International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

A STUDY OF SUITABLE CRYPTOGRAPHIC KEY FOR CYBER SECURITY

SASIKALA RASAMSETTY, DR. RAJEEV YADAV

DESIGNATION- RESEARCH SCHOLAR MONAD UNIVERSITY HAPUR U.P
DESIGNATION- (PROFESSOR) MONAD UNIVERSITY HAPUR U.P

ABSTRACT

One of the fundamental issues in the Internet of Things is effective cryptography based key management, which arises from the anytime/anywhere nature of computing in IoT systems. Initialization, generation, registration, backup, update, recovery, and revocation are all steps in the key management life cycle. Our original contribution is a survey of recent work on key management for various settings, including Internet of Things, wireless sensor networks, and mobile ad hoc networks. Moreover, the reasons and repercussions of the security breach for Internet of Things are highlighted, and a variety of concerns unique to the IoT ecosystem are examined. We also propose future directions to combat attacks on confidentiality, integrity, authentication, and availability of security services in the Internet of Things environment, and we identify the two key management schemes, namely identity and threshold schemes for Internet of Things, to solve the problem of Internet of Things key management.

KEYWORDS: Suitable Cryptographic Key, Cyber Security, IoT systems, Internet of Things, mobile ad hoc networks.

INTRODUCTION

Changes in the use of encryption for any firm are mostly attributable to the need to protect high-profile data, secret data, and sensitive business information. An organization may employ hundreds of instances of encryption software, hardware, and encryption tools, requiring an equally huge number of encryption keys. Each government or affiliated entity establishes its own security standards and regulatory compliances to safeguard businesses, rivals, and nations. There are a lot of encryption keys floating around in security and regulatory infrastructures. Encryption keys are sensitive information and should be kept in a safe and secure location.

Generation, distribution, exchange, storage, usage, revocation, etc. of cryptographic keys are all part of key management in a cryptographic system. User protocols, policies, guidelines,

policy standards, protocol design, key server, cryptographic algorithms, coordination among system components, group and subgroup management, peer-to-peer communication, system framework, user training, etc. are all part of key management.

The keys used in a cryptographic system are the system's most crucial component. The cryptographic system's security relies heavily on the care with which cryptographic keys are handled. The true difficulty of key management is in the efficient management of the entire key life cycle, not in the storage and encryption of keys.

Two main types of cryptography systems exist. First, there are cryptographic systems that use symmetric keys, and then there are those that use asymmetric keys. Symmetric key cryptography is a form of public-key encryption in which both sender and receiver share the same secret key.

There are two types of keys used in asymmetric key cryptography: the Public Key and the Private Key. One key is used for encryption while the other is utilized for decryption; these two keys are mathematically related[1]-[4]. Each member of a group using the same key is known as a Symmetric Group Key. Group members share information by encrypting it with a common key and sending it to one another[5].

Group Key (GK) encryption and decryption is widely used in modern cyber security applications. In these setups, the shared data is broadcast to the other group members or sub-groups through multicast via the Group Controller (GC). One-to-many transmission is used in various contexts, including multimedia, distance learning, video conferencing, data replication, defense systems, distributed networks, cloud computing, multiplayer gaming, and so on[6]-[8]. By encrypting frequently used data only once, we can reduce network traffic, guarantee that data will arrive on time, and enhance service quality. Conditional Access Systems (CAS) are an example of a type of Multimedia transmission in which group keys are utilized to encrypt and decrypt the sent signals[9], [10].

Changes in the use of encryption for any firm are mostly attributable to the need to protect high-profile data, secret data, and sensitive business information. An organization may employ hundreds of instances of encryption software, hardware, and encryption tools, requiring an equally huge number of encryption keys. Each government or affiliated entity establishes its own security standards and regulatory compliances to safeguard businesses, rivals, and nations. There are a lot of encryption keys floating around in security and

regulatory infrastructures. Encryption keys are sensitive information and should be kept in a safe and secure location.

Generation, distribution, exchange, storage, usage, revocation, etc. of cryptographic keys are all part of key management in a cryptographic system. User protocols, policies, guidelines, policy standards, protocol design, key server, cryptographic algorithms, coordination among system components, group and subgroup management, peer-to-peer communication, system framework, user training, etc. are all part of key management.

