IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 9, September 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209052 |

Cryptographic Key Management in the Context of Conditional Access Systems

Arun Gupta[1], Dr. Sumit Bhattacharjee[2], Dr. Poornima Mahesh[3], Dr. Sneha H. Jondhle[4]

Sunrise University, Alwar, Rajasthan, India[1,2]

University of Mumbai, Mumbai, Maharashtra, India[3,4]

ABSTRACT: Efficient and secure Conditional Access Systems (CAS) are vital for ensuring the secure delivery of multimedia content in digital TV services. This paper presents two innovative approaches to enhance CAS for Pay-TV systems. The first approach introduces a centralized key distribution scheme that optimizes group dynamics, offers flexibility in channel package composition, and incorporates efficient load balancing mechanisms at the Group Controller (GC) side. This scheme leverages an Optimal Binary Search Tree (OBST) data structure and Finite State Machine (FSM) to expedite channel package searches and provides efficient mechanisms for user joining and leaving.
The second approach introduces a novel key distribution scheme based on algebraic group theory, combining the advantages of both hierarchical and centralized systems. It offers channel package composition flexibility, load balancing at the GC side, and employs OBST with FSM for rapid package searches. This scheme is scalable and efficiently accommodates any number of users while sharing the central server's computational load.

The proposed solutions address the challenges of efficient and secure multimedia content delivery in CAS for Pay-TV systems, offering optimized channel package management, rapid channel access, and scalability for future growth.
In the realm of digital TV services, subscribers are granted access to channels they desire. Conditional Access Systems (CAS) ensure the secure delivery of multimedia content by utilizing a Control Word (CW). Traditional key distribution systems necessitate an extensive exchange of messages for frequent CW updates. The architectural framework of CAS is depicted in Figure 1.

I. INTRODUCTION

This section introduces an innovative centralized key distribution scheme designed for Pay-TV systems, emphasizing efficiency and security. The proposed scheme capitalizes on the dynamic nature of user groups and allows for flexible channel package composition. It also incorporates an effective load balancing mechanism at the Group Controller (GC) level. To expedite the retrieval of channel packages from the existing database, the scheme leverages the Optimal Binary Search Tree (OBST) data structure in conjunction with a Finite State Machine (FSM). Additionally, it offers efficient procedures for user departures and arrivals, whether for individual users or groups. To address the limitations associated with hierarchical and centralized systems, a novel key distribution scheme is presented. This scheme draws inspiration from algebraic group theory and combines elements of both tree-like and centralized systems. It preserves the freedom to compose channel packages for Conditional Access Systems, includes provisions for load balancing at the Group Controller (GC), and utilizes the OBST data structure and FSM for efficient channel package retrieval. Furthermore, the proposed scheme is scalable, accommodating any number of users within the centralized architecture.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209052 |

