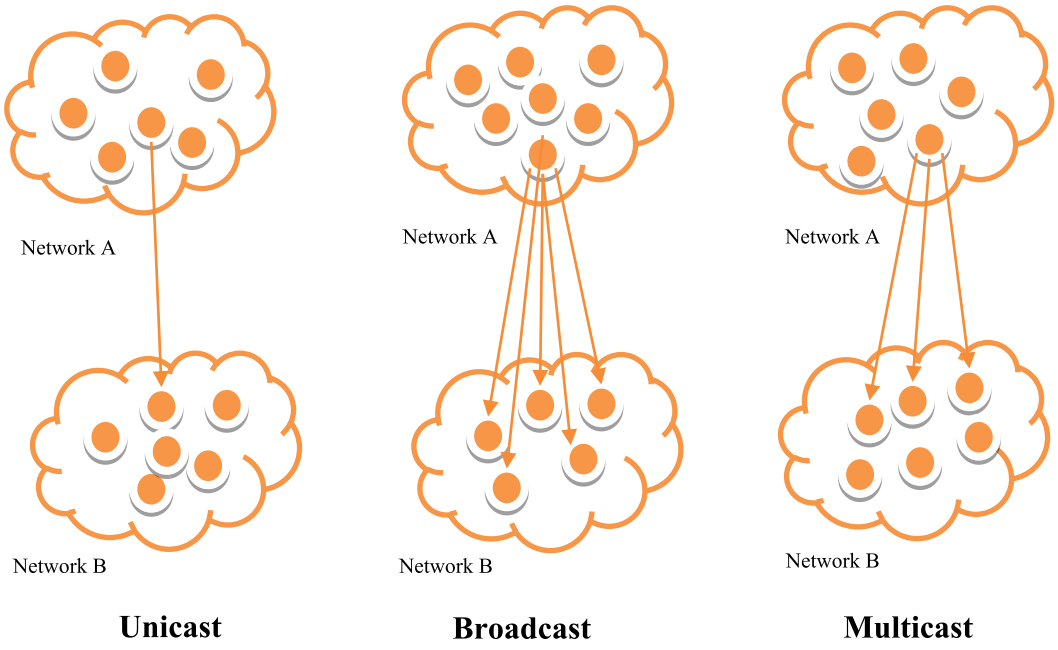

FIGURE 12. Types of communication.

how Chinese Remainder Theorem-based algorithms can be implemented in an LDACS system while accounting for their higher message size needs [77].

Regarding LDACS control channels, there are several possible future paths that could be studied [77]. These include deeper research on the implementation of GKM procedures and how they can provide enhanced security against malicious actors and unauthorized access attempts. In addition, it would be advantageous to research new cryptographic algorithms that may give better performance than solutions based on the Chinese Remainder Theorem while still offering appropriate security for these networks [77].

In short, our investigation into multiple areas of application revealed distinct obstacles and prospective remedies pertaining to protecting group communication and managing cryptographic keys. Although certain challenges have been addressed in previous research papers, there remain unresolved aspects that offer potential for further research and development.

VIII. CONCLUSION

This study conducted an SLR to examine the factors associated with secure group communication in IoT settings. This study concentrated on the existing challenges that researchers in the field of IoT are endeavoring to address with respect to GKM. We examined several GKM approaches that have been put forth for IoT networks that are limited in resources. Based on our examination of 48 studies conducted from 2013 to 2022, it was determined that the majority of GKM schemes utilize conventional cryptographic methods. However, these techniques are insufficient in mitigating the security risks that arise in IoT settings, particularly considering quantum attacks.

The results of our study emphasize the necessity of implementing GKM solutions that are resistant to quantum attacks in the context of IoT settings. The present study identified the domains of application and utilization that involve significant GKM concerns, underscoring the criticality of devising and sustaining robust security frameworks. Through the exploration of these research inquiries, we aim to illuminate the obstacles and constraints inherent in current GKM methodologies, while also establishing a basis for subsequent investigations within this domain.

