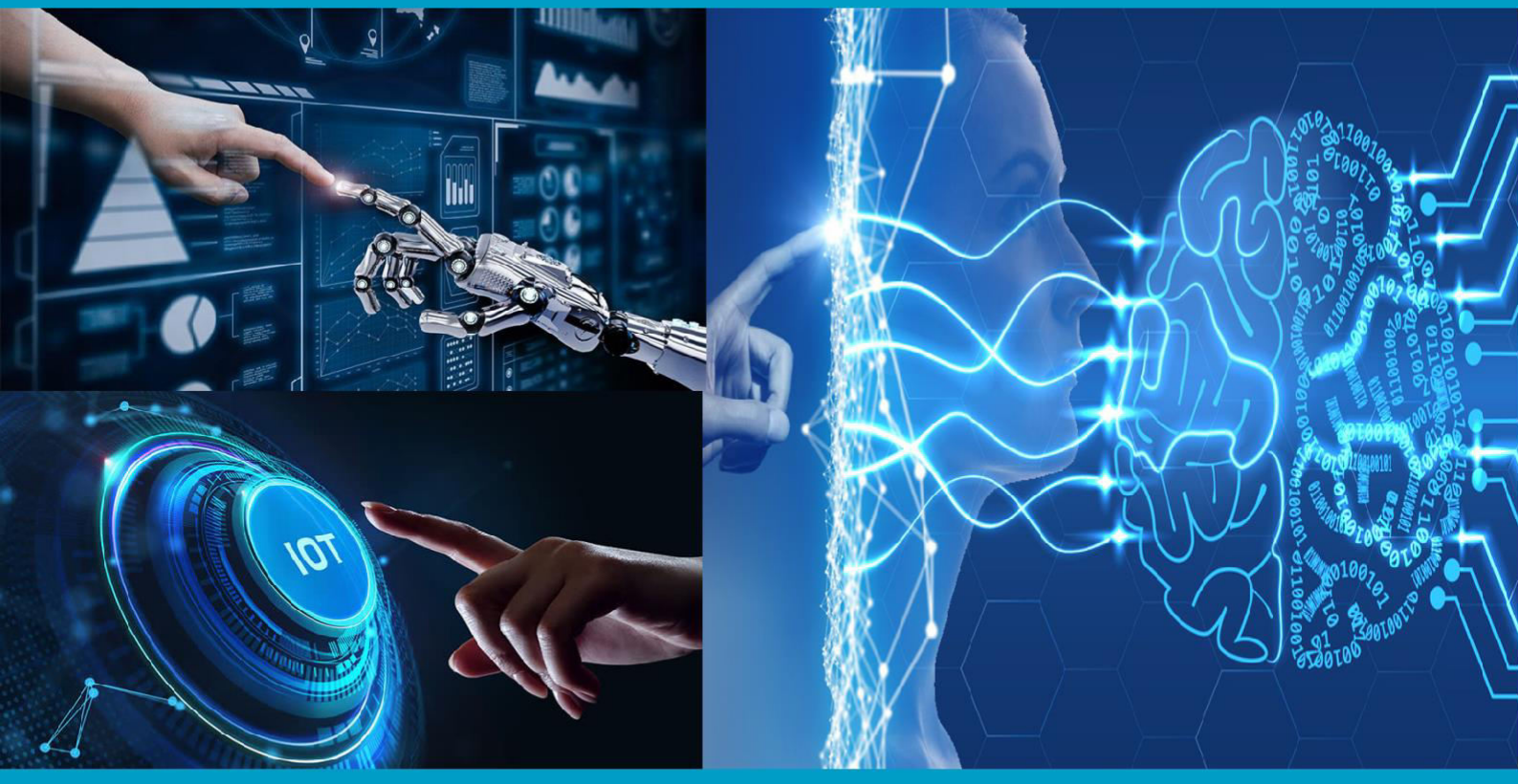
IJMRSETM

e-ISSN: 2395 - 7639



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 10, Issue 9, September 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.580

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 10, Issue 9, September 2023 |

Creating and Implementing Effective Cryptographic Key Management Strategies to Enhance Cybersecurity

Arun Gupta[1], Dr. Sumit Bhattacharjee[2]

Sunrise University, Alwar, Rajasthan, India

ABSTRACT: The adoption of encryption within organizations primarily stems from the necessity to safeguard high-value data, confidential information, and sensitive corporate assets. To attain the desired levels of confidentiality and integrity, businesses often employ a multitude of encryption software, hardware solutions, and cryptographic tools, which results in the management of a substantial volume of encryption keys. Governments and affiliated entities establish security standards and regulatory frameworks to protect businesses, competitors, and national interests. These security and regulatory frameworks often necessitate the use of numerous encryption keys within infrastructure. Encryption keys are classified as sensitive information and must be securely stored.