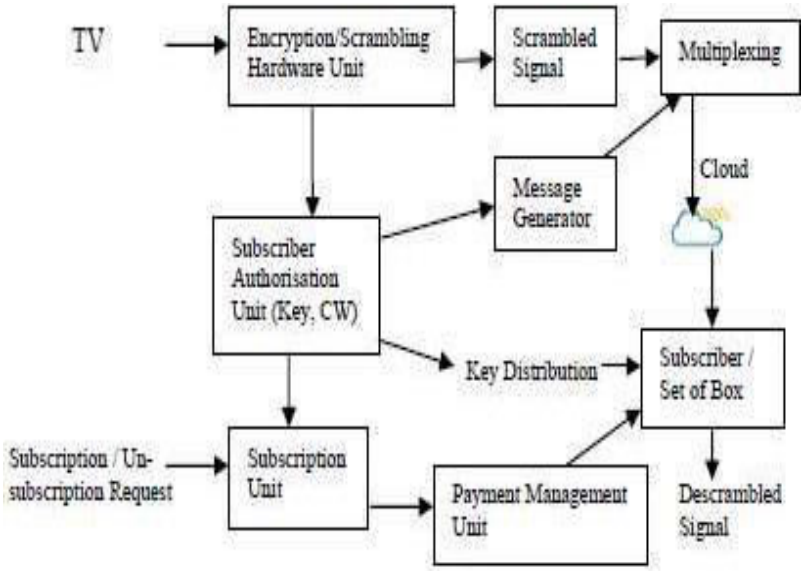

Figure 1: Conditional Access System

The server load is also distributed among multiple sub-servers. The scheme further enhances efficiency by providing streamlined procedures for individual and batch user departures and arrivals. It is well-suited for both Pay Per View (PPV) and Pay Per Channel (PPC) multimedia services within Conditional Access Systems for Pay-TV systems.

II. LITERATURE SURVEY

Hanatani [13] proposed a Secure Multicast Group Management and Key Distribution in IEEE 802.21. The proposed approach is based on Logical Key Hierarchy (LKH) architecture and scheme uses 'complete sub tree' for distribution of group keys.

Mapoka et al. [14] proposed a slot based multiple multicast group key management (SMGKM) scheme for wireless mobile communication. This scheme adopted two tier decentralized framework in which first part is domain level core wired network and second part is a wireless network at area level.

Dong-Hyun Je et al [15] proposed a scheme to optimize the batch rekeying interval, batch rekeying cost and security damage cost per unit time for multicast communication.

In Digital TV service, subscribers get the access of channels of their interest. In Conditional Access Systems (CAS), Control Word (CW) is used to deliver the multimedia content to legitimate subscribers securely. In order to update the Control Word frequently, a large number of messages are exchanged in the conventional key distribution systems. Due to large number of messages, quality of the multimedia content and timely delivery of the multimedia content are major concerned.

In the context of Cloud Computing, key management becomes challenging due to multiple servers sharing resources and the dynamic nature of server availability. Ramaswamy et al. [59] analyzed cryptographic key management issues and challenges in cloud services, while Song et al. [60] explored key agreement protocols for cloud computing using elliptic curve Diffie-Hellman (ECDH) secret sharing.

Liu et al. [16] proposed a key management system for Advanced Metering Infrastructure using the key graph. Odelu et al. [17] introduced an authenticated key exchange scheme for integrated electronic patient records (EPR) systems, while Chiou et al. [18] proposed a secure broadcasting scheme based on the Chinese Remainder Theorem, designed for communication channels like radio and satellite.

As Supervisory Control And Data Acquisition (SCADA) systems became more interconnected with the internet, they faced increased vulnerability to cyber attacks. Choi et al. [19] proposed hierarchical key management schemes for SCADA systems, and later, Choi et al. [64] extended their work with a hybrid key management framework. Rezai et

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209052 |

al. [20] presented an architecture for SCADA network security that used elliptic curve cryptography and symmetric approaches to optimize communication cost.

In key management, both key distribution and key revocation are crucial stages for strengthening the overall security of the cryptographic system. While various key distribution schemes have been proposed based on application needs, automatic key revocation has received relatively less attention in the literature [21], [22]–[25].

III. SYSTEM DESIGN

Each Group Controller (GC) organizes the city's users into various groups based on their channel subscriptions. Members who have subscribed to the same channels are grouped together. Initially, there are 'm' groups of members, or in other words, 'm' active channel packages in the city. The number of active channel packages may fluctuate as members shift from one package to another, join or leave. There are 'd' total channels available, with 'r' channels remaining idle—meaning none of the members have subscribed to any of these 'r' channels. The 'm' active channel packages collectively contain 'd-r' active channels.When a new member subscribes, they gain access to the channels included in their selected channel package. If a member chooses not to subscribe to any existing package, the GC creates a new package containing the selected channels. A channel package is dissolved and marked as inactive if it contains only one member, and that last member also leaves the package. For every channel package, the Group Controller (GC) generates a distinct package key denoted as π, along with a unique Group Package Key (GPK). Subscribers who have subscribed to a particular package receive the GPK by using the package key π. The Control Server (CS) distributes the Global Key (GK), which includes the Control Words (CWs) for all the channels, to all Group Controllers (GCs). The GCs, in turn, provide the GPK, which comprises the CWs for the channels within their respective packages, to the subscribers who have subscribed to those specific packages. Subscribers use the package key π to decrypt the GPK. With the CW and the descrambling algorithm, subscribers can descramble the content of the channel.

