International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/211628 Volume 9, Issue 1, January – February (2022)

REVIEW ARTICLE

A Review of Chronological Development in Group and Hierarchical Key management Schemes in Access Control Model: Challenges and Solutions

Smita Athanere
Computer Engineering, Institute of Engineering and Technology, Devi Ahilya Vishwavidyalaya Indore, Madhya Pradesh, India
smita.athanere@gmail.com

Ramesh Thakur
Master of Computer Application, International Institute of Professional Studies, Devi Ahilya Vishwavidyalaya Indore, Madhya Pradesh, India
r_thakur@gmail.com

Received: 16 December 2021 / Revised: 26 January 2022 / Accepted: 05 February 2022 / Published: 28 February 2022

Abstract – With tremendous growth in communication model, the application dependent on group communication like stock exchange activities, file sharing, war gaming, teleconferencing, pay per view, online education also grown. But in such application security is prime concern. All related things are encrypted via keys and shared to achieve privacy and security. In this paper we identified all methodologies used for group and hierarchical key management and done their analysis. We identified major algorithms for management of group key in communication networks and study several criteria of performance such as computation, storage, and communication overhead at the time of revocation of different users considering evaluation parameters. We find challenges in designing key management algorithm based on various factors. We found power of key management lies in minimization of overhead involved in time and storage at the moment of generation of key, distribution of keys and key updation when a node member joins or leaves the communication group. So it is need to guarantee to safe group key and safe group communication. Research work must be intended toward secure generation of keys, distribution of keys and exchanges of messages in secure environment. Analysis of all methodologies gives an idea for designing a good group key management algorithm either for wired, wireless, IoT devices and cloud platform. This review paper explored various security challenges and issues for handling group key like network compatibility, related to performance and security. This paper enables researcher to take better decisions since all schemes are mentioned in chronological order.

Index Terms – Cryptography, Access Control, Hierarchical Group Key Management.

1. INTRODUCTION

Security is achieved in the current communication system by encrypting data, transferred to different node members from a member by the use of a secret known as shared key treated as key for encryption. To secure communication, members shares keys and perform encryption and decryption. To perform encryption and decryption, each node must have another member's key. This key is encrypted by a public key at the sender side, and at the destination side, this key is decrypted by a member's own private key. In a traditional group key exchange method, a centre for key generation present, key exchanges and encryption/decryption are carried out with each node member sharing a secrets with only the network's authorized users.

Nodes can join and nodes can be deleted over time. When someone sends joining request to the group key server, the server uses the authentication protocol to verify the new member's identity by sharing both the group and auxiliary keys. Rekeying is also used by the key server to deal with leaving members leaving. The foundation for group key management is cryptography. Many group communication applications require group key management as part of their security offerings. As a result, only authorized members can view and interpret the message sent. In multicasting communication, more than one key server is in charge of managing group membership. In a key update message, the RSA key exchange technique is utilized for secure communication [1].

1.1. Major Issues and Related Challenges of Group Key Management

Performance-Related Issues: In a wired or wireless network, group key management must provide efficiency in processes such as communication, key storage, and computation to reduce overhead.

Concerns about Security: The group key is safeguarded when a member enters or exits. Key management is necessary to keep the key, for group and its auxiliary supporting keys safe from non- members and leftover group members.

Problems with the Network: Many ways of group key management exist due to the variety of networks, such as wireless and wired. There isn't a single strategy that works.

1.2. Major Requirements for Group Key Management

We came up with different types of requirements for establishing secure group communication after examining several group key management techniques compatible with wired and wireless networks. We divided the specified criteria into four categories: quality of service (QoS), security, server load minimization, and member load minimizing. This is depicted in Figure 1.

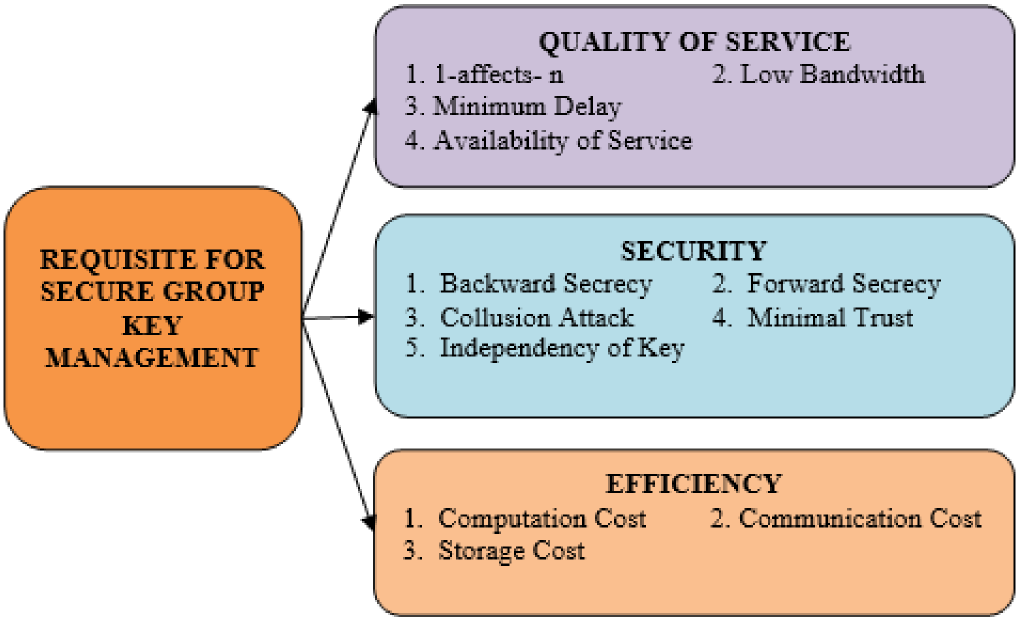

Figure 1 Group Key Management Requirements

1.3. Quality of Service Issues

It refers to, the upkeep of service quality throughout group communication.

1 affect n: Any change or update in single membership, while joining or exiting, affects all other members of the group. It reduces the number of rounds required.

The low bandwidth demand: For the dissemination of key and encrypted messages, the bandwidth requirement should be as low as feasible.

Minimum delay: During message transmission, it is critical that there be as little delay as possible.

Service availability: Services should be available at all times.

1.4. Security Issues

System should take care of safety of keys while new member joining the group leaving the group or whole group communication takes place. Listing is given below-

Backward secrecy: A secure group communication system should preserve this to prevent newly recruited members from decrypting earlier communications.

Forward secrecy: This is a safeguard against a disgruntled member obtaining keys to future group communication and being unable to decipher communications.

Collusion Attack: This is a defense against a scenario in which a group of left members attempts to frame a key for active group communication by reusing old key material.

Minimal Trust: Because proper deployment and operation can be jeopardized, the system should not trust third-party or intermediate entities for services.

Independency of key: Key independence indicates that if one key is revealed, it should not undermine the security of other keys. It's only conceivable if crucial material is self-contained.

1.5. Efficiency Issues

The cost of computing keys, the cost of communicating keys or messages, and the cost of storing keys or messages should all be as low as feasible in group communication performance.

Computation Cost: It the cost in count of bits to evaluate a fresh key, rekey when a member joins, key when a member exit from the group.

Communication Cost: It is the cost involved in distribution of a fresh key.

Storage Cost: The cost of storing the keys created during group communication is known as storage cost. Both sides, of the server and group members it is important.

Key Server and group member side Issue: The key server and members are the most significant elements in group communication, thus the following are the requirements.

Storage requirement: It informs the key server and member node of the minimal number of keys that should be utilized for communication so that they can work efficiently and quickly. As a result, it should be as simple as feasible.

Computation Requirement: If used, the number of keys on the server and among group members must be kept to a minimum. Then only a small amount of computation is required. Low computation reduces both response time and efficiency.

1.6. Problem Statement

Key management for wireless or wired networks is one of the most critical challenges from privacy and security point of view. The study of key management in these networks holds a lot of potential for future research. Key management solutions are now a trade-off for security and performance in exchange for reduced message delivery overhead and memory consumption. Primary purpose of key management systems primary purpose is to offer secure communication over wireless or wired networks with little overhead. All key management approaches were grouped into three groups in this study: centralized, decentralized, and distributed. An overview and tabular breakdown of the main features of numerous key management approaches provided by various scholars has been considered. We also present taxonomy of other main management approaches, together with their benefits and drawbacks. Finally, we discovered that a better key management scheme is still required for open research challenges.

1.7. Motivation

Although much study has been done on the topic of key management for both wireless and wired networks, there are still certain outstanding concerns and issues with the design and development of key management approaches. This section contains a list of open tasks that may be useful to scholars and provide motivation for this article. The following are the unresolved issues:

- The majority of key management techniques are static in nature.
- The key distribution system (KDS) is assumed to be trustworthy in most key management schemes.
- Because the same key is used in the network, validation and verification of the sender's identity is impossible in symmetric key systems. As a result, determining the message's originality and validity becomes challenging.
- A secure channel for secure key exchange is critical.
- When a secret key is generated for new user communication, there is a problem with managing and ensuring the security of the key.