Key management in a cryptographic system encompasses activities such as key generation, distribution, exchange, storage, utilization, revocation, and more. This multifaceted process involves user protocols, policies, guidelines, policy standards, protocol design, key servers, cryptographic algorithms, coordination among system components, group and subgroup management, peer-to-peer communication, system architecture, user training, and other elements. It is crucial to recognize that the cornerstone of any secure cryptosystem is the cryptographic key itself. The security of the cryptographic system heavily relies on the meticulous handling of cryptographic keys. The true challenge in key management lies in effectively overseeing the entire lifecycle of cryptographic keys, extending beyond mere key storage and encryption.

I. INTRODUCTION

In the internet era, effective key management plays a pivotal role in ensuring secure communication, especially in the context of both two-party and multi-party interactions [11]–[15]. Key management is a critical requirement for safeguarding various applications, such as online banking transactions, video conferencing, audio and video transmission, distance learning, distributed databases, data replication, multi-party games, distributed simulation, network services, and many more.

As defined by Menezes et al. [16], key management encompasses a set of techniques and procedures that facilitate the establishment and maintenance of keying relationships among authorized parties. This involves several key aspects:

1. Initialization of System Users: The process begins with the initialization of system users, ensuring that they are properly authorized and authenticated.
2. Generation, Distribution, and Activation of Keying Material: Key management involves the generation, secure distribution, and activation of keying material, which is essential for encryption and decryption processes.
3. Supervision of Keying Material: This aspect encompasses the ongoing management of keying material, including key generation, secure distribution, key exchange, and revocation when necessary, to maintain the security of communications.
4. Storage, Destruction, and Archival of Keying Material: To ensure long-term security and compliance, keying material must be securely stored, properly destroyed when no longer needed, and archived as necessary.
5. Effectively managing cryptographic keys is fundamental to maintaining the confidentiality and integrity of sensitive information in a connected world.

II. LITERATURE SURVEY

In this section, we conduct a comprehensive review of the literature related to key management. This survey encompasses various aspects, including key distribution, key revocation, key exchange protocols, group key management schemes, key management for Wireless Sensor Networks (WSN), key distribution in conditional access systems, and key management for Blockchain Technology, among others.

ISO/IEC 11770 is a standard that defines a range of key agreement policies, guidelines, key establishment, and key transport protocols. A systematic analysis of the ISO/IEC 11770 standard was carried out by Cas Cremers and Marko Horvat [31], focusing on key management techniques, including key transport protocols, key agreement, and key establishment protocols. The authors also examined the security properties of various protocols and their variations.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 10, Issue 9, September 2023 |

One of the primary challenges in symmetric key cryptography is establishing a secure key exchange between two parties. Whitfield Diffie and Martin Hellman [32] introduced the concept of key exchange over an insecure channel, although it suffered from the vulnerability of man-in-the-middle attacks. Subsequent work by authors such as [12], [13], [33] extended the Diffie-Hellman two-party protocol to support multi-party key exchanges. Harn et al. [34] proposed three key agreement protocols based on a single cryptographic assumption, including RSA factoring, ECC, and discrete logarithm-based methods.

Adi Shamir [35] introduced the concept of Identity-Based Public Key Cryptography,where a member's public key is based on their identity. This approach allows senders to encrypt information using the recipient's identity, simplifying key management and reducing reliance on trusted third parties. Practical implementation of Identity-Based Cryptography using Weil Pairing was presented by Boneh et al. [36] in 2003, and subsequent research has explored public key cryptography schemes based on identity-based encryption [37]–[41].

Trappe et al. [45] proposed embedding cryptographic keys into multimedia content, eliminating the need for a separate channel for key transfer. Giri et al. [46] introduced a Biometric and Password-based session key agreement protocol, although Haq et al. [47] identified vulnerabilities in this approach and proposed an improved key agreement protocol for Universal Serial Bus Mass Storage Devices (USB-MSD). These studies highlight the wide range of applications and challenges associated with cryptographic key management across various domains, including communication systems, secure storage, wireless sensor networks, cloud computing, healthcare, and industrial control systems.