In brief, our research enhances comprehension of the challenges associated with GKM in the context of the IoT, provides a comprehensive examination of GKM primitives, and investigates various GKM approaches developed for IoT networks with limited resources. The research highlights the importance of implementing quantum-safe measures in IoT settings. It is anticipated that this study will provide guidance to cryptographers in the creation and upkeep of robust security protocols. Subsequent investigations in this domain ought to prioritize the creation and assessment of GKM schemes that are impervious to quantum attacks, while considering the distinct limitations and prerequisites of IoT implementations.

IX. LIMITATIONS AND FUTURE EXTENSION

Post-quantum cryptography is a relatively new field that is presently being researched and developed by the private sector, government security agencies, and the academic community; consequently, its foundations are still being established. Such a circumstance involves that the advancement of the mentioned fields and their application to IoT present significant challenges. With the advent of quantum computing, traditional cryptographic tools become

susceptible to assault, necessitating the development of post-quantum cryptographic tools. Successful post-quantum IoT cryptosystems can improve the security of a variety of fields whose applications heavily rely on resource-constrained and battery-dependent IoT devices, such as home automation [2], [80], smart transportation [66], smart grids [72], [74], [76] and industrial IoT [81], etc.

In future extensions of this work, we intend to concentrate on designing resource-constrained devices and low-bandwidth environment-specific efficient scheme implementations. In addition, we plan to investigate the security analysis of these schemes in the Quantum Random Oracle Model (QROM) to evaluate their resistance to quantum attacks. By incorporating quantum computing principles into our security analysis, we can obtain valuable insight into the robustness and quantum resistance of our proposed schemes. These future extensions will contribute to the development of secure and possible group key management solutions for resource-constrained networks.

REFERENCES

[1] M. Dammak, S.-M. Senouci, M. A. Messous, M. H. Elhdhili, and C. Gransart, "Decentralized lightweight group key management for dynamic access control in IoT environments," *IEEE Trans. Netw. Service Manag.*, vol. 17, no. 3, pp. 1742–1757, Sep. 2020.

[2] G. Kaur and 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 *Computing and Network Sustainability*. Singapore: Springer, Jul. 2017.

[3] E. V. Gravrock. (2019). *How 5G, AI and IoT are Set to Accelerate Digital Transformation*. Boston, MA, USA, Forbes. [Online]. Available: https://www.forbes.com/sites/forbeslacouncil/2019/05/23/how-5g-ai-and-iot-are-set-to-accelerate-digital-transformation/?sh=5fced97183a2

[4] H. Tan and I. Chung, "Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor," *IEEE Access*, vol. 7, pp. 151459–151474, 2019.

[5] G. Perrone, M. Vecchio, R. Pecori, and R. Giaffreda, "The day after mirai: A survey on MQTT security solutions after the largest cyber-attack carried out through an army of IoT devices," in *Proc. 2nd Int. Conf. Internet Things, Big Data Secur.*, 2017, pp. 246–253.

[6] N. G. Felde, T. Guggemos, T. Heider, and D. Kranzlmuller, "Secure group key distribution in constrained environments with IKEv2," in *Proc. IEEE Conf. Dependable Secure Comput.*, Aug. 2017, pp. 384–391.

[7] M. A. Kandi, H. Lakhlef, A. Bouabdallah, and Y. Challal, "An efficient multi-group key management protocol for heterogeneous IoT devices," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–6.

[8] T. Prantl, D. Prantl, A. Bauer, L. Iffländer, A. Dmitrienko, S. Kounev, and C. Krupitzer, "Benchmarking of pre- and post-quantum group encryption schemes with focus on IoT," in *Proc. IEEE Int. Perform., Comput., Commun. Conf. (IPCCC)*, Oct. 2021, pp. 1–10.

[9] D. K. Ajmani, "Homomorphic multicast group key management: Using routing protocol for low power and lossy networks," in *Proc. 4th Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, 2020, p. 6.