1.8. Objectives

The intention for this research paper is to do a literature evaluation of various approaches provided by various scholars to attain the following objectives:

- Analysis of several key management strategies.
- Determine whether a metric is required to compare various key management strategies.
- Determining which security metrics need to be improved in current key management techniques.
- To summarize exiting key management techniques or algorithms based on numerous important factors or metric.
- To explore various security challenges and issues of group key management

2. ACHIEVING CIA IN GROUP KEY COMMUNICATION

Administration of group communication, key plays a crucial role in ensuring safe data transfer. This covers sub-activities such as group member identification and authentication, granting access to only authorized members, and the keying process when members join or depart the group. Key management must assure confidentiality, integrity, and availability in order to accomplish security [2].

Confidentiality: Any member node that is not on the authorized list of registered users should be unable to decode communications floating in the group, as well as all messages encrypted with the main key of group.

Integrity: The system should be in a stable, error-free condition.

Authentication: Identification of valid users can be done by the authentication process. It is a very important process to secure the whole system. It is highly required for access control.

Scalability: Because new members can join the system, the group's size can grow as the number of members grows. While key management, the scalability property have a one to one consequence on the system's throughput. A system's scalability can be described as its ability to manage growing group sizes.

Reliability: Reliability is the property that ensures secure transport of messages required for rekeying and recovery mechanism for missed rekeying messages in set time duration. In communication, rekey messages can be lost or delayed because of many network problems. If the receiver did not get an indented rekey message then it cannot open and see the messages encrypted by the someone. Left members should not be able to decrypt messages since the sender did not receive a new key. Table 1 displays metrics that can be used to assess security-related algorithms. Abbreviations are provided in Table 2.

Metric	Discussion
Type	Asymmetric or symmetric
Type of Functions	Algorithm needful for Secrecy or integrity of message, authentication, digital signatures
Key size	The Key Length Metric means number of bits required to design a key
Rounds	Because rounds, like word and block size, are not universal properties, they were investigated but may not be a significant statistic.
Complexity	Number of bits needful for key creation
Attack	Brute force-try all combination of keys, Phishing, main in middle etc.
Strength	Capabilities of algorithm based on complexity
1-affects-n	single membership changes, how many affected
Forward secrecy	Safety from old members for future communications
Backward secrecy	Safety from new members for previous communications
Collusion Freedom	A collusion attack means to a situation in which a set of departing members work together to recover the current group key by using old keying materials that they are familiar
Rekey	How quickly can a rekey be completed in order to ensure forward and backward secrecy
Key Independence	Key material used is different for different keys. It keep safe from exposure of one key
Minimal Delays	When multicast services are used, there is a minimum delay during packet transmission and high packet delivery during communication-jitter
Storage Overhead	It means how maximum keys required, ensuring that key-servers operate quickly and have quick access to memory
Availability of Services	Availability of services means the operation of key management structures during the multicast session is unaffected by a single node failure.

Table 1 Overview of Metric Involved in Key Management Schemes

Abbreviations	Explanations	Abbreviations	Explanations
RSA	Rivest–Shamir–Adleman -public Key method	DLKH	Distributed Logical key Hierarchy
QoS	Quality of service	TAKM	Topology Aware Key Management
KDS	Key Distribution System	HKM	Hierarchical Key Management
KDC	Key Distribution Centre	GKS	Group Key Server
GKP	Group Key Packet	CKS	Centralized Key Server
GKEK	Group Key Encryption Key	CKC	Code for Key Calculation

LKH	Logical key Hierarchy	MKMS	multicast key management scheme
KEK	Key Encryption Key (KEK)	MAG	Mobile Access Gateways
OFT	One Way Function	VKE	Visitor Encryption Key
CBT	Core Based Tree	ABE	Attribute-Based Encryption
DKD	Domain Key Distributor	CP-ABE	Encryption -Cipher text Policy Attribute-based
AKD	Area Key Distributors	AHAC	Attribute Hierarchical Access Control
DHCP	Dynamic Host Configuration Protocol	GSA	Group Security Agent
DNS	Domain Name Server	CIA	Confidentiality, Integrity, and Availability
ANN	Artificial neural networks	MITM	Man-in-the-Middle
KNN	K-nearest Neighbor	RBM	Restricted Boltzmann Machines
SVM	Support vector machine	GAN	Generative Adversarial Networks
LR	Logistic Regression	DBN	Deep Brief Networks
CNN	Convolution Neural Networks	DNN	Deep Neural Networks
IDS	Intrusion Detection System	SQL	Structured Query Language

Table 2 Overview of Abbreviations Used

- Confidentiality: Any member node that is not on the authorized list of registered users should be unable to decode communications floating in the group, as well as all messages encrypted with the main key of group.
- Integrity: The system should be in a stable, error-free condition.
- Authentication: Identification of valid users can be done by the authentication process. It is a very important process to secure the whole system. It is highly required for access control.
- Scalability: Because new members can join the system, the group's size can grow as the number of members grows. While key management, the scalability property have a one to one consequence on the system's throughput. A system's scalability can be described as its ability to manage growing group sizes.
- Reliability: Reliability is the property that ensures secure transport of messages required for rekeying and recovery mechanism for missed rekeying messages in set time duration. In communication, rekey messages can be lost or delayed because of many network problems. If the receiver did not get an indented rekey message then it cannot open and see the messages encrypted by the someone. Left members should not be able to decrypt messages since the sender did not receive a new key.

2.1. RSA Algorithm

The RSA algorithm is a fundamental and effective type of public key encryption. In 1978, Rivest, Shamir, and Adleman invented the RSA algorithm, also known as the Rivest, Shamir, and Adleman algorithm. Characteristics of RSA are: There are two different types of key private and public. The integers employed in this method are large enough to make the problem difficult to solve.RSA algorithm is a very popular and widely used one and make use of exponentiation includes in a finite field over integers. Steps of RSA Algorithm

- Step1: Create the RSA modulus in step first

To compute modulus, choose two different prime numbers, a and b, and multiply their products by M (a big number), as given by in N = a*b.

- Step 2: Obtaining a Derived Number (g)

The g must be interpreted as a calculated number greater than 1 but less than (a-1) and (b-1). Except 1, no common factor between (a-1) and (b-1).

- Step 3: Derivation by Public Key Derivation an RSA sharable public key is a paired numbers of p and g.
- Step 4: Derivation of Key (Private)
- Private key x is made up of the numbers a, b, and g. mathematically: 1 mod (a-1) = ed (b-1) Extended Euclidean Algorithm is a sort of algorithm
- An Encryption Formula

Consider the following scenario: a transmitter sends a plain message (text) to a recipient whose sharable public key is (p, g).cipher text can be calculated as

Pe mod p = C

- A Decryption Formula

Decryption is a straightforward procedure that comprises calculation-based analytics. The modulus of the result is computed as if the private key d were associated with receiver

Plaintext = Cd mod p

2.2. Research Tools

This section mentions the research tools for that fit for security oriented researches

- Infection Monkey
- NeSSi2
- CALDERA
- FORESEETI
- Attack IQ
- SKYTHE
- XMCYBER
- Randori
- Picus

2.3. Role of Machine Learning

The role of machine learning in detecting intrusions and extrusions is discussed in this section. Examine the security threats as well. Supervised and unsupervised machine learning algorithms can be categories as two: The supervised learning makes use of the beneficial information in labeled data. Despite the fact that classification is the most common supervised learning activity, as well as the most popular and frequently used in IDS, it is an expensive and time-consuming method of data labeling. However, the absence of adequate labeled data is the fundamental issue in supervised learning.

Unsupervised learning, on the other hand, retrieves significant features as information from unlabeled data, making it far more practical. Data for training is obtained using the same technique. Unsupervised learning approaches, but from the other contrary, typically performs less well in terms of detection than supervised learning methods.

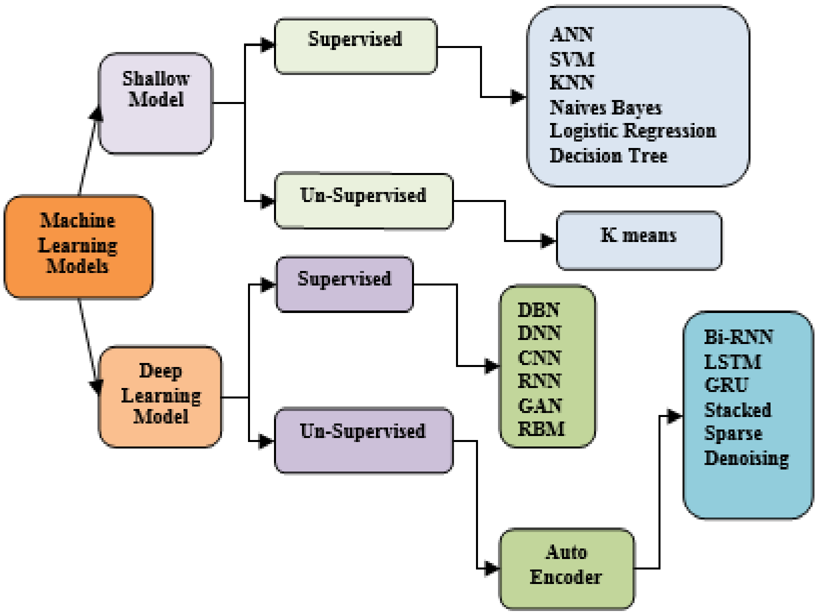

Figure 2 Overview of Machine Learning Approaches Needful in Intrusion Detection

Classical machine learning models, commonly known as shallow models, are helpful to detect intrusions. Only a few of the shallow models encompass artificial neural networks (ANN), support vector machine (SVM), K-nearest neighbor (KNN), naive Bayes, decision trees, logistic regression (LR), clustering, and mixed and hybrid methodologies. The vast of these techniques have been investigated for decades, and their procedure is well-established. These techniques are centered on data management and detection effectiveness.