The keys used in a cryptographic system are the system's most crucial component. The cryptographic system's security relies heavily on the care with which cryptographic keys are handled. The true difficulty of key management is in the efficient management of the entire key life cycle, not in the storage and encryption of keys.

KEY MANAGEMENT CHALLENGES

One of the trickiest parts of working in cryptography is taking care of the keys. The key is not managed in any special or consistent manner. In order to effectively manage keys, many different factors must be considered. The following are some of the obstacles:

(i) When selecting keys, care must be taken to adhere to all applicable security policies and laws.

(ii) It is important that keys can be efficiently computed by authorized users.

(iii) Key distribution requires a reliable and safe channel.

(iv) Timely and necessary key revocation is required

(v) Minimal storage requirements are ideal.

(vi) Security for shorter key lengths should be improved.

(vii) The price of re-keying must be kept to a minimum.

(viii) Effective key recovery system

(ix) If a key is compromised or lost, the consequences should be minimal

(X) Relying too heavily on a third party is not recommended.

(x) It is important to safely keep keys and to frequently replace stored keys. Common information should be disseminated in multicast or broadcast mode to obtain the greater data transmission rate with good quality of data stream.

KEY STATES

A cryptographic key can be in a variety of states, from being generated to being discarded. Protecting the cryptographic system relies on careful administration of all key states. Here are the fundamental transitions in any cryptographic system:-

- **Generation:** This is the initial phase, in this phase key is generated.
- **Activation:** In this phase, produced keys are made operational according to the established parameters.
- **Key exchange**: It's when one person gives up part or all of their key to another user. The keying material is exchanged between both parties by mail.
- **Key Distribution**: This can be a one-to-one or many-to-many key distribution.
- The receiver does not provide the sender with any keying information.
- **Key storage**: In this state, key is stored for the future use.
- **Key usage**: This is the current encryption/decryption state in which the key is being used..
- **Deactivation:** When the use of a certain key is no longer required, it is disabled. The key can no longer be used for encryption or decryption once it has been deactivated.
- **Suspension:** Under this state, key is temporarily deactivated.
- **Expiration:** There is a time limit on when the key will no longer work. When a key reaches this status, it is said to have "expired."
- **Key Deletion:** If there is no imminent need for the current key, it is discarded..
- **Key Archival:** When a key isn't being used right now, but could be in the near future, it's put away for safekeeping..
- **Revocation:** This is the replacement of the existing key with new key.

GROUP KEY MANAGEMENT

A group key is a shared cryptographic key used for the encryption and decryption of data by several users. After producing the group key, the controller can safely distribute it to all members of the group, according to some protocols in which individual members contribute to the construction of the group key. Sometimes, the group key for further group communication is generated with partial input from each member. Most forms of modern communication, such as Pay-TV, VoD, network games, and distant learning, are multicast in nature, necessitating a robust Group Key Management System (GKMS) to facilitate secure and reliable group conversations. Multicasting is a method of sending the same message to many different receivers at once.

Keeping the group's absolute secrecy while distributing its key to its intended users is a challenging problem. Complete group secrecy is ensured by working to keep information both within and outside of the group out of the public eye. Forward secrecy is achieved by rekeying such that a departing member is unable to decipher messages in the future. When a new member is added to the group, it is also necessary to change the keys. This protects the group's anonymity in retrospect. In addition to the difficulties already mentioned, multicast communication presents its own unique set of difficulties, such as increased communication overhead, limited scalability, poor service quality, high storage and key initialization costs, excessive computing demands, etc. Keeping the group's complete secrecy is a critical challenge for any Key Server in dynamic multicast communication, when members join and leave the group regularly.

KEY MANAGEMENT APPLICATIONS

Key management is a fundamental requirement for maintaining the security of many applications, as detailed in the introductory portion of this chapter. Both Conditional Access System key management and Blockchain Technology key management are discussed here.

1. Key Management for Conditional Access Systems

The pay-per-view (PPV) model of television allows viewers to pay only for the channels they actually watch. Users pay the private broadcast provider for the television show. Events are shown to subscribers via broadcast by the broadcaster. All paying customers watch the event live and simultaneously. Pay-per-view is distinct from VOD. Pay-per-view video broadcasts are available to all customers at the same time on their televisions, while VOD allows users to purchase offline videos and watch them whenever they like.