[10] T. Prantl, P. Ten, L. Ifflander, S. Herrnleben, A. Dmitrenko, S. Kounev, and C. Krupitzer, "Towards a group encryption scheme benchmark: A view on centralized schemes with focus on IoT," in *Proc. ACM/SPEC Int. Conf. Perform. Eng.*, 2021, pp. 233–240.

[11] A. Kabra, S. Kumar, and G. S. Kasbekar, "Efficient, flexible and secure group key management protocol for dynamic IoT settings," *Netw. Internet Archit.*, vol. 21, no. 25, p. 14, 2020, doi: 10.4108/eai.3-3-2021.168862.

[12] Y.-H. Kung and H.-C. Hsiao, "GroupIt: Lightweight group key management for dynamic IoT environments," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 5155–5165, Dec. 2018.

[13] C.-L. Hsu, "A time bound dynamic group key distribution scheme with anonymous three-factor identification for IoT-based multi-server environments," in *Proc. 15th Asia Joint Conf. Inf. Secur. (AsiaJCIS)*, Taipei, Taiwan, Aug. 2020, pp. 20–21.

[14] Q. Cheng, C. Hsu, Z. Xia, and L. Harn, "Fast multivariate-polynomial-based membership authentication and key establishment for secure group communications in WSN," *IEEE Access*, vol. 8, pp. 71833–71839, 2020.

[15] E. Abirami and T. Padmavathy, "Proficient key management scheme for multicast groups using group key agreement and broadcast encryption," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2017, pp. 1–5.

[16] S. Iqbal, M. L. M. Kiah, A. U. Rehman, Z. Abbas, and B. Daghighi, "DM-GKM: A key management scheme for dynamic group based applications," *Comput. Netw.*, vol. 182, Dec. 2020, Art. no. 107476.

[17] A. Albakri and L. Harn, "Non-interactive group key pre-distribution scheme (GKPS) for end-to-end routing in wireless sensor networks," *IEEE Access*, vol. 7, pp. 31615–31623, 2019.

[18] T. Gebremichael, U. Jennehag, and M. Gidlund, "Lightweight IoT group key establishment scheme using one-way accumulator," in *Proc. Int. Symp. Netw., Comput. Commun.*, 2018, pp. 1–7.

[19] 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.

[20] G. Alagic. (Jan. 31, 2019). *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*. [Online]. Available: https://www.nist.gov/publications/status-report-first-round-nist-post-quantum-cryptography-standardization-process

[21] *NIST*. Accessed: Jul. 7, 2022. [Online]. Available: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[22] Q. Cheng, C. Hsu, and L. Harn, "Lightweight noninteractive membership authentication and group key establishment for WSNs," *Math. Problems Eng.*, vol. 2020, pp. 1–9, May 2020.

[23] Y. Hanna, M. Cebe, S. Mercan, and K. Akkaya, "Efficient group-key management for low-bandwidth smart grid networks," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2021, pp. 188–193.

[24] O. Cheikhrouhou, "Secure group communication in wireless sensor networks: A survey," *J. Netw. Comput. Appl.*, vol. 61, pp. 115–132, Feb. 2016.

[25] R. J. Torraco, "Writing integrative literature reviews: Guidelines and examples," *Human Resource Develop. Rev.*, vol. 4, no. 3, pp. 356–367, Sep. 2005.

[26] A. Piccoli, M.-O. Pahl, and L. Wüstrich, "Group key management in constrained IoT settings," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Rennes, France, 2020, pp. 1–6, doi: 10.1109/ISCC50000.2020.9219619.

[27] H. Gu and M. Potkonjak, "Efficient and secure group key management in IoT using multistage interconnected PUF," in *Proc. Int. Symp. Low Power Electron. Design*, Jul. 2018, pp. 1–6.