Supervised learning models such as Auto encoders, Boltzmann restricted machines, and adversarial generative networks, while unsupervised learning methods such as deep brief networks, deep, and recurrent neural networks are created using a diverse deep network of Auto encoders, Boltzmann machines which are restricted and adversarial generative networks. From 2015 to now, the count of studies which makes use of deep learning method based intrusion detection programs has raised dramatically. These models learn to represent features directly from original data such as texts and images. This is an end-to-end process. These models have an advantage over traditional models. Study of these models concentrates on network architecture, hyper parameter selection, and optimization strategy. The most important and liked machine learning algorithms used in IDSs are shown below in Figure 2.

2.4. Security Attacks

A hostile and unauthorized attempt to disclose, steal, or damage data from an information system, such as your website, is designated as a security attack. Its types are as follows.

- Malware: This term refers to a wide range of threats such as viruses, Trojans, worms, ransom ware, and spyware. Malware takes advantage of flaws in the system's security by infecting it with malware by clicking on unsafe links in email attachments. These malicious files prevent essential network components from being accessed. It has the ability to either retrieve crucial data from the system or render it useless.

- Brute-Force Attacks: These involve repeatedly trying different password combinations until they unlock. Once an attacker has access, they have complete control over all vital information.

- Phishing: Phishing is a fairly common practice of intruder, in which an intruder sends a very immense number of bogus emails to users while pretending to be from a reliable source. When you open these emails, malicious software is installed and is able to access your computer's information. Phishing techniques include spear phising, pharrming, and whaling.

- Man-in-the-Middle (MITM): This occurs when an intruder intercepts a transaction between two parties Attackers can steal and modify data by stopping traffic. If an unsecured network is present, they will.

- (DoS): These attacks involve flooding or crowding the server and network with messages in order to jam or overburden the bandwidth and resources. This renders the system unusable, preventing legitimate users from submitting requests. Ping-of-death assaults, TCP SYN flood attacks, teardrop attacks, bonnets, and smurf attacks are examples of denial of service attacks. It is a Denial-of-Service attack.

- SQL Injection: This attack injects malicious code into a server via a structured query command, forcing it to provide vital information. This attack most commonly affects unprotected websites. Secure coding practices, such as using prepared statements in parameterized queries, are a great method to protect your system from SQL injections.

3. STEPS OF HOW TO ESTABLISH GROUP KEY COMMUNICATION

The most fundamental component of a system responsible for reliable group communication framework is proper handling of keys, is dependent on an effective key management techniques. Part of the input information for cryptography methods is contained in the key. The majority of cryptosystems rely on a safe, dependable, and effective key management system. A key might be numeric or non-numeric, and when we apply it to a message, it changes it into an encrypted message. Plaintext can be used to derive the key either implicitly or explicitly. The generated key is also known as an auto key or implicit key derivation when it is part of plaintext. An explicit key, sometimes known as an individual key, is one that is not part of the plaintext. All schemes are shown in Figure 3.

Initialization of keys, agreement between two communicating entities, key distribution, and key cancellation are all required for safe group communication key management [3]. The key activities involved are as given:

- Key Generation: The key creation or generation process entails the establishment of a group key as well as any necessary auxiliary keys. After that, keep track of the key and distribute it to all approved members or genuine members.

- Distribution of Keys: The main key and related supporting keys are delivered to the respective group members throughout the key distribution process. Because group members are mobile and geographically dispersed, it is necessary to provide respective keys securely and promptly. This is the most crucial task to complete; otherwise, keys may be compromised.

- Key Updating (rekeying): During joining of a new member and leaving of exiting member, it needs to send updated keys to members of groups as the group key and related auxiliary keys need to be modified. Rekeying provides forward and reverse secrecy.

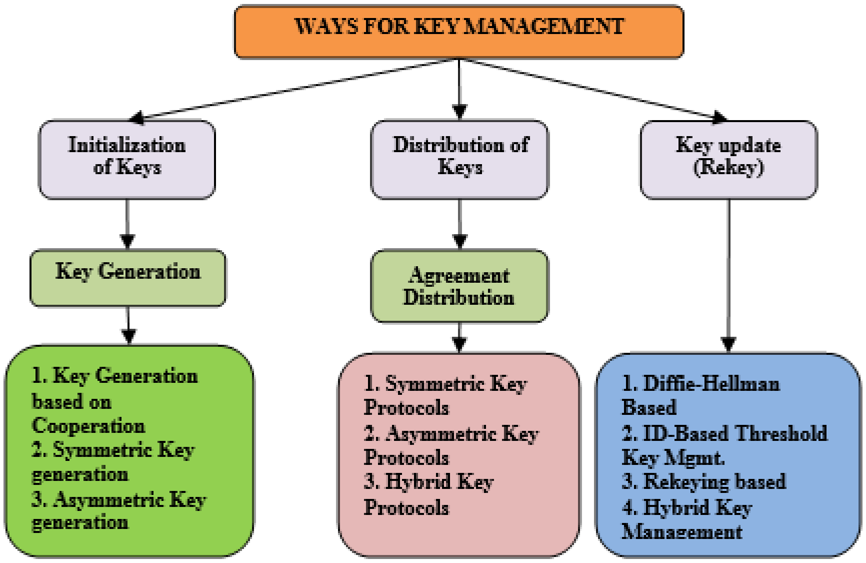

Figure 3 Taxonomy of Group Key Management

4. TYPES OF APPROACHES FOR ESTABLISHING GROUP KEY COMMUNICATION

Literature presents a number of different techniques. Based on how much network architecture is involved in key management, these systems can be split into three categories: network dependent, network independent, and centralized, decentralized and distributed. This is depicted in Figure 4.

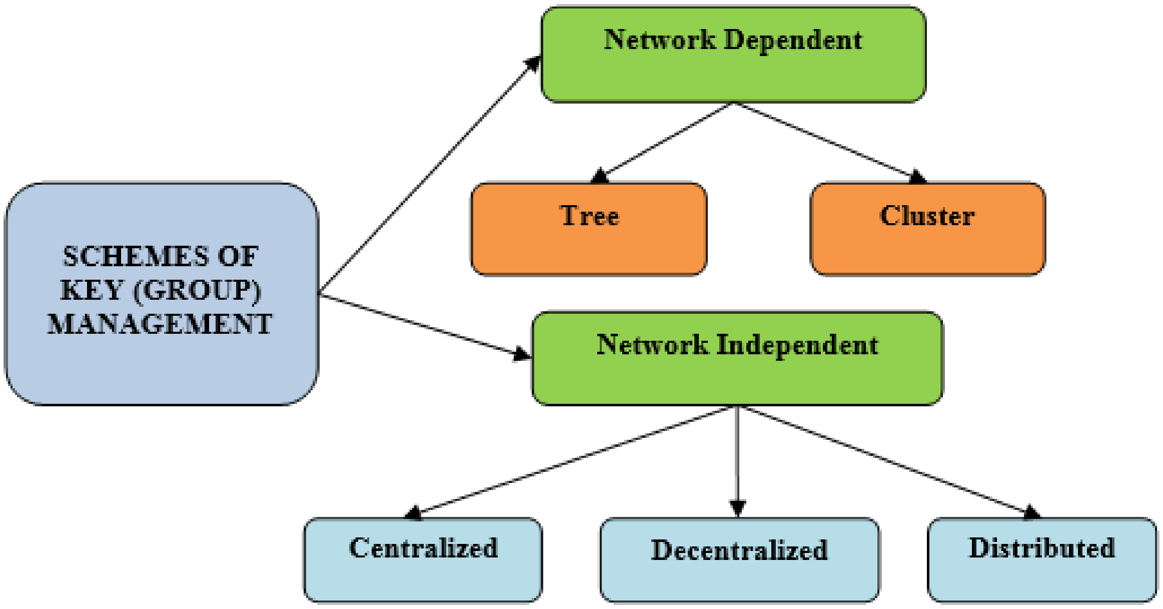

Figure 4 Schemes of Group Key Management

4.1. Centralized Key Management

All group members obtain keys from a central authority under a centralized key management scheme, which is primarily responsible for distribution. A trustworthy third party, a group authority, or a central controller could serve as this central authority. The entire group is under the control of a centralized key approach. Because of the centralized control, this system reduces both the receiver's and sender's computational and storage costs [4]. However, the problem of single-point failure still exists.

Different key management techniques have evolved, but the majority of them use a key distribution center (KDC) to assist group members in joining the group. Group and Traffic keys make a packet of keys (group). When a new member joins the group, KDC sends them a packet including the group key. Forward secrecy is not maintained since all members have permission for the same Group Key Encryption Key (GKEK). After quitting a group, this can only be accomplished by creating a fresh GKEK and distributing it to all the k-1 members [5-9].