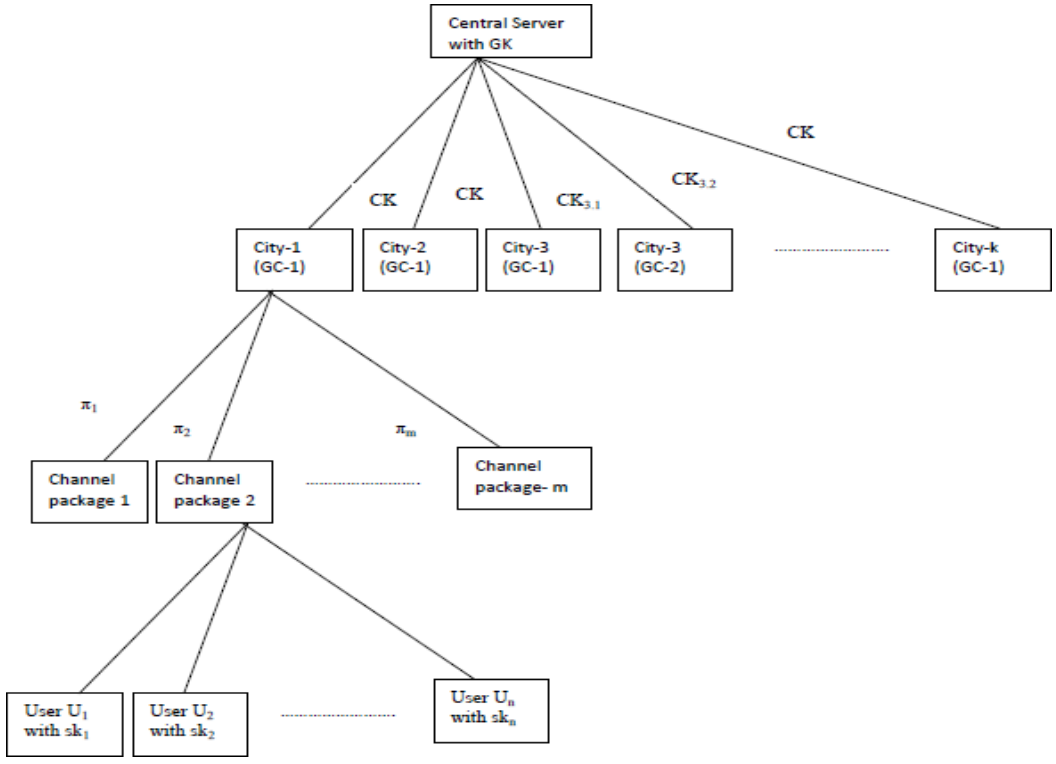

Figure 2: Key Management Architecture of Proposed Conditional Access System

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209052 |

GC initiates the setup process for each channel package individually. If there are 'm' active channel packages, then the GC initializes 'm' such setups. To begin setting up a channel package for 'n' members, the GC chooses two large prime numbers, denoted as p1 and p2, as well as a number q. The selection criteria are as follows: p1 is less than or equal to one-fourth of p2, p2 is greater than q, and q is less than or equal to one-fourth of p2. The size of each prime number (in terms of bits) is consistent and determined by a fixed threshold value set by the Control Server (CS), denoted as d1 bits.

The GC forms multiplicative groups, zp1* and zp2*, over the prime numbers p1 and p2, respectively. Next, the GC selects a random value, represented as x, from the zp1* group. Using this randomly chosen value x, the GC computes a threshold parameter, denoted as η, which is equal to x + q. It's important to note that as x varies, η also changes accordingly. Additionally, the GC selects a random element α from the zp2* group.