[28] T. Prantl, T. Zeck, A. Bauer, P. Ten, D. Prantl, A. E. B. Yahya, L. Ifflaender, A. Dmitrienko, C. Krupitzer, and S. Kounev, "A survey on secure group communication schemes with focus on IoT communication," *IEEE Access*, vol. 10, pp. 99944–99962, 2022, doi: 10.1109/ACCESS.2022.3206451.

[29] A. Piccoli, M.-O. Pahl, S. Fries, and T. Sel, "Ensuring consistency for asynchronous group-key management in the industrial IoT," in *Proc. 16th Int. Conf. Netw. Service Manag. (CNSM)*, Izmir, Turkey, 2020, pp. 1–5, doi: 10.23919/CNSM50824.2020.9269080.

[30] J. Park, M. Jung, and E. P. Rathgeb, "Survey for secure IoT group communication," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, 2019, pp. 1026–1031.

[31] M. Faisal, I. Ali, M. S. Khan, J. Kim, and S. M. Kim, "Cyber security and key management issues for Internet of Things: Techniques, requirements, and challenges," *Complexity*, vol. 2020, pp. 1–9, Dec. 2020, p. 9, 2020.

[32] M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, "A decentralized batch-based group key management protocol for mobile Internet of Things," in *Proc. IEEE Int. Conf. Comput. Inf. Technol., Ubiquitous Comput. Commun., Dependable, Autonomic Secure Comput., Pervasive Intell. Comput.*, 2015, pp. 1109–1117.

[33] T. TshepoMapoka, "Group key management protocols for secure mobile multicast communication: A comprehensive survey," *Int. J. Comput. Appl.*, vol. 84, no. 12, pp. 28–38, Dec. 2013, doi: 10.5120/14629-2985.

[34] B. Kitchenham, "Systematic reviews," Procedures Performing Systematic Rev., Keele Univ., Tech. Rep. TR/SE-0401, 2004, vol. 33, pp. 1–26.

[35] S. Kalhoro, M. Rehman, V. Ponnusamy, and F. B. Shaikh, "Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review," *IEEE Access*, vol. 9, pp. 99339–99363, 2021.