A KDC keeps all keys in the shape of a tree in the Logical Key Hierarchy (LKH). There are different sorts of nodes in the tree, such as leaf nodes, intermediate nodes, and root nodes. Child nodes are member nodes of the group, and that leaf node is with the key-encryption key (KEK). Each member has a replica of KEK and may follow it from the last leaf node towards the root node, tracing it via its parent nodes [10].

Each and every node member of the group must have (log$_2$ n) +1 keys, where log$_2$ n is the depth of the key tree from root. It improves LKH since uses function of one way. The blindfolded keys in this KEK are related to nodes. A one-way function generates blinded keys while a mixing function does the mixing. The number of re keyed messages is brings down from two (Log$_2$ n) - just one (log $_2$ n). The function of one way (OFT) chain tree with some modification is another refinement to OFT. Instead of employing a one-way function, this technique generates fresh KEKs using a pseudo-random generator. This key generation, however, is only applicable to members' situations that are about to leave. A chain tree using one-way function chain tree is the term for this method. However, the communication overhead is the same as it was previously [11-14]. An overview of centralized key management algorithms is shown in Table 3. (L- key size in bits, d-height of the tree, i-number of bits in member ID, n-number of the group members.

Approaches	Secure Lock [5]	GKMP [6,7]	LKH [8,9 and 10]	OFT [11,12 and 13]	CFKM [14]
1-affects-n	no	maintains	maintains	maintains	maintains
Forward Secrecy	no	no	maintains	maintains	maintains
Backward Secrecy	no	maintains	maintains	maintains	maintains
Collusion Freedom	maintains	maintains	maintains	maintains	no
Rekey (Multicast)		2L	(2d–1)L	(d+1)L	2iL
			i+2dL	i+(d+1)L	2iL
Storage Overhead	2nL	2L	(2n–1)L	(2n–1)L	(2i+1)L
	2L	2L	(d+1)L	(d+1)L	(i+1)L
Overhead Involved	computation	rekey	storage	storage	storage

Table 3 Overview of Key Management for Centralized Approaches

4.2. Decentralized Key Management

A large group divides into a smaller subgroup. A different controller manages each subgroup. It reduces the workload of a single main controller so ultimately minimizing the issue of a single point of failure. In scalable multicast key distribution, the core-based tree (CBT) multicasting scheme to securely transmit the keys to node members builds the tree. It is used for routing. Primary core authenticates the router. Routers present in the path of any new joining member authenticate the group members. This scheme is not resolving forward secrecy issue, means the only solution is a recreation of the entire new group [15-17].

By separating the entire group into several subgroups, decentralized design provides a means to address the scalability challenge in group key management. It is ideal for large-scale networks like cellular wireless networks, such as the forthcoming 5G. This is the only way to solve the 1-affect-n dilemma. This is about large-scale networks, not about competently distributing vital particulars to different group members. So, this method entails to be associated with other different approaches to have an integrated solution for group key management.

Intra domain key distributor (DKD) which is the main entity. In Intra-Domain Group Key Management. It further divides into Area Key Distributors (AKD). This Area Key Distributor is dealing with their allotted area. DKD generates the key and it is circulated among all group node members through AKDs. This is said as the All-KD group because of the arrangement of DKD and AKDs. This All-KD-Group performs rekey messages when members deletes or add by DKD to all AKDs. The same group key is available for all areas in the given domain. Therefore, there is no requirement to convert data packets from one area to another. In case of the non-availability of AKD, no single members in that area can access the group communication. For naming, authentication, and timing, the network depends on a centralized dedicated server like Dynamic Host Configuration Protocol (DHCP) and Domain name Server (DNS) [18-24]. The overview of decentralized key management algorithms is shown in Table 4.

Approaches	SKMD [15,16,17]	IGKMP [18,19]	Hydra [20]	Kronos [21]	MARKS [22]	DEP [23,24]
Key Independence	maintains	maintains	maintains	no	no	maintains
1-affects-n	maintains	maintains	maintains	no	no	maintains
Local Rekey	no	no	no	no	no	no
Rekey	no	maintains	maintains	no	no	no
Fault Tolerant	no	no	maintains	maintains	maintains	no

Table 4 Overview of Key Management for Decentralized Approaches

4.3. Distributed Key Management

Centralized controller is not needful in the distributed model, the system is fault resilient. Group key generation is done in a contributing fashion, which means that all members contribute their secrets to the calculation of the group key, or it can be provided by a single person. Because key generation necessitates a security mechanism, it cannot be left to group members to generate new members in this system. As a result, members are linked to this random number generator. Above, as group membership varies, the distributed key scheme weakens security. Every member must keep track of the others to see if they are participating in the key generation or not. When the group grows larger, this strategy also affects computation and communication overhead. Key generation can be done in three different ways in this scheme: ring-based, broadcast-based, and virtual topology-based, and hierarchy-based. The number of messages sent is the most important component in this approach. b) The computational cost c) the number of rounds necessary

The group controller is completely removed in DLKH, which stands for distributed logical key hierarchy, and a logical hierarchy key is kept for group members. At the same time, no one knows where the keys are. The concept of a mutual key agreement on sub trees is used in this technique. Both the left sub-group and the right sub-group must be constructed. The Diffie Hellman algorithm is best suited to lessen the number of keys required for all communicating members. At the top level, key = (αkey1key2 mod p) was generated with the help of their two children on the left and right. The acronym CKA stands for Conference Key Agreement. It's an agreement protocol in which all members of the group agree on and contribute to the same group key. K = f (n1, h (n2), h (nm)) is the function for combining in which h is 1- way function. The secret of each communicating member is Ni, and the group size is m. A summary of distributed key management [25-34] algorithms is shown in Table 5 (a), and (b). (l is number of members).

Approaches	Ingemarson [25]	DFM [26]	Octopus [27]	STR [28]	D-LKH [29]
Rounds	l–1	l	2(l–1)/4+2	l	three
Multicasting	-	l	-	l	one
DH Key	maintains	maintains	maintains	maintains	no
Leader Requirement	no	no	maintains	no	maintains

Table 5 (a) Overview of Key Management for Distributed Approaches

Approaches	D-FT [30]	D-OFT [31]	Fiat-Naor [32]	CKA [33]	BD [34]
Rounds	n	log2l	2	3	3
Multicasting	-	-	l	l	2l
DH Key	no	no	maintains	no	no
Leader Requirement	maintains	no	maintains	maintains	no

Table 5 (b) Overview of Key Management for Distributed Approaches

4.4. Tree-Based Key Management

Topology-Aware Key Management (TAKM) is proposed as an effective key administration system for secure multicasting for wireless network and topology-aware key management methodologies in the article (TAKM). It does it by employing the LKH key tree and maintaining three-level hierarchies. A base station, supervisor host, and mobile users are all involved. TAKM efficiently manages member relocation within a cell. Each cell has a WTB connected to it to keep track of previous and new group members. SH is in charge of the BS. The supervisor host is in charge of managing keys in a cell, which includes both key generation and key support. It is built on a centralized structure and has a reduced communication overhead because only useful members are broadcast to. It is at risk to a single point of failure [35-37].

A hybrid or composite key management approach to secure mobile multicast (HKM) for wireless environments topologically similar to TAKM was presented in a paper titled "A composite as well hybrid key administration approach for secure mobile multicast." It is built on two key management trees for managing highly mobile or less mobile members, who minimizes the figure of rekey messages that must be generated upon revocation. Every member has a session key, a set of KEKs, and a set of private keys. The 1-affect-n problem is more prevalent, and bandwidth requirements are higher [38].

The WANG technique, which relies on distributed group key management on underlined network, was proposed in a paper titled "Hybrid group key administration system for secure multicasting for wireless platform", all members of the group are separated into two categories: general members and leader members. It proposed two-tier logical frameworks for cellular network topology. The use of a key server minimizes transmission costs. With independent key servers and group servers, two entities collaborate. At the first level, there is a Group Key Server (GKS), and at the work level, there is a Centralized Key Server (CKS). It fails in forward and backward secrecy, as well as having a high storage cost because each member must keep a huge number of keys. When numerous members begin moving at the same time, there is an authentication delay. The raised figure of levels complicates key governance and increases packet delivery [39].

An approach for handling dynamical topology for group key handling is proposed in a paper titled "simple and secure password method for authentication and craw: Mixture of re-keying and authentication in wireless networks for safe multicasting enhancing the competence of member movement of joining and leaving ", Decentralization is at the root of this. Multicasting information, such as log files of joining and departing operations and inter-cell mobility, is distributed by the main server to the area key servers. AWS is in charge of authentication and key distribution to group members, as well as multicasting information. CRAW is a key management protocol that performs rekeying for each subgroup using Code for Key Calculation (CKC) (a better version of LKH). It's also devoid of the need for a network connection. It is more secure since it uses a one-time password and a one-way function. The server's load decreases. Authentication and group key management are the two phases of the activities. Although there is minimal rekey overhead because keys are not generated when a member transfers to various areas, CKC suffers from the 1-affect-n problem because common TEK is utilized. Because the relay resides on a single primary server during the re-authentication and handoff procedures, it faces single point of failure. Because it doesn't handle multiple authentication issues, it slows down the server [40-43].