Revocation of cryptographic keys depends on several factors, including key length, the method of key transmission, potential attack vectors, and the available computational power required to compromise a key. When the key length is sufficiently long and the cryptosystem is secure against key leakage, existing keys can remain effective for an extended period. However, if a key is compromised, whether through cryptographic attacks or other means, it must be revoked immediately. In key management, both key distribution and key revocation are crucial stages for strengthening the overall security of the cryptographic system.

III. PROBLEM STATEMENT

The study of cryptographic key management in the context of cyber security is essential due to the numerous challenges faced by applications in this domain. Many cyber security applications, such as multimedia transmission, defense systems, and distributed computing, require robust authentication of participants, reduced re-keying costs, efficient storage of keying material, minimized encryption/decryption overhead, and secure multicast communication over networks. To address these challenges, there is a pressing need to design and develop effective cryptographic key management schemes.

The primary objective of this paper is to explore cryptographic key management within the realm of cyber security. The specific problem statement is defined as "Designing and developing key management schemes for cyber security applications." This overarching problem can be further broken down into the following sub-problems:

Sub-Problem 1:
Designing key management life cycles for both symmetric and asymmetric cryptographic systems.

Sub-Problem 2:
Designing and developing cryptographic key management schemes capable of creating group keys for cyber security applications.

Sub-Problem 3:
Designing a key management scheme tailored for Conditional Access Systems.

Sub-Problem 4:
Designing and analyzing key management schemes for Blockchain Technology and Internet of Things (IoT) devices.

Sub-Problem 5:
Designing and analyzing a key revocation model for key management systems.

Sub-Problem 6:
Designing and analyzing key exchange protocols.

The need for this study is driven by the increasing importance of safeguarding high-profile data, confidential information, and sensitive business assets. Enterprises often employ a wide array of encryption tools, software, and hardware to maintain confidentiality and integrity, resulting in the management of numerous encryption keys. Additionally, governments and regulatory bodies establish security standards and compliance requirements to protect

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 10, Issue 9, September 2023 |

enterprises, competitors, and national interests, all of which necessitate the use of a substantial number of encryption keys. Given the sensitivity of encryption keys, secure storage and protection are paramount.

Key management in a cryptographic system encompasses a range of activities, including key generation, distribution, exchange, storage, utilization, and revocation. It also involves user protocols, policies, guidelines, standards, protocol design, cryptographic algorithms, coordination among system components, group and subgroup management, peer-to-peer communication, system architecture, and user training. Cryptographic keys serve as the foundation of any cryptographic system, and the level of security in such a system heavily relies on effective key management. The true challenge in key management lies not only in key storage and encryption but also in the efficient management of the entire key lifecycle.

IV. RESEARCH METHODOLOGY

In this study, our research will be structured as follows:

1. Estimation of Key Revocation Time: We will begin by addressing the estimation of the appropriate time for revoking cryptographic keys within cryptographic systems. Our study will propose a model for estimating the remaining lifespan of existing keys and recommend timely key revocation. This step is crucial for maintaining the security of cryptographic systems.
2. Enhanced Key Exchange Mechanism: Next, we will introduce an improved key exchange mechanism with a focus on entity authentication. The proposed protocol will eliminate vulnerabilities like impersonation attacks that may exist in existing protocols, such as the one employed in Nanli's protocol.
3. Group Key Management Schemes: Our study will present two novel Group Key Management Schemes designed to facilitate secure group communication. These schemes will efficiently distribute keys with minimal communication overhead while enhancing cryptographic security.
4. Key Management for Conditional Access Systems: We will explore two distinct Key Management Schemes specifically tailored for conditional access systems. These schemes will build upon the foundation of Group Key Management, allowing the Group Controller to distribute control words to authorized users with the lowest possible communication cost and heightened security compared to existing approaches.
5. Key Management Challenges in Blockchain Technology: This section will delve into the unique key management challenges associated with Blockchain Technology. We will propose a Group Key Management scheme specifically designed for Blockchain applications, aiming to address the complexities and security requirements of this innovative field.

Overall, our study will contribute to advancing cryptographic key management practices, addressing various application-specific challenges, and enhancing the security of cryptographic systems in the context of cyber security.