[36] B. Kitchenham, R. Pretorius, D. Budgen, O. P. Brereton, M. Turner, M. Niazi, and S. Linkman, "Systematic literature reviews in software engineering—A tertiary study," *Inf. Softw. Technol.*, vol. 52, no. 8, pp. 792–805, 2010.
[37] M. A. Kandi, H. Lakhlef, A. Bouabdallah, and Y. Challal, "An efficient multi-group key management protocol for Internet of Things," in *Proc. 26th Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, Sep. 2018, pp. 1–6.
[38] S. Sharma and C. R. Krishna, "An efficient distributed group key management using hierarchical approach with elliptic curve cryptography," in *Proc. IEEE Int. Conf. Comput. Intell. Commun. Technol.*, Feb. 2015, pp. 687–693.
[39] T. Gebremichael, U. Jennehag, and M. Gidlund, "Lightweight IoT group key establishment scheme from the one time pad," in *Proc. 7th IEEE Int. Conf. Mobile Cloud Comput., Services, Eng. (MobileCloud)*, Apr. 2019, pp. 101–106.
[40] L. Harn and C.-F. Hsu, "Predistribution scheme for establishing group keys in wireless sensor networks," *IEEE Sensors J.*, vol. 15, no. 9, pp. 5103–5108, Sep. 2015.
[41] S. Naskar, "OTP-based symmetric group key establishment scheme for IoT networks," in *Proc. 47th Annu. Conf. IEEE Ind. Electron. Soc.*, Toronto, ON, Canada, 2021, pp. 1–8. [Online]. Available: https://ieeexplore.ieee.org/xpl/conhome/9588332/proceeding
[42] M. A. Mughal, P. Shi, A. Ullah, K. Mahmood, M. Abid, and X. Luo, "Logical tree based secure rekeying management for smart devices groups in IoT enabled WSN," *IEEE Access*, vol. 7, pp. 76699–76711, 2019, doi: 10.1109/ACCESS.2019.2921999.
[43] K. Nishat and B. R. Purushothama, "Group-oriented encryption for dynamic groups with constant rekeying cost," *ACM Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4120–4137, 2016.
[44] T. Prantl, P. Ten, L. Iffländer, A. Dmitrenko, S. Kounev, and C. Krupitzer, "Evaluating the performance of a state-of-the-art group-oriented encryption scheme for dynamic groups in an IoT scenario," in *Proc. 28th Int. Symp. Model., Anal., Simul. Comput. Telecommun. Syst. (MASCOTS)*, Nov. 2020, pp. 1–8.
[45] U. Mustafa and N. Philip, "Group-based key exchange for medical IoT device-to-device communication (D2D) combining secret sharing and physical layer key exchange," in *Proc. IEEE 12th Int. Conf. Global Secur., Saf. Sustainability*, London, U.K., Jan. 2019, pp. 1–7.
[46] H. Harb, A. William, O. A. El-Mohsen, and H. A. Mansour, "Multicast security model for Internet of Things based on context awareness," in *Proc. 13th Int. Comput. Eng. Conf. (ICENCO)*, Cairo, Egypt, Dec. 2017, pp. 303–309.
[47] M. T. Dong and H. Xu, "Group key management scheme for multicast communication fog computing networks," *Processes*, vol. 8, no. 10, p. 1300, Oct. 2020.
[48] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, "Internet of Things security: Challenges and key issues," *Secur. Commun. Netw.*, vol. 2021, pp. 1–11, Sep. 2021.
[49] O. S. Althobaiti and M. Dohler, "Cybersecurity challenges associated with the Internet of Things in a post-quantum world," *IEEE Access*, vol. 8, pp. 157356–157381, 2020.
[50] T. M. Fernández-Caramés, "From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6457–6480, Jul. 2020.
[51] R. Asif, "Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms," *IoT*, vol. 2, no. 1, pp. 71–91, 2021.
[52] A. Lohachab, A. Lohachab, and A. Jangra, "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks," *Internet Things*, vol. 9, Mar. 2020, Art. no. 100174.
[53] Q. Zhang, L. Zhu, Y. Li, Z. Ma, J. Yuan, J. Zheng, and S. Ai, "A group key agreement protocol for intelligent Internet of Things system," *Int. J. Intell. Syst.*, vol. 37, no. 1, pp. 699–722, Jan. 2022.
[54] R. Prabha, M. Razmah, S. Senthilpandi, S. Suganthi, and S. Sridevi, "Design of a novel group communication framework to improve security in Internet of Things," in *Proc. 8th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, vol. 1, Mar. 2022, pp. 967–970.
[55] M. S. Kumar and T. Purosothaman, "Multivariate broadcast encryption with group key algorithm for secured IoT," *Comput. Syst. Sci. Eng.*, vol. 45, no. 1, pp. 925–938, 2023.
[56] A. Ghafoor, M. Sher, M. Imran, and K. Saleem, "A lightweight key freshness scheme for wireless sensor networks," in *Proc. 12th Int. Conf. Inf. Technol.-New Generat.*, Las Vegas, NV, USA, Apr. 2015, pp. 169–173.