In a paper titled MKMS: key management for multi casting scheme in proxy mobile IPV6 networks, multicast extended support for proxy MIPv6 and proxy mobile IPV6 proposed two schemes for multicast key management (MKMS), which are Anchor for Local Mobility (LMA) and Gateway for Mobile Access (MAG) based secure group communication in a decentralized structure for proxy mobile IPV6 networks, in a paper titled MKMS: multicast key management scheme for mobile using proxy IPV6 networks, multicast extended support for proxy MIPv6 and It's a tweaked version of LKH that guarantees both backward and forward secrecy. For mobility management, a mobile using proxy IPV6 is employed to minimize the handover latency raised by a host. MAG promotes a steady environment, while LMA supports dynamic and high-speed networks. The essential components of this design are the Anchor for Local Mobility (LMA) and Gateway for Mobile Access (MAG). LMA relies on MAGs to signal MN and mobile node movements. It is unable to deal with repeated authentications. When a very large number of members begin to move, the problem of tunnel coverage arises [44-45]. An overview of tree-based key handling techniques is shown in Table 6.

Approaches	TMKM[35,36,37]	HKM[38]	WANG[39]	CRAW[40-43]	MKMS[44-45]
Key Dependence	maintains	maintains	maintains	maintains	no
1-affects-n	maintains	maintains	maintains	maintains	maintains
Membership Change	no	no	maintains	no	no
Scalability	maintains	maintains	maintains	maintains	maintains
Security Services	no	no	maintains	no	maintains
Fault Tolerant	no	no	maintains	no	no
Rekey Overhead	maintains	maintains	maintains	yes	no

Table 6 Overview of Key Management for Tree Based Approaches

4.5. Cluster-Based Key Management

Rekeying in Secure Mobile Multicast Communications was a paper that described a decentralized area rekeying system that worked for member mobility. VKE (visitor encryption key) is employed in this case. The controller of server for local keys of group and the key server for domain group controller key server are engaged in this algorithm. DGCKS generates TEK and distributes it to all LGCKS. LGCKS then sends these keys in encrypted form to their corresponding group members in their region (I j) via their keys (KEKi, KEKj), which are handled by GCKS (GCKSi, GCKSj). Each member's CKS contains two lists: an owner list having extra key (EKOL) and a list of static members. The visitor's key owner list (VKOL) is another list that contains information about mobile members. After a member moves, two signals are transmitted at the same time. VEKj local area key was recently distributed by GCKSj to a new member within the area j in a secure manner. Because there are two alternative approaches, one for static and the other for mobility, the overhead of rekeying a region is reduced. It guarantees both forward and backward confidentiality. It suffers from the 1-affect-n problem as a result of widespread TEK, and it is also unable to handle high mobility and numerous requests for rekey operations [46].

A group key management method using cluster, network-dependent approach for wireless environments was proposed in a study titled "Technique of host mobility, for secure group communication in mobile platforms and an implementation of secure group communication in a wireless environment." To handle fluctuating cellular networks and group members, it employs common TEK and a list. The major entities and placement entities are the entities involved. Members of the network are grouped into two tiers based on these entities: area level and domain level. The generation, distribution, storage, and deletion of key materials are all handled by domain-level organizations. Within a domain, area key managers fulfill the same job as domain key managers. To keep track of member mobility, a list called "mob list" was created, which includes moving members, multicast group G, and both areas from and to. In each hands-off process, this is updated. At several levels, it uses a shared symmetric key to guarantee security. It suffers from increased storage overhead due to the use of more keys. It has difficulty with 1-affect-n. It provides backward secrecy rather than forward concealment. It is affected by the area's joining latency. The TEK rekey procedure is done independently [47-49].

In a paper titled "Key handling with Mobility for Host in Adaptive and Dynamic Groups. Key Management Protocol for Wireless Communications," researchers suggested a new key management technique for achieving reliable data transmission in a mobile network platform with nil cost for Rekeying. Since the use of independent TEK per subgroup, it has had no effect. Domain key distributors and area key distributors are involved in this. DKD is in charge of all AKDs, which in turn are in charge of all group members. Clusters are formed from all of the participants. While DKD controls each cluster at the domain level, AKD controls each cluster at the area level. DKD uses common TEK, so there is no requirement for rekey. Each area key distributor keeps two lists, one with current members and the other with prior members' information. Backward and forward secrecy is guaranteed with this technique. If a group member participates in many sessions, additional keys must be stored, increasing storage overhead [50, 51].

KMGM uses graphs to improve the attainment of adaptive clustering for key handling in scalable and dynamic group communications method by involving mobility to the multicast members in the mobile network platform. It supports inter as well as intra-cluster communication. It employs a hybrid approach that includes both independent and common TEK. In the forms of AKD and DKD, members are organized into a hierarchical structure that is decentralized in character. Active and passive forms of AKD exist. The message is simply received and forwarded by passive AKD, which does not make any data changes. Both AKDs keep separate lists of current and former members. When there is an inter-cluster relocation, KMGM additionally focuses on rekeying [52]. The summary of cluster key management algorithms is shown in Table 7.

Approaches	Kellil et al.[46]	GKMF[47-49]	Gharout et al.[50,51]	KMGM[52]
Key Dependence	maintains	maintains	yes-infra cluster	yes-intra cluster
1-affects-n	maintains	maintains	yes-intra cluster	yes-intra cluster
Multiple Membership Changes Support	no	no	no	no
Capability	maintains	maintains	maintains	maintains
Security Services	no	no	maintains	maintains
Fault Tolerant	no	no	maintains	maintains
Rekey Overhead	maintains	maintains	no	no

Table 7 Overview of Key Management for Cluster Based Approaches

4.6. Access Control Scheme Based on Hierarchy

Key administration scheme which is dynamic in nature in wireless networks sing sensors: In a publication, the survey results were reported. Wireless communication networks are far more vulnerable than cable ones, according to this report. As a result, security becomes a top priority in wireless networks, necessitating extra attention and techniques due to the limited capacity of nodes. One way to accomplish this is through key management. This type of key management can be both dynamic and static. The proposed method can help the researcher gain a good understanding of dynamic key management [53].

Pourghebleh gave a presentation titled "A Extensive Study on Techniques for Trust Management in the Internet of Things." It is discussed that trust management in an IoT setting where physical items linked to the internet were converted into smart devices to collect data in this article. A systematic review is offered in this publication. The availability, accuracy, heterogeneity, adaptability, integrity, dependability, privacy, and scalability of selected publications are grouped into four types in this evaluation based on recommendation, prediction, and trust [54].

A survey on threats and authentication needful for security approaches in wireless networks using sensor was published in an article titled same. Data is collected by sensors placed in certain places and sent to other different sensors or another portion of the network in these types of environment. These networks are self-healing and self-managing as they are not reliant on a centralized node and do not follow any set topology. Integrity, privacy, availability, authentication, and no repudiation are all advocated in this work. This study [55] examines current issues and related security practices.

A survey of trust building and management strategies for the Internet of Things was published in a paper titled "Trust Management Techniques for the Internet of Things: A Survey." They mentioned the Internet of Things (IoT) in their study as a method to intelligently connect all gadgets. By providing users' confidence, security, and enjoyment, they can collect a large volume of data. The lack of trust is a fundamental roadblock to the growth of IoT communication, limiting the number of new applications. In this work, a great deal of analysis is done, as well as benefits and drawbacks. As a result, researchers can use this work to extract concepts about how different systems fit together to provide desired functions without having to validate standards. And all of the flaws are highlighted, indicating that more research is needed [56].

A blockchain-based decentralized, lightweight authentication technique for IoT-based devices is described in a paper. The Internet of Things (IoT) is outlined as a collection of diverse, smart, and Internet-connected devices. IoT is used in the open environment to deliver novel services like cities which are smart, smart health managing devices, and communities. Because these instruments generate highly sensitive data, security solutions have become a top priority for ensuring efficiency and safety. This method is decentralized and may be scaled up for larger circumstances. The use of fog computing and public blockchain produced excellent results [57].

According to a paper titled "Dynamic Wireless Sensor Networks (DWSNs)", it is a significant form of data collection from the industrial Internet of Things (IIoT), in which trust can be maintained through reliability and security, according to a paper titled "Dynamic Wireless Sensor Networks (DWSNs). Key administration is performed by a non-reliable base station (BS) that is easy victim due to dynamism. The computing load on base stations and, as a result, on sensors is increased as a result of the key distribution. The block chain-based secure key management scheme (BC-EKM) can address these security and performance concerns. In this case, the block chain is built on the basis of a hybrid sensor network. They then established techniques for node mobility and cluster creation that were both safe. The stake block chain functions as a trust machine, executing base station operations and resolving the issue of non-trust that is tied to it. They've done a lot of simulations and security checks. This analysis demonstrates and confirms that this approach to key management is efficient and effective, as well as increasing security and confidence [58].