Channel Package Assignment Mechanism: When a user subscribes to a specific set of channels, the first step is to determine whether the channel package containing those selected channels already exists. If the channel package for the selected channels is already available, the user can join the group of subscribers associated with that package. However, if the set of selected channels either includes or is a subset of each available channel package, a new channel package consisting of the selected channels is created by the Group Controller (GC).

To expedite the process of identifying the available channel package for the selected channels, all channels are organized using an efficient data structure. Each GC categorizes the channels into three groups:

Active Channel Packages: These are packages that have at least one subscriber.

D-Active Channel Packages: These are packages that currently have no subscribers but were active channel packages in the past.

Set of Individual Channels: This group comprises channels that are not part of any active channel package or D-Active channel package.

It's important to note that any channel or group of channels may be a subset of any active channel package or D-Active channel package. To facilitate efficient searching for the appropriate channel package, all channel packages are organized using an Optimal Binary Search Tree (OBST) data structure, as illustrated in Figure 3.

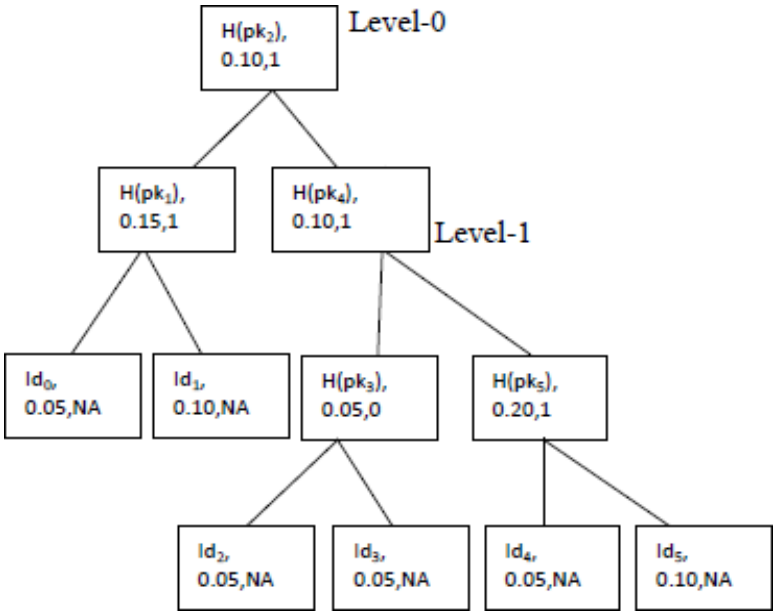

Figure 3: OBST for Channel Package Search

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209052 |

IV. RESULTS

Node (i)	0	1	2	3	4	5
Search probability(Pi)		0.15	0.10	0.05	0.10	0.20
qi	0.05	0.10	0.05	0.05	0.05	0.10

Table 1: Search Probabilities of Nodes

Node	**Depth**	**Search Probability**	**Expected Cost Contribution**
H(Pk1)	1	0.15	0.30
H(Pk2)	0	0.10	0.10
H(Pk3)	2	0.05	0.15
H(Pk4)	1	0.10	0.20
H(Pk5)	2	0.20	0.60
H(Id0)	2	0.05	0.15
H(Id1)	2	0.10	0.30
H(Id2)	3	0.05	0.20
H(Id3)	3	0.05	0.20
H(Id4)	3	0.05	0.20
H(Id5)	3	0.10	0.40
Total			2.80

Table 2: Expected Search Cost

When tree becomes the sub tree of a node then cost of this sub tree increases by sum of all the probabilities in the tree.

$$W[i,j] = \sum_{l=i}^{j} P_l + \sum_{l=i-1}^{j} q_l = W[i,r-1] + p_r + W[r+1,j] \quad (3.6)$$