[57] S.-H. Seo, J. Won, S. Sultana, and E. Bertino, "Effective key management in dynamic wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 371–383, Feb. 2015.
[58] X. Bao, J. Liu, L. She, and S. Zhang, "A key management scheme based on grouping within cluster," in *Proc. 11th World Congr. Intell. Control Automat.*, 2014, pp. 3455–3460.
[59] P. Szalachowski and T. H. J. Kim, "Secure broadcast in distributed networks with strong adversaries," *Secur. Commun. Netw*, vol. 8, no. 18, pp. 3739–3750, 2015.
[60] W. Song, M. Liu, T. Baker, Q. Zhang, and Y. Tan, "A group key exchange and secure data sharing based on privacy protection for federated learning in edge-cloud collaborative computing environment," *Int. J. Netw. Manag.*, p. e2225, Mar. 2023, doi: 10.1002/nem.2225.
[61] P. Sharma and B. R. Purushothama, "A lightweight group key management scheme with constant rekeying cost and public bulletin size," *Inf. Secur. J., A Global Perspective*, pp. 1–24, Apr. 2023, doi: 10.1080/19393555.2023.2198737.
[62] R. Barskar and M. Chawla, "A survey on efficient group key management schemes in wireless networks," *Indian J. Sci. Technol.*, vol. 9, no. 14, pp. 1–16, May 2016.
[63] *41.6 Billion IoT Devices Will be Generating 79.4 Zettabytes of Data in 2025*, 2019. [Online]. Available: https://www.helpnetsecurity.com/2019/06/21/connected-iot-devices-forecast/
[64] A. Musuroi, B. Groza, L. Popa, and P.-S. Murvay, "Fast and efficient group key exchange in controller area networks (CAN)," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 9385–9399, Sep. 2021.
[65] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.
[66] C.-M. Chen, X. Deng, W. Gan, J. Chen, and S. K. H. Islam, "A secure blockchain-based group key agreement protocol for IoT," *J. Supercomput.*, vol. 77, no. 8, pp. 9046–9068, Aug. 2021.
[67] A. Rivero-García, I. Santos-González, C. Hernández-Goya, P. Caballero-Gil, and M. Yung, "Patients' data management system protected by identity-based authentication and key exchange," *Sensors*, vol. 17, no. 4, p. 733, Mar. 2017, doi: 10.3390/s17040733.
[68] H. Tan and I. Chung, "A secure and efficient group key management protocol with cooperative sensor association in WBANs," *Sensors*, vol. 18, no. 11, p. 3930, Nov. 2018, doi: 10.3390/s18113930.
[69] A. M. Perumal and E. R. S. Nadar, "Architectural framework of a group key management system for enhancing e-healthcare data security," *Healthcare Technol. Lett.*, vol. 7, no. 1, pp. 13–17, 2019, doi: 10.1049/htl.2018.5114.
[70] S. Iqbal, M. L. M. Kiah, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, and M. A. Alsalem, "Real-time-based e-health systems: Design and implementation of a lightweight key management protocol for securing sensitive information of patients," *Health Technol.*, vol. 9, no. 2, pp. 93–111, Mar. 2019.
[71] A. Ghosal and M. Conti, "Key management systems for smart grid advanced metering infrastructure: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2831–2848, 3rd Quart., 2019.
[72] V. Patil, V. Kulkarni, and H. Patil, "Improvised group key management protocol for SCADA system," in *Proc. Int. Conf. Smart City Emerg. Technol. (ICSCET)*, Mumbai, India, Jan. 2018, pp. 1–4.
[73] O. B. J. Rabie, P. K. Balachandran, M. Khojah, and S. Selvarajan, "A proficient ZESO-DRKFC model for smart grid SCADA security," *Electronics*, vol. 11, no. 24, p. 4144, Dec. 2022, doi: 10.3390/electronics11244144.
[74] Z. Wang, R. Huo, and S. Wang, "A lightweight certificateless group key agreement method without pairing based on blockchain for smart grid," *Future Internet*, vol. 14, no. 4, p. 119, 2022, doi: 10.3390/fi14040119.
[75] H. Nicanfar and V. C. Leung, "Password-authenticated cluster-based group key agreement for smart grid communication," *Secur. Commun. Netw.*, vol. 7, no. 1, pp. 221–233, 2014, doi: 10.1002/sec.726.
[76] M. Benmalek and Y. Challal, "eSKAMI: Efficient and scalable multi-group key management for advanced metering infrastructure in smart grid," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, 2015, pp. 782–789.
[77] N. Mäurer, T. Gräupl, C. Schmitt, G. D. Rodosek, and H. Reiser, "Advancing the security of LDACS," *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 4, pp. 5237–5251, Dec. 2022.
[78] M. Schnell, U. Epple, D. Shutin, and N. Schneckenburger, "LDACS: Future aeronautical communications for air-traffic management," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 104–110, May 2014.