Existing group key distribution protocols [59-64] are divided into three categories:

- Centralized method: the entire group is overseen by a single authority.
- A decentralized method divides the group of members into multiple small groups, each of which is overseen by an intermediate key distribution server, and the total group is partitioned into multiple sub-groups, each of which is governed by its own subgroup administrator.
- A distributed method divides the group of members into multiple small groups, each of which is overseen by an intermediate key distribution server, and the total group is partitioned into multiple sub-groups and governed by their respective subgroup administrators. A trusted server maintains a hierarchical tree structure in this technique.

A network flow analysis-based approach was presented by Bhushan and Gupta. It detects and mitigates fraud-related hazards in the context of a multimedia cloud [65]. Some procedures are designed with several different authorities. Attribute-Based Encryption (ABE), which uses attributes to link data throughout the encryption process, is another unique technology. In a key policy-based ABE proposed by Goyal et al. [66], private keys link data and attributes. However, current access control systems have a number of shortcomings, including the inability to deal with collusion assaults. The researchers also propose several novel techniques to prevent collision-based attacks in order to address these difficulties [67].

An Efficient Data Access Control, Attribute-Based Hierarchical Scheme in Cloud Computing [68] uses a cipher text-policy hierarchical attribute-based encryption (CP-ABE) algorithm with secret sharing access method , linear in nature, to achieve fine-grained access control of numerous hierarchical files. They also provide attribute-based hierarchical access control architecture (AHAC). When the qualities of a data requestor match a component of the access control system, the data associated with that portion can be decrypted. It boasts a high level of performance and security. AHAC's efficiency will become even more apparent when the amount of encrypted data grows. The authors proposed that the IBE technique be developed for devices which are resource constraint. In this paper, we look into several attribute authorities, taking into account some related work such as [69-73], which all are handling security challenges in cloud systems.

Li and colleagues introduced a novel distribution system for multicast key that enables multi-level controllers to handle a specific group of people. The suggested method properly balances controller activity, improves distribution of group key dependability, and allows communicating members to establish dynamic sessions besides interruption of the controller [74- 76].

The Iolus architecture was introduced in a study titled Iolus: A structure and Framework for Scalable Secure Multicasting, in which the Group Security Agent (GSA) is in charge of the subgroup [77].

In this technique, Nair provided a mechanism for access control; public-key cryptography is base for file control; public-key cryptography is utilized for identification [78]. Niu et al. [79] proposed an access controlling scheme that allows lightweight computing devices for safe access resources in cloud environment.

Title of the article is Scalable Data Sharing in Cloud Storage which is Hierarchical Access Control. In this research, a new key-aggregate encryption-based hierarchical access control system is presented that allows users to exchange data in cloud storage with any communicating group. In the suggested strategy, the length of used key is not changing and unaffected by the scale of the user structure which is hierarchical. By eliminating the key derivation that is often used in existing hierarchical key allocation techniques [80-82], the suggested strategy makes key administration more convenient.

Approaches	Key Generation Overhead			
	Authority Server		Member Node of Group	
	Joining Phase	Leaving Phase	Joining Phase	Leaving Phase
Classical [59-61]	2	1	0	0
LKH [62- 74]	log2L	log2L-1	0	0
Proposed Scheme 1	log2L	0	0	1
Proposed Scheme 2	log2√L	0	0	1

Table 8 Analysis of Key Generation

Approaches	Total Storage Complexity	
	Authority Server	Authority Server
Classical [59-61]	L	2
LKH [62- 74]	2L	log2L+1
Proposed Scheme 1	2L	log2L+1
Proposed Scheme 2	2√L	log2√L+1

Table 9 Analysis of Storage Overhead

Approaches	Encryption and Decryption Overhead			
	Authority Server	Member Node of Group	Authority Server	Member Node of Group
	Joining Phase	Joining Phase	Leaving Phase	Leaving Phase
Classical [59-61]	2	L-1	1	1
LKH [62- 74]	3. log2L	2. log2L	log2L	log2L
Proposed Scheme 1	log2L+1	log2L-1	1	0
Proposed Scheme 2	log2√L +1	log2√L -1	1	0

Table 10 Analysis of Encryption and Decryption Overhead

Approaches	Communication Overhead
	Domain Authorities to Group Members
Classical [59-61]	Not Supported
LKH [62- 74]	Not Supported
Proposed Scheme 1	$|UAT_{UID}| * \delta$
Proposed Scheme 2	$|UAT_{UID}| * \delta$

Table 11 Analysis of Communication Overhead

Shen's study, Lightweight Certificate Cloud based Less Authentication Technique with Anonymity for Wireless Networks, ensures that only the network manager has access to the user's genuine identity [83].

This study work describes about well-organized and coherent hierarchy-based group communication governing method for a cloud and hierarchical group key management for safe data sharing. To secure cloud uploads and downloads data in the cloud, this system executes cryptographic operations using keys generated by the Key Distribution Server (KDS). In addition, for scalability, the hierarchy for logical key (LKH) technique is basis to keep up a hierarchy shape. The secret values assigned to each group member, as well as the secret values assigned by KDS, are used to generate the group key. Provably secure group communication and secure resource categorization are also recommended [84-87].

Wuu [88] proposed a quorum-based technique in key administration systems for wireless sensors based networks. The quorum-based strategy, in addition to several other strategies, can be employed in a hierarchical multi-authority access system. Group communication [89, 90] discusses a quorum-dependent distributed method for group mutual exclusion

Zkik et al. developed a homomorphic encryption-based authentication and confidentiality technique, as well as a recovery-based approach, for providing secure remote access for mobile users to a multi-cloud server [90].

Now a day's outsourcing of data on cloud storage is very popular. So many organizations attracted towards this to store data on cloud since dealing with huge amount of data. Cloud also allows convenient and efficient data exchange among their authorized clients/users. This type of data sharing raises privacy and security issues since highly sensitive data. This is the actual challenge with cloud based data sharing. Existing security models facing several limitations like single point failure, lack of convenience and efficiency during user revocation and weak data model etc. This research paper proposes two types of schemes a) Non Quorum based scheme b) Quorum based scheme. We incorporated these two schemes with Hierarchical Multi Authority Access Control Scheme (HMA-ACS) to secure data sharing in cloud storage conveniently and efficiently. By experimental and theoretical analysis we have proved that proposed schemes are performing cryptographic key operations efficiently as well secured and adaptive in the standard model in support of access policies. These schemes are assessed and compared with exiting techniques with reference to average encryption and decryption performance, storage overhead and computation overhead. Proposed schemes are ensures data privacy and security and resistant to security threats. The overhead of key creation, storage, encryption/decryption, and communication in various hierarchical key management systems is shown in Tables 8, 9, 10 and 11. (L in number of members).

5. CONCLUSION

We mentioned all the schemes for secure group communication handling that can be further divides into two: like independent and dependent of network. We concluded different key management solutions to achieve CIA mean confidentiality, Integrity, and availability. The main objective of key administration is to make available secure methods for managing cryptographic keying algorithms. Every approach is having its style to secure the data like secure means of generation of keys, distribution of keys, and maintenance like rekeys operation when new members add or exit the group. In-network independent there are three categories to manage keys centralized, decentralized and distributed. In the case of network dependence, two categories are there cluster-based and tree-based. We analyzed major methodologies involved in-group key management found that they all are targeted to minimize the computation cost, communication cost, fault-tolerance to avoid single-point error, key independence, local rekey, and key storage overhead for both the key distribution server and group members. Major challenges are scalability, the 1-affect-N problem, and the trust issue. We need to consider and focus on these challenges of centralized, decentralized, and distributed group key management schemes applied in any platform like wired, wireless, or cloud. The complexity and computational load for key management are purely subjected to the mobility of group members, dynamic environment, bandwidth restrictions, and resources availability of that node. In hierarchical group key management technique, we analyzed overheads related to key generation, encryption /decryption, and total storage complexity at node side and domain authority server over classical methods. Therefore, this paper can help researchers in developing a key management technique.

REFERENCES

[1] Judge, P., M. Amma R., "Security Issues and Solutions in Multicast Content Distribution: A Survey- Network", IEEE, Vol. 17, pp. 30-36. 2003.
[2] Yongdae Kim, Adrian Perrigy, Gene Tsudik, "Simple and Fault-Tolerant Key Agreement for Dynamic Collaborative Groups", Copyright ACM 1-58113-203-4/00/0011, pp. 1-58, 2000.
[3] Kin-Ching Chan, S.H. Gary Chan, "Distributed Servers Approach for Large-Scale Secure Multicast", IEEE Journal on Selected Areas in Communications, Vol. 20, Issue No 8, 2002.
[4] Wei Chi Ku, Shuai Min Chen, Fu Jen, "An Improved Key Management Scheme for Large Dynamic Groups Using One-Way Function Trees", IEEE Conference, Catholic University, 2003.
[5] Chiou, G. H., W. T. Chen, "Secure Broadcast Using Secure Lock", IEEE Transactions on Software Engineering, Vol. 15, Issue No 8, pp. 929-934, August 1989.
[6] Harney, H., C. Muckenhirn, "Group Key Management Protocol (GKMP) Architecture", In RFC 2093, July 1997.
[7] Harney, H., C. Muckenhirn, "Group Key Management Protocol (GKMP) Specification", In RFC 2094, July 1997.