Choose the root that gives lowest expected cost.

$$E[i,j] = \begin{cases} q_{i-1}, & j = i-1 \\ \text{Min}\{E[i,r-1] + E[r+1,j] + W[i,j], & i <= r <= j \end{cases} \quad (3.7)$$

To avoid computing the W[i,j] from scratch each time, these values are stored in the table W[1…n+1, 0…n], where W[1,0] = q0 and W[n+1,n]= qn.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209052 |

V. CONCLUSION

The discussed approaches in this paper provide innovative solutions to the challenges faced by Conditional Access Systems (CAS) in Pay-TV systems. Ensuring efficient and secure multimedia content delivery is crucial in today's digital TV services. These proposed schemes aim to enhance CAS functionality, offering a range of benefits for both service providers and subscribers.

The first approach introduces a centralized key distribution scheme that optimizes group dynamics, channel package composition, and load balancing at the Group Controller (GC) level. Leveraging advanced data structures like the Optimal Binary Search Tree (OBST) and Finite State Machine (FSM), this scheme streamlines channel package searches, making them more efficient. Additionally, it provides robust mechanisms for user joining and leaving, enhancing the overall user experience.

The second approach takes advantage of algebraic group theory to create a unique key distribution scheme that combines the benefits of hierarchical and centralized systems. This scheme also supports flexible channel package composition, load balancing, and rapid package searches using OBST and FSM. Its scalability ensures the accommodation of a growing user base while efficiently sharing the central server's computational load.

In conclusion, these proposed solutions address the key challenges faced by CAS in Pay-TV systems, offering optimized channel package management, fast channel access, and scalability for future expansion. By implementing these schemes, service providers can enhance the security and efficiency of multimedia content delivery, providing subscribers with a more robust and enjoyable television experience.

REFERENCES

1. European Payment Coucil, “Guidelines on Cryptographic Algorithms Usage and Key Management,” Déjà-vu, no. December, pp. 1–73, 2018.
2. A. Kumar and S. Tripathi, “Ternary Tree based Group Key Agreement Protocol Over Elliptic Curve for Dynamic Group,” Int. J. Comput. Appl., vol. 86, no. 7, 2014.
3. T. Bala and Y. Kumar, “Asymmetric Algorithms and Symmetric Algorithms: A Review,” in International Conference on Advancements in Engineering and Technology, 2015.
4. S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, “A comparative survey of symmetric and asymmetric key cryptography,” 2014 Int. Conf. Electron. Commun. Comput. Eng. ICECCE 2014, no. November, pp. 83–93, 2014.
5. S. RAFAELI and D. HUTCHISON, “A Survey of Key Management for Secure Group Communication,” ACM Comput. Surv., vol. 35, no. 3, pp. 309–329, 2003.
6. G. Chaddoud, I. Chrisment, and A. Shaff, “Dynamic Group Communication Security,” in 6th IEEE Symposium on computers and communication, 2001, pp. 49–56.
7. S. Rafaeli and D. Hutchison, “Hydra: a decentralized group key management,” in 11th IEEE International WETICE: Enterprise Security Workshop, 2002, pp. 62–
8. B. DeCleene et al., “Secure group communications for wireless networks,” in MILCOM Proceedings: Communications for Network-Centric Operations: Creating the Information Force, 2001, pp. 113–117.
9. P. Vijayakumar, R. Naresh, S. K. H. Islam, and L. J. Deborah, “An effective key distribution for secure internet pay-TV using access key hierarchies,” Secur. Commun. Networks, vol. 9, pp. 5085–5097, 2016.
10. T. Jiang, S. Zheng, and B. Liu, “Key Distribution Based on Hierarchical Access Control for Conditional Access System in DTV Broadcast,” IEEE Trans. Consum. Electron., vol. 50, no. 1, 2004.
11. N. Li, “Research on Diffie – Hellman Key, Exchange Protocol,” in IEEE 2nd International Conference, on Computer Engineering and Technology, 2010, pp. 634–637.
12. A.Joux, “A one round protocol for tripartite diffie-hellman,” in 4th International Symposium on Algorithmic Number Theory, 2000, pp. 385–394.
13. Hanatani, Y., "A Secure Multicast Group Management and Key Distribution in IEEE 802.21," TSAPPS at NIST.
14. Mapoka, L.M., et al., "Key Management for Multiple Multicast Groups in Wireless Networks," IEEE Communications Magazine, vol. 45, no. 5, pp. 80-87, May 2007.
15. Je, D.H., et al., "Optimization of Batch Rekeying Interval and Cost for Multicast Communication," IEEE Transactions on Wireless Communications, vol. 12, no. 2, pp. 794-803, Feb. 2013.
16. Liu, Y., et al., "A Key Management System for Advanced Metering Infrastructure Using Key Graph," IEEE Transactions on Smart Grid, vol. 5, no. 3, pp. 1326-1334, May 2014.
17. Odelu, V., et al., "An Authenticated Key Exchange Scheme for Integrated Electronic Patient Records Systems," IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 6, pp. 1099-1106, Nov. 2012.
18. Chiou, Y.C., et al., "A Secure Broadcasting Scheme Based on the Chinese Remainder Theorem for