[79] T. Ewert, N. Mäurer, and T. Gräupl, "Group key distribution procedures for the L-band digital aeronautical communications system (LDACS)," in *Proc. IEEE/AIAA 40th Digit. Avionics Syst. Conf. (DASC)*, San Antonio, TX, USA, Oct. 2021, pp. 1–10.
[80] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Jose, CA, USA, May 2016, pp. 636–654.
[81] S. Selvarajan, G. Srivastava, A. O. Khadidos, A. O. Khadidos, M. Baza, A. Alshehri, and J. C.-W. Lin, "An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems," *J. Cloud Comput.*, vol. 12, no. 1, p. 38, Mar. 2023, doi: 10.1186/s13677-023-00412-y.
[82] K. Seyhan, T. N. Nguyen, S. Akleylek, and K. Cengiz, "Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: A survey," *Cluster Comput.*, vol. 25, no. 3, pp. 1729–1748, 2021.

FOUZIA SAMIULLAH received the B.S.I.T. degree (Hons.) from Arab Open University, Saudi Arabia, in 2015, and the M.Phil. degree in computer sciences from the Kinnaird College, Women University Lahore, Pakistan, in 2017. She is currently pursuing the Ph.D. degree with Universiti Tunku Abdul Rahman, Malaysia. Her research interests include the area of cybersecurity, post-quantum cryptography, and the IoT security.

MING-LEE GAN (Member, IEEE) received the B.Eng. degree in electrical and electronics from Universiti Tenaga Nasional, Malaysia, in 2004, the M.Sc. degree in systems engineering and management from the Malaysia University of Science and Technology, in 2006, and the Ph.D. degree in computer science from Universiti Tunku Abdul Rahman, Malaysia, in 2013. He is currently an Assistant Professor at Universiti Tunku Abdul Rahman. His research interests include cybersecurity, blockchain optimization, network path protection, network routing algorithms, and network reliability analysis.

SEDAT AKLEYLEK received the B.Sc. degree in mathematics major in computer science from Ege University, Izmir, Turkey, in 2004, and the M.Sc. and Ph.D. degrees in cryptography from Middle East Technical University, Ankara, Turkey, in 2008 and 2010, respectively. He was a Postdoctoral Researcher at the Cryptography and Computer Algebra Group, TU Darmstadt, Germany, from 2014 to 2015. He was an Associate Professor at the Department of Computer Engineering, Ondokuz Mayis University, Samsun, Turkey, from 2016 to 2022. He has been a Professor at the Department of Computer Engineering, Ondokuz Mayis University, since 2022. He has been with the Chair of Security and Theoretical Computer Science, University of Tartu, Tartu, Estonia, since 2022. His research interests include the areas of post-quantum cryptography, algorithms and complexity, architectures for computations in finite fields, applied cryptography for cyber security, malware analysis, the IoT security, and avionics cyber security. He is an Editorial Board Member of IEEE Access, *Turkish Journal of Electrical Engineering and Computer Sciences*, *Peerj Computer Science*, and *International Journal of Information Security Science*.

Y. AUN is a passionate educator with five years of experience teaching computer networking and cybersecurity subjects. He has developed a reputation for his engaging and interactive teaching style. He founded the Youtube channel AvoTechTV, which garners thousands of views on computer networking videos. Outside teaching, he actively trains students to participate in ICT competitions to showcase their talents at the international level. In research, he has consistently published and contributed to top tiers journals in big data, networking, and cybersecurity. Throughout the years, he also supervised more than 50 undergraduate and postgraduate students combined. He has also served as a Consultant at Vitrox, Huawei, and SimplifyNetwork on several ICT projects; to bridge the gap between industry and academia. He has also served as a reviewer and program committee member for several conferences.