[8] Ritesh Mukherjee, J.William Atwood, “Proxy Encryption for Secure Multicast Key Management”, Proceedings of the 28th Annual IEEE International Conference on Local Computer Networks (LCN‟03) 0742-130/03 $ 17.00 © IEEE Proceedings, 2003.

[9] Wong, C. K., M. Gouda, S. S. Lam, “Secure Group Communications Using Key Graphs”, In Proceeding of ACM SIGCOMM, 1998.

[10] Wong, C. K., M. Gouda, S. S. Lam, “Secure Group Communications Using Key Graphs”, IEEE/ACM Transactions on Networking, Vol. 8, Issue No 1, pp. 16-30, February 2000.

[11] Balenson, D., D. Mc Grew, A. Sherman, “Key Management for Large Dynamic Groups: One Way Function Trees and Amortized Initialization”, Internet-Draft.-balenson-group key management-00.txt, February 1999.

[12] Canetti, R., J. Garay, G. Itkis, D. Micciancio, M. Naor, B. Pink an s., “Multicast Security: Taxonomy and Efficient Constructions”, In Proceeding of IEEE INFOCOM, pp. 708-716, March 1999.

[13] Mc Grew, D. A., A. T. Sherm, “Key Establishment in Large Dynamic Groups Using One-Way Function Trees”, Technical Report TR-0755, World Academy of Science Engineering and Technology, May 1998.

[14] Waldvo gel, M., G. Caroni, D. Sun, N. Weiler, B. Plattner, “Centralized Flat Table Key Management-The Versa Key Framework: Versatile Group Key Management”, IEEE Journal on Selected Areas in Communications (Special Issues on Middleware), Vol. 17, Issue No 8, pp. 1614-1631, August 1999.

[15] Bibo, J. H. Xiulin, “A Survey of Group Key Management”, In International Conference Computer Science and Software Engineering, pp. 994-1002, 2008.

[16] Ballardie A., “Core Based Trees (CBT Version 2) Multicast Routing Protocol Specification”, In RFC 2189, September 1997.

[17] Ballardie, T., I. P. Francis, J. Crowcroft, “Core Based Trees: An Architecture for Scalable Inter-Domain Multicast Routing”, In Proceeding of ACM SIGCOMM, pp. 85-95, 1993.

[18] DeCleene, B., L. Dondeti, S. Griffin, T. Hardjono, D. Kiwior, J. Kurose, D.Towsley, S. Vasudevan, C. Zhang, “Secure Group Communications for Wireless Networks”, MILCOM, June 2001.

[19] Hardjono, T., B. Cain, I. Mong a, “Intra-Domain Group Key Management for Multicast Security”, IETF Internet-Draft, September 2000.

[20] Rafaeli, S., D. Hutchison, “Hydra: A Decentralized Group Key Management”, In 11th IEEE International WETICE-Enterprise Security Workshop, June 2002.

[21] Setia, S., S. Koussih, S. Jajodia, E. Harde, “Kronos: A scalable Group Re-Keying Approach for Secure Multicast”, In IEEE Symposium on Security and Privacy, May 2000.

[22] Briscoe, B., “MarkS: Multicast Key Management Using Arbitrarily Revealed Key Sequences”, In 1st International Workshop on Networked Group Communication, November 1999.

[23] Dondeti, L. R., S. Mukherjee, A. Samal, “Scalable Secure One-to-Many Group Communication Using Dual Encryption”, Computer Communications, Vol. 23, Issue No 17, pp. 1681-1701, November 2000

[24] Dondeti, L. R., S. Mukherjee, A. Samal, “Comparison of Hierarchical Key Distribution Schemes” In IEEE Globecom Global Internet Symposium, 1999.

[25] Ingemarson, D. Tang, C. Wong, “A Conference Key Distribution System”, IEEE Transactions on Information Theory, Vol. 28, No 5, pp. 714-720, September 1982.

[26] Steiner, M., G. Tsudik, M. Waidner, “Diffie-Hellman Key Distribution Extended to Group Communication”, In 3rd ACM Conference on Computer and Communications Security, pp. 31-37, March 1996.

[27] Becker, C., U. Wille, “Communication Complexity of Group Key Distribution”, In 5th ACM Conference on Computer and Communications Security, November 1998.

[28] Kim, Y., A. Perrig, G. Tsudik, “Communication-Efficient Group Key Agreement”, In Proceeding of IFIP SEC, June 2001.

[29] Rodeh, O., K. Birman, D. Dolev, “Optimized Group Rekey for Group Communication Systems”, Network and Distributed System Security, February 2000.

[30] Waldvogel, M., G. Caron i, D. Sun, N. Weiler, B. Plattner, “Distributed flat table-The Versa Key Framework: Versatile Group Key Management”, IEEE Journal on Selected Areas in Communications (Special Issues on Middleware), Vol. 17, Issue No 8, pp. 1614-1631, August 1999.

[31] Dondeti, L., S. Mukherjee, A. Samal, “A Distributed Group Key Management Scheme for Secure Many-to-Many Communication”, Technical Report PINTL-TR-207-99, 1999.

[32] Fiat, A., M. Naor, “Broadcast Encryption”, In CRYPTO’93, LNCS (773), pp. 480-491, 1993.

[33] Boyd, C., “On Key Agreement and Conference Key Agreement”, In Information Security and Privacy: Australasian Conference, LNCS (1270), pp. 294-302, 1997.

[34] Burmester, M., Y. Desmedt, “A Secure and Efficient Conference Key Distribution System,” In: EUROCRYP’94 LNCS (950), pp. 275-286. 1994

[35] Yan, S., W. Trappe, K. J. R. Liu, “An Efficient Key Management Scheme for Secure Wireless Multicast”, In ICC’02. IEEE International Conference Communications, Vol. 2, pp. 1236-1240, 2002.

[36] Yan, S., W. Trappe, K. J. R. Liu, “Topology-Aware Key Management Schemes for Wireless Multicast”, In IEEE Global Telecommunications Conference, GLOBECOM’03, Vol. 3, pp. 1471-1475, 2003.

[37] Lin, L., L. Xueming, C. Yong, “HKM: A Hybrid Key Management Scheme for Secure Mobile Multicast”, International Conference on Networking, Architecture, and Storage, pp. 109-114, 2007.

[38] Yiling, W., L. PhuDun g, B. Srinivasan, “Hybrid Group Key Management Scheme for Secure Wireless Multicast”, International Conference in Computer and Information Science, pp. 346-351, 2007.

[39] Yiling, W., L. PhuDung, B. Srinivasan, “Efficient Key Management for Secure Wireless Multicast”, In 3rd International Conference on Convergence and Hybrid Information Technology, pp. 1131-1136, 2008.

[40] Eidkhani, E., M. Hajyvahab zadeh, S. A. Mortazav, A. N. Pour, “CRAW: Combination of Re-Keying and Authentication in Wireless Networks for Secure Multicast Increasing Efficiency of Member Join/Leave and Movement,” International Journal of Computer Networks & Communications (IJCNC), Vol. 4, pp. 107-128, 2012.

[41] Sandirigama, M., S. Akihiro, M. Noda, “Simple and Secure Password Authentication Protocol”, IEICE Transaction Communication, Vol. 83, pp. 1363-1365, 2000.

[42] Hajyvahab zadeh, M., E. Eidkhani, S. A. Mortazavi, A. N. Pour, “A New Group Key Management Protocol Using Code for Key Calculation: CKC”, In International Conference on Information Science and Applications (ICISA’10), pp. 1-6, 2010.

[43] Ming-Chin, C., L. Jeng-Farn, “MKMS: Multicast Key Management Scheme for Proxy Mobile IPv6 Networks”, In International Conference on Consumer Electronics, Communications and Networks (CECNet’11), pp. 1402-1405, 2011.

[44] Jianfeng, G., Z. Huachun, Z. Hong Ke, H. Luo, “Multicast Extension Support for Proxy MIPv6”, In Consumer Communications and Networking Conference (CCNC’10), 7th IEEE, pp. 1-5, 2010.

[45] Gunda Velli, S., K. Leung, V. Devar Palli, K. Chowdhury, B. Patil, “Proxy Mobile IPv6”, RFC 5213, August 2008.

[46] Kellil, M., J. C. A. Olivereau, P. Janneteau, “Rekeying in Secure Mobile Multicast Communications”, United States Patent Application Publications, US 2007/0143600 A1.25, 2007.

[47] Kiah, L. M., K. M. Martin, “Host Mobility Protocol for Secure Group Communication in Wireless Mobile Environments”, In Future Generation Communication and Networking (FGCN’07), pp. 100-107, 2007.

[48] Kiah, M. L. M., K. M. Martin, “Host Mobility Protocol for Secure Group Communication in Wireless Mobile Environments”, International Journal of Security and its Applications, Vol. 2, pp. 39-52, January 2008.

[49] Kiah, M. L. M., B. Daghighi, “An Implementation of Secure Group Communication in a Wireless Environment”, International Journal of Computer and Electrical Engineering, Vol. 4, December 2012.

[50] Gharout, S., A. Bouabdallah, M. Kellil, Y. Challal, “Key Management with Host Mobility in Dynamic Groups”, In Proceeding of 3rd International Conference on Security of Information and Networks Taganrog Rostov-on-Don, Russian Federation, 2010.