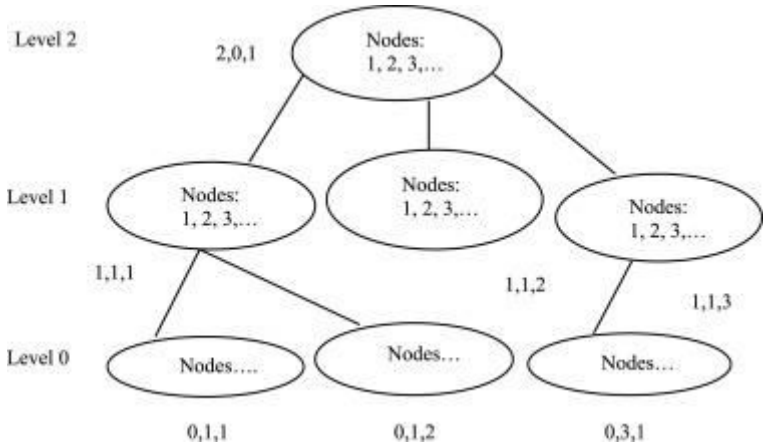


Figure 1: GKM Framework

Each group of GKM framework is represented by a code (i, j, k) where i denotes the level, j denotes the position of parent group in upper layer and k denotes the position of
the group in current layer under the parent group. Let □□□,□,□ represents the Group Key (GK) of the group having the code (i, j, k) and this GK is used to encrypt or decrypt the common messages for the group members who belong to the group having code (i, j, k).

At level 0, Group Keys are assigned to each group. In Fig. 4 Group Keys GK0,1,1, GK0,1,2 and GK0,3,1are assigned to groups who have codes (0,1,1), (0,1,2) and (0,3,1) respectively. Group Keys of groups of higher layers (other than level 0) are computed using the group keys of child groups using the one-way function. One-way function f(.) generates

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 10, Issue 9, September 2023 |

the output of length d therefore, length of □□□,□,□ is also d. Let □1, □2, … □□ arethe children of the group having the code (i,j,k) then □□□,□,□ is computed in the following way-

□□□,□,□ = □□□□−□,□,□□, □□□−□,□,□□ , … … □□□−□,□,□□ (□)

Parent groups have higher privileges and they can view the confidential data of the children groups. No group can access confidential data of parent groups and groups which are at the same layer. To manage the GKM network, root groups assign the GKs to the groups which are at level 0 with the consensus of members of the root group. In case of any membership change for any group, root group updates the concerned group keys with consensus of members of the root group.

In the proposed framework transactions are open to all members of the concerned group as well as for members of the parent group but for non-members, transactions are confidential. Proposed framework contains all benefits of Blockchain Technology with restriction on openness for non-members [30].

V. PROPOSED RESULTS

The proposed Group Key Management (GKM) framework for Blockchain Technology is a significant contribution, addressing the challenges related to preserving transaction confidentiality and efficient payload encryption during the consensus phase. Here is a summary of the key points in this section:

1. Challenges in Consensus Phase: The consensus phase of Blockchain Technology faces challenges related to ensuring the confidentiality of sensitive transactions and efficiently encrypting payload data. These challenges are crucial for maintaining the integrity and security of Blockchain networks.
2. Secure and Efficient GKM Framework: To address these challenges, a secure and efficient Group Key Management framework is proposed. This framework is designed to facilitate the management of cryptographic keys within the Blockchain network, ensuring the confidentiality and security of transactions and payload data.
3. Multi-Layered Architecture: The proposed GKM framework operates within a multi-layered architecture. In this architecture, nodes in the upper layers possess greater privileges and rights compared to nodes in the lower layers. This hierarchical approach allows for more fine-grained control and access management within the Blockchain network.
4. Notations: The section provides a table (Table 7.1) that describes the notations used in the proposed framework, aiding in the understanding and implementation of the framework's components and processes.
5. Enhanced Security: By implementing this GKM framework, Blockchain networks can enhance their security posture during the consensus phase. The management of cryptographic keys is critical for ensuring the confidentiality and integrity of transactions and data within the network.

Overall, the proposed GKM framework addresses key security and encryption challenges in Blockchain Technology, contributing to the continued evolution and secure deployment of Blockchain networks.

VI. CONCLUSION

The preservation of information confidentiality within any cryptographic system hinges on the security of cryptographic keys. Efficient key management is undeniably one of the most challenging tasks in the field of cryptography. In this paper, we have undertaken a comprehensive analysis of various cryptographic key management schemes and addressed key management challenges.

For both symmetric and asymmetric cryptographic systems, we have proposed key management life cycles, providing a structured approach to managing cryptographic keys throughout their lifespan. One of the critical aspects of key management is key revocation. To address this, we introduced a key revocation model designed to estimate the remaining life of a key and enable automatic key revocation when necessary. Our analysis indicates that the proposed key revocation model outperforms existing models, offering more efficient key revocation processes.