Multimedia services that transmit a data stream to a group of people include pay-per-view broadcasts, live sporting events, live religious services, video conferencing, and so on. The encrypted data stream of the event is transmitted by the broadcaster. Users who have paid to access the broadcasts will be given the Control Word (CW), which serves as both an encryption and decryption key. Users would not be able to access the media files without the genuine key. Customers can only see the shows for which they have paid. The CAS abbreviation stands for "Conditional Access System," which describes the system's conditional access method.

2. Key Management for Blockchain Technology

Bitcoin, digital money based on a technology called the Blockchain, was suggested [28] in 2009 by an anonymous creator. Bitcoin is a digital currency where transactions may be made between users and where users can function as currency managers. Bitcoin, a digital virtual money, stands out since it doesn't require a trusted third party to verify purchases or sales.

Blockchain technology, also known as a decentralized secure ledger, is now one of the most talked-about innovations because of its potential to do away with the need for a trusted third party to verify transactions made via a P2P network. Validation of network transactions is achieved through the collective judgment of the currently active nodes. With Blockchain Technology, participants in a network maintain a shared, distributed ledger of all transaction history, which is periodically updated by the addition of a new "block" of transactions.

Blockchain's decentralized infrastructure uses PKI for authentication of entities and to safeguard the Blockchain's data integrity. To identify and authenticate the members to participate in the Blockchain network, Blockchain Technology relies on the Public Key Infrastructure (PKI). Several authors have proposed methods to authenticate Blockchain nodes without relying on a central authority. Reducing Blockchain Technology's reliance on CAs is a difficult problem to solve. Managing the vast number of keys required by Bitcoin's decentralized architecture is another difficulty with Bitcoin transactions. Bitcoin wallet private keys, seeds, and keys must be securely saved in external hardware in the Block chain network. The decentralized nature of node authentication is a key feature of Block chain Technology. Confidentiality of private Block chain data must also be protected. The privacy of sensitive data stored on Block chain networks is rarely discussed in the existing literature. A suitable GKM method for Block chain Technology is needed to ensure the privacy of sensitive documents while they are transmitted through the network.

CONCLUSION

As long as the cryptographic keys are kept safe, the confidentiality of the entire cryptographic system is maintained. One of the trickiest problems in cryptography is creating an effective system for managing keys. This study examines the problems with and solutions to key management in the context of cryptographic key management techniques. Key management life cycles have been developed for both symmetric and asymmetric cryptographic systems. The ability to revoke a key before its expiration is a crucial feature. A key revocation model has been suggested for automatically revoking keys and estimating how long they have left. The existing literature on key revocation is reviewed, and it is determined that the proposed key revocation model is superior. Cryptographic keys can be revoked quickly and easily with the help of the suggested key revocation paradigm. The distribution of a common key to all participants in a group conversation must be done securely and efficiently. Several group key management techniques have been examined, and two have been recommended as optimal in terms of rekeying cost, storage cost, and computational burden on central server, group secrecy, and group dynamism. One of the proposed schemes is an ECC-based group key management scheme, which offers improved cryptographic security over current systems while simultaneously decreasing the associated costs of member storage, central server computation, and member communication. When compared to popular existing group key management techniques, the suggested approach comes out on top in terms of computational overhead, storage cost, communication cost, and rekeying cost. Forward and backward secrecy are both attained by the suggested technique.

REFERENCES

- European Payment Coucil, “Guidelines on Cryptographic Algorithms Usage and Key Management,” *Déjà-vu*, no. December, pp. 1–73, 2018.
- 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.
- T. Bala and Y. Kumar, “Asymmetric Algorithms and Symmetric Algorithms: A
- Review,” in *International Conference on Advancements in Engineering and Technology*, 2015.

- 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.
- 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.
- G. Chaddoud, I. Chrisment, and A. Shaff, "Dynamic Group Communication
- Security," in *6th IEEE Symposium on computers and communication*, 2001, pp. 49–56.
- S. Rafaeli and D. Hutchison, "Hydra: a decentralized group key management," in *11th IEEE International WETICE: Enterprise Security Workshop*, 2002, pp. 62–
- 67.
- 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.
- 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.