[51] Gharout, S., A. Bouabdallah, Y. Challal, M. Achemlal, “Adaptive Group Key Management Protocol for Wireless Communications”, International Journal of Universal Computer-JUCS, Vol. 18, pp. 874-898, May 2012.

[52] Chung Kei, W., M. Gouda, S. S. Lam, “Secure Group Communications Using Key Graphs”,IEEE/ACM Transactions on Networking, Vol. 8, pp. 16-30, 2000.

[53] Yousefpoor MS, Barati H, “Dynamic key management algorithms in wireless sensor networks: A survey”, Computation Communication, Vol. 134, pp. 52–69, 2019.

[54] Pourghebleh B, Wakil K, Navimipour NJ, “A comprehensive study on the trust management techniques in the internet of things”, IEEE Internet ,Vol. 6, Issue No 6, pp.9326–9337, 2019

[55] A. Karakaya, and S. Akleylek, “A survey on security threats and authentication approaches in wireless sensor networks”, In 6th IEEE international symposium on digital forensic and security (ISDFS), pp. 1-4, 2018.

[56] Din IU, Guizani M, Kim BS, Hassan S, Khan MK, “Trust management techniques for the Internet of Things: a survey”, IEEE Access Vol. 7, pp. 29763-29787, 2018.

[57] U. Khalid, Md. Asim, T. Baker, P. C. K. Hung, Md. A. Tariq, and L.Rafferty, “A decentralized lightweight blockchain-based authentication mechanism for IoT systems”, Cluster Computing, Vol. 23, Issue No 3, pp. 2067-2087, 2020.

[58] Y. Tian, Z. Wang, J. Xiong, and J. Ma., “A Blockchain-Based Secure Key Management Scheme with Trustworthiness in DWSNs”, IEEE Transactions on Industrial Informatics, 2020.

[59] Aslan, H. K., “A Scalable and Distributed Multicast Security Protocol Using a Subgroup-Key Hierarchy”, Computers & Security, Vol 23, pp. 320-329, 2004.

[60] Bethencourt, J., Sahai, A. & Amp Waters, B., “Ciphertext-Policy Attribute-Based Encryption”, IEEE Symposium on Security and Privacy (Sp’07), 2007.

[61] Bonmariage, N. & Leduc, G., “A Survey of Optimal Network Congestion Control for Unicast and Multicast Transmission”, Computer Networks, Vol. 50, 448-468, 2006.

[62] Cao, J., Liao, L. & Wang, G., “Scalable Key Management for Secure Multicast Communication in the Mobile Environment”, Pervasive and Mobile Computing, Vol. 2, pp. 187-203, 2006.

[63] Challah, Y. & Seba, H., “Group Key Management Protocols: A Novel Taxonomy”, International Journal of Information Technology, Vol 2, pp.105-118, 2005.

[64] Chan, K. C. & Chan, S.H., “Key Management Approaches to Offer Data Confidentiality for Secure Multicast”, IEEE Network, Vol. 17, 30-39, 2003.

[65] Bhushan, K. & Gupta, B. B., “Network Flow Analysis for Detection and Mitigation of Fraudulent Resource Consumption (FRC) Attacks”, In Multimedia Cloud Computing. Multimedia Tools and Applications, Vol.78, pp. 4267-4298, 2019.

[66] Goyal, V., Pandey, O., Sahai, A. & Waters, B., “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data”, Proceedings of the 13th Acm Conference on Computer and Communications Security, 89-98, 2006.

[67] Harte L., “Introduction to Data Multicasting, IP Multicast Streaming for Audio and Video Media Distribution”, Cary, NC: Althos Publishing; 2008.

[68] He, H., Zheng, L.-H., Li, P., Deng, L., Huang, L. & Chen, X., “An Efficient Attribute-Based Hierarchical Data Access Control Scheme in Cloud Computing”, Human-Centric Computing and Information Sciences, Vol. 10, pp. 1-19, 2020.

[69] Jiang, J.R., Huang, S.T. & Kuo, Y.C. Cohorts, “Structures for Fault-Tolerant K Entries to a Critical Section”, IEEE Transactions on Computers, Vol. 46, pp. 222-228, 1997.

[70] Jouini, M., Rabai, L.B.A., “A security framework for secure cloud computing environments”, International Journal Cloud Application Computation (IJCAC), Vol. 6 Issue3, pp. 32-44, 2016.

[71] Jun, Z., Yu, Z., Fanyuan, M., Dawu, G. & Yingcai, B., “An Extension of Secure Group Communication Using Key Graph”, Information Sciences, Vol. 176, pp. 3060-3078, 2006.

[72] Lang, S. & Mao, L., “A Torus Quorum Protocol for Distributed Mutual Exclusion”, Proceeding of the 10th International Conference on Parallel and Distributed Computing and Systems, Citeseer, pp.635-638, 1998.

[73] Lewko, A. & Waters, B., “Decentralizing Attribute-Based Encryption”, Annual International Conference on the Theory and Applications of Cryptographic Techniques Springer, pp. 568-588, 2011.

[74] Li, J., Chen, X., Chow, S. S., Huang, Q., Wong, D. S. & Liu, Z., “Multi-Authority Fine-Grained Access Control with Accountability and Its Application in Cloud”, Journal of Network and Computer Applications, Vol. 112, pp. 89-96, 2018.

[75] Li, J., Yao, S., Liu, J. & Wu, Y., “A Hierarchical Multicast Key Distribution Protocol”, Journal of Electronics, Vol. 10, 995-1016, 2021.

[76] Lopriore, L., “Key Management in Tree Shaped Hierarchies”, Information Security Journal: A Global Perspective, Vol. 27, pp. 205-213, 2018.

[77] Mittra, S., “Iolus: A Framework for Scalable Secure Multicasting”, ACM Sigcomm Computer Communication Review, Vol. 27, pp. 277-288, 1997.

[78] Nair, S. K., Dashti, M. T., Crispo, B. & Tanenbaum, A. S., “A Hybrid Pki-Ibc Based Ephemerizer System”, IFIP International Information Security Springer Conference, pp. 241-252, 2007.

[79] Niu, S., Tu, S. & Huang, Y., “An Effective and Secure Access Control System Scheme in the Cloud”, Chinese Journal of Electronics, Vol. 24, pp. 524-528, 2015.

[80] Qiu, Z., Zhang, Z., Tan, S., Wang, J. & Tao, X., “Hierarchical Access Control with Scalable Data Sharing In Cloud Storage”, Journal of Internet Technology, Vol 20, pp 663-676, 2019.

[81] Riad, K. & Ke, L. Rough Droid, “Operative Scheme for Functional Android Malware Detection”, Security and Communication Networks, 2018.

[82] Sahai, A. & Waters, B., “Fuzzy Identity-Based Encryption”, Annual International Springer Conference on the Theory and Applications of Cryptographic Techniques, pp. 457-473, 2005.

[83] Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H. & Tang, Y., “Cloud-Aided Lightweight Certificate less Authentication Protocol with Anonymity for Wireless Body Area Networks”, Journal of Network and Computer Applications, Vol. 106, pp. 117-123, 2018.

[84] Velumadhava Rao, R., Selvamani, K., Kanimozhi, S. & Kannan, A., “Hierarchical group key management for secure data sharing in a cloud-based environment”, Concurrency and Computation: Practice and Experience, Vol. 31, pp. 48-66, 2019.

[85] Waters, B., “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization”, International Springer Workshop on Public Key Cryptography, pp. 53-70, 2011.

[86] Wu, Y., “Developing a Taxonomic Framework of Security Methods for Security Management and Information Resource Management”, Journal of Strategic Security, Vol. 13, pp. 64-77, 2020.

[87] Wu, Y. & Meng, F., “Categorizing security for security management and information resource management”, Journal of Strategic Security, Vol. 11, pp. 72-84, 2018.

[88] Wuu, L.C., Hung, C.-H. & Chang, C.-M., “Quorum-based key management scheme in wireless sensor networks”, Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication. pp. 1-6, 2012.

[89] Toyomura, M., Kamei, S. & Kakugawa, H., “A quorum-based distributed algorithm for group mutual exclusion”, Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, IEEE, pp.742-746, 2003.

[90] Zkik, K., Orhanou, G. & El Hajji, S., “Secure mobile multi-cloud architecture for authentication and data storage”, International Journal of Cloud Applications and Computing, Vol. 7, pp. 62-76, 2017.

Authors

Smita Athanere is a Ph.D. research scholar of Computer Engineering IET DAVV Indore MP India. She teaches or taught numerous master's and bachelor's classes over the last 14 years. She earned master's degree from SGSITS, Indore MP India and a Bachelor's degree from SGSITS, Indore MP India. Presented papers in many journals and conference.

Dr Ramesh Thakur is a reader in International Institute of Professional studies, DAVV, Indore MP India. He teaches or taught numerous Doctoral, master's and bachelor's classes over the last 20 years. Presented papers in many journals and conference.

How to cite this article:

Smita Athanere, Ramesh Thakur, "A Review of Chronological Development in Group and Hierarchical Key management Schemes in Access Control Model: Challenges and Solutions", International Journal of Computer Networks and Applications (IJCNA), 9(1), PP: 84-102, 2022, DOI: 10.22247/ijcna/2022/211628.