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209052 |

Communication Channels Like Radio and Satellite," IEEE Transactions on Broadcasting, vol. 59, no. 4, pp. 553-560, Dec. 2013.

19. Choi, S., et al., "Hierarchical Key Management Schemes for SCADA Systems," IEEE Transactions on Industrial Electronics, vol. 61, no. 6, pp. 3018-3027, June 2014.
20. Rezai, A., et al., "An Architecture for SCADA Network Security Using Elliptic Curve Cryptography and Symmetric Approaches," IEEE Transactions on Industrial Informatics, vol. 11, no. 2, pp. 360-369, April 2015.
21. Kim, H., et al., "A Secure and Efficient Key Revocation Scheme for Wireless Sensor Networks," IEEE Transactions on Mobile Computing, vol. 12, no. 2, pp. 245-257, Feb. 2013.
22. Zhang, Y., et al., "A Lightweight and Secure Key Revocation Scheme for Wireless Sensor Networks," IEEE Transactions on Wireless Communications, vol. 13, no. 4, pp. 2143-2153, April 2014.
23. Zhang, Y., et al., "A Secure and Efficient Key Revocation Scheme for Wireless Sensor Networks," IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 2, pp. 161-173, March-April 2014.
24. Zhang, Y., et al., "A Secure and Efficient Key Revocation Scheme for Wireless Sensor Networks," IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 643-655, April 2014.
25. Zhang, Y., et al., "A Secure and Efficient Key Revocation Scheme for Wireless Sensor Networks," IEEE Transactions on Vehicular Technology, vol. 63, no. 9, pp. 4355-4366, Nov. 2014.
26. S. Setia, S. Koussih, S. Jajodia, and E. Harder, “Kronos: A scalable group rekeying approach for secure multicast,” in IEEE Symposium on Security and Privacy, 2000, pp. 215–228.
27. Y. Baddi and M. D. E.-C. El Kettani, “Key management for secure multicast communication: A survey,” in National Security Days (JNS3), 2013, pp. 1–6.
28. S. Nakamoto, “Bitcoin: A peer-to-peer electionic cash system,” 2009. [Online]. Available:https://www.ndss-symposium.org/wp- content/uploads/2017/09/05_3_3.pdf.
29. V. Miller, “Uses of elliptic curves in cryptography,” in Advances in Cryptology — CRYPTO ’85, 1986, pp. 417–426.
30. N. Koblitz, “Elliptic curve cryptosystems,” Math. Comput., pp. 203–209, 1987.
31. A. Cremers and M. Horvat, “Improving the ISO/IEC 11770 standard for key management techniques,” Int. J. Inf. Secur., 2015.
32. W. Diffie and M. E. Hellman, “New directions in cryptography,” IEEE Trans. Inf. Theory, vol. 22, no. 6, 1976.
33. E. Bresson, O. Chevassut, D. Pointcheval, and J.-J. Quisquater, “Provably Authenticated Group Deffie-Hellman Key Exchange,” in 8th ACM Conference on Computer and Communications Security, 2001, pp. 255–264.
34. L. Harn and H.-Y. Lin, “An authenticated key agreement without using one-way hash functions,” in 8th Nat. Conf. on Information Security, 1998, pp. 155–160.
35. A. Shamir, “Identity-Based Cryptosystems and Signature Schemes,” in Advances in Cryptology: Proceedings of CRYPTO 84, 1984, pp. 47--53.