In the context of group communication, the secure and efficient distribution of a common key to each group member is paramount. We conducted a thorough examination of various group key management schemes and presented two novel schemes. The first scheme is based on Elliptic Curve Cryptography (ECC) and offers advantages such as low storage requirements, shared computational load among network members, reduced communication costs, and enhanced cryptographic security when compared to existing systems. Our analysis demonstrated that the proposed ECC-based scheme outperforms existing alternatives in terms of computational overhead, storage cost, communication cost, and rekeying cost while also achieving forward and backward secrecy.

The second proposed scheme is founded on algebraic group theory and further reduces the server's computational load while maintaining forward and backward secrecy. This scheme offers dynamic group key computation capabilities, making it highly adaptable to varying network member compositions.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 10, Issue 9, September 2023 |

In the realm of Conditional Access Systems (CAS), we addressed the challenge of frequently updating Control Words (CWs) with large message exchanges in conventional key distribution systems. We presented two key distribution schemes tailored for CAS. The first scheme boasts dynamic channel package creation, efficient load balancing at the controller, accelerated channel package searches via Optimal Binary Search Trees (OBST), and efficient mechanisms for user joining and leaving, both individually and in batches. The scheme is scalable and significantly reduces computational costs.

The second key distribution scheme for CAS leverages Elliptic Curve Cryptography (ECC) and employs secret polynomial shares to compute fresh channel package keys for CW decryption. This scheme achieves backward and forward secrecy, boasts low communication costs, and enhances cryptographic security.

In conclusion, this paper contributes to the advancement of cryptographic key management practices, offering solutions to key management challenges and enhancing the security and efficiency of cryptographic systems across a range of cyber security applications.

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– 67.
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. M. Steiner, G. Tsudik, and M. Waidner, “Diffie-Hellman Key Distribution Extended to Group Communication,” in CCS ’96 Proceedings of the 3rd ACM conference on Computer and communications security, 1996, pp. 31–37.
14. A. Mahalanobis, “Deffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups,” Florida Atlantic University, Boca Raton, Florida, 2005. [Ph.D. Thesis: Online]. Available: https://eprint.iacr.org/2005/223.pdf.
15. S. A. Mortazavi, A. N. Pour, and T. Kato, “An efficient distributed group key management using hierarchical approach with Diffie-Hellman and Symmetric Algorithm: DHSA,” in International Symposium on Computer Networks and Distributed Systems (CNDS), 2011, pp. 49–54.
16. A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. CRC Press, 1996.
17. A. Naureen, A. Akram, R. Riaz, K.-H. Kim, and H. F. Ahmed, “Performance and Security Assessment of a PKC Based Key Management Scheme for Hierarchical Sensor Networks,” in IEEE Vehicular Technology Conference, 2008, pp. 163– 167.
18. M. M. Haque, A.-S. K. Pathan, C. S. Hong, and E.-N. Huh, “An Asymmetric KeyBased Security Architecture for Wireless Sensor Networks,” KSII Trans. INTERNET Inf. Syst., vol. 2, no. 5, 2008.
19. J. Ma, S. Zhang, Y. Zhong, and Y. Wu, “PEAN: A Public Key Authentication Scheme in Wireless Sensor and Actor Network,” in Sixth IEEE International Conference on Computer and Information Technology, 2006, p. 230.
20. M. Misbahuddin, P. Premchand, and A. Govardhan, “A User Friendly Password Authenticated Key Agreement for Multi Server Environment,” in International Conference on Advances in Computing, Communication and Control, 2009, pp. 113–119.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 10, Issue 9, September 2023 |

21. T.-Y. Wu, C.-M. Chen, K.-H. Wang, C. Meng, and E. K. Wang, "A provably secure certificateless public key encryption with keyword search," *J. Chinese Inst. Eng.*, vol. 42, no. 1, pp. 20–28, 2019.
22. A. Ballardie, "Core Based Trees (CBT version 2) Multicast Routing protocol specification." p. RFC 2189, 1997.
23. R. Aparna and B. B. Amberker, "Dynamic Authenticated Secure Group Communication," *WORLD Acad. Sci. Eng. Technol.*, vol. 34, pp. 359–362, 2007.
24. Y. Challal, A. Bouabdallah, and H. Seba, "A Taxonomy of Group Key Management Protocols: Issues and Solutions," *World Acad. Sci. Eng. Technol.*, vol. 6, 2005.
25. A. Ballardie, "Scalable Multicast Key Distribution." p. RFC1949, 1996.
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.
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.

Impact Factor: 7.580

INTERNATIONAL JOURNAL
OF MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

+91 99405 72462 +91 63819 07438 ijmrsetm@gmail.com