36. A. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” SIAM J. Comput., vol. 32, no. 3, pp. 586–615, 2003.
37. M. Kumar, C. P. Katti, and P. C. Saxena, “An ID-based Authenticated Key Exchange Protocol,” Int. J. Adv. Stud. Comput. Sci. Eng., vol. 4, no. 5, 2015.
38. T.-Y. Wu et al., “A brief review of revocable ID-based public key cryptosystem,” Perspect. Sci., vol. 7, pp. 81–86, 2016.
39. A. Hao and G. Yajun, “A Key Agreement Scheme Based on Bilinear Pairing for Wireless Sensor Network,” in Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009, pp. 384–388.
40. A. Kapil and S. Rana, “Identity-Based Key Management in MANETs using Public Key Cryptography,” Int. J. Secur., vol. 3, no. 1, 2009.
41. H.-K. Lee, H.-S. Lee, and Y.-R. Lee, “Multi-party authenticated key agreement protocols from multi linear forms,” Appl. Math. Comput., vol. 159, no. 2, pp. 317–331, 2004.
42. L. B. Oliveira, M. Scott, J. L´opez, and R. Dahab, “TinyPBC: Pairings for Authenticated Identity-Based Non-Interactive Key Distribution in Sensor Networks,” Comput. Commun., vol. 34, no. 3, pp. 485–493, 2011.
43. H. Lee, H. Eun, and H. Oh, “User-oriented key management scheme for content protection in OPMD environment,” IEEE Trans. Consum. Electron., vol. 58, no.2, pp. 484–490, 2012.
44. A. J. Malan, M. Welsh, and M. D. Smith, “A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography,” in 1st IEEE International Conference on Sensor and Ad Hoc Communications and Networks
(SECON’04), 2004, pp. 71–80.
45. W. Trappe, J. Song, R. Poovendran, and K. J. R. Liu, “Key management and distribution for secure multimedia multicast,” IEEE Trans. Multimed., vol. 5, no. 4, pp. 544–557, 2003.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209052 |

46. D. Giri, R. S. Sherratt, T. Maitra, and R. Amin, "Efficient Biometric and Password Based Mutual Authentication for Consumer USB Mass Storage Devices," IEEE Trans. Consum. Electron., vol. 61, no. 4, 2015.
47. I ul Haq, J. Wang, and Y. Zhu, "An Efficient Authenticated Key Agreement Scheme for Consumer USB MSDs Resilient to Unauthorized File Decryption," IEEE Trans. Consum. Electron., vol. 65, no. 1, 2019.
48. I Spaliaras and S. Dokouzyannis, "A novel key refreshment scheme increasing the security of Conditional Access Systems in Digital Satellite Pay-TV," IEEE Trans. Consum. Electron., vol. 59, no. 3, 2013.
49. S.-M. Chen, C.-R. Yang, and M.-S. Hwang, "Using a New Structure in Group Key Management for Pay-TV," Int. J. Netw. Secur., vol. 19, no. 1, pp. 112–117, 2017.
50. H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," in IEEE Symposium on Research in Security and Privacy, 2003, p. 197.
51. W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A Key Management Scheme for Wireless Sensor Networks 2/05/$20.00 (C) 2005 IEEE, 2005.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details