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 10, Special Issue 2, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

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: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

A Review on Dynamic Key Based Cryptographic Techniques

Dr. D.J.Evanjaline[1], V. Elamurugu[2]

Asst. Professor, Department of Computer, Rajah Serfoji Govt Arts and Science College, Thanjavur, India[1]

Research Scholar, Department of Computer, Rajah Serfoji Govt Arts and Science College, Thanjavur, India[2]

ABSTRACT: Data security is one of the most daunting facets of today's information and communication technology. To ensure safe communication between various entities, cryptography is an important, effective and efficient component. In cryptography, encryption is the process to secure the data before it is communicated. It is a process of altering an intelligible form of data into an unintelligible form based on an encryption algorithm. To get the original data back, a decryption process is used. A key must be needed to encrypt or decrypt data. Protection is also based on holding the secret of the key. Many attacks will crack the key. A dynamic key is created to decrease the cryptanalysis attack risk. Dynamic keys are one-time used cryptographic keys, which significantly improve the security of cryptographic systems. In this paper, dynamic key-based cryptographic techniques are analyzed. This paper reviews the studies related to dynamic keys and makes some identification of the problem and offer some suggestions in the future for secure communication.

KEYWORDS: Cryptography, Encryption, Decryption, Dynamic Key

I. INTRODUCTION

Security plays a vital role in securely storing information and transmitting it through unknown networks. The secure communication is, therefore, the essential requirement of each network transaction. Cryptography is an essential component for secure communication and information transfer through security services such as confidentiality, integrity of data, control of access, authentication and non-repudiation. It offers a way of preserving confidential information by transferring it into unintelligible information which can only be viewed by the designated recipient by transforming it into the original text. The encryption process is called the process to turn the plaintext into cipher text with the key and the decryption process is called to reverse the encryption process [21]. Cryptographic algorithm design is secure and reliable, low cost, requires a small memory footprint, is simple to implement and is used on many platforms. The broad range of applications is built using various mathematical processes to secure cryptographic algorithms.

The cryptography system can be divided into keyless [15] and key-based system [20]. The association between plaintext and cipher text having a different version of the message is strictly based on the encryption algorithm in the keyless cryptosystem. The keyless cryptosystem is generally less secure than key-based systems because anyone can gain access to the algorithm will be able to decrypt every message that was encoded using keyless cryptosystem such as Caesar cipher [19]. In key based cryptosystem, the term key may refer to a simple key (e.g., 128-bitstring) or a more complex key construct (e.g., a symmetric key polynomial). A large number of keys need to be managed in order to encrypt and authenticate sensitive data exchanged. The key can be categorized into static and dynamic methods based on their capability in updating the encryption key at runtime [31].

In networking, static key is restricted to key pre-distribution and keys are fixed during the network's lifespan. However, if an encryption key is used for a long time, it becomes substantially more likely to be attacked. In contrast, dynamic key management regenerates keys over the lifespan of the network. Therefore, in network based operations, dynamic key management is known to be more promising [12]. Dynamic key management is a collection of processes used for re-keying, whether periodically or according to the demand of the network. Dynamic key management schemes greatly improve the survival and resilience of networks, as the keys of malicious node are revoked during the re-keying process.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Improved network survivability is the main benefit of dynamic keying, since any caught key(s) is exchanged in a method known as re-keying in a timely manner. Another benefit of dynamic keying is greater support for network expansion; the likelihood of network capture does not inherently increase when adding additional nodes, unlike static keying, which uses a fixed pool of keys.

In this paper, dynamic key based cryptographic technique is analyzed. This paper survey, dynamic key based encryption and decryption for different types of document like text and images. The remaining section of this paper is organized as follows: Section 2 explains cryptography concept, different types of keys used in cryptography is described in section 3, the related work of dynamic keys based cryptography methods are explained in section 4 and finally section 5 concludes the paper.

II. CRYPTOGRAPHY

Cryptography is the science of preventing unauthorized access to private information, maintaining data confidentiality and authentication, and other activities. The cryptography algorithm is a method or some formula that makes data or network secure by providing security. Cryptosystems are complex hardware and software combinations used to translate plain text into a sequence of unintelligible characters known as cipher text, then back to their original plaintext. Cryptography provides

- **Confidentiality** is the fundamental security function supplied by cryptography. It is a security service that holds data from an unauthorized user. Often it is referred to as secrecy or privacy.
- **Data Integrity** deals with the detection of any data modification. Data is changed by unauthorized party deliberately or inadvertently. It checks whether or not the data has been intact since the last approved user produced, transferred, or stored it.
- **Authentication** establishes the originator's identification. It ensures to the receiver that the data received has been sent only by a recognized and confirmed sender.
- **Non-repudiation:** A security service ensuring that a person is unable to refuse possession of a prior undertaking or action. It is a guarantee that the original data creator does not refuse the creation or transmission of the said data to a recipient or third party.

The terms used in cryptography is shown in Table 1

Table 1 Cryptography Terms

Terms	Description
Plain Text	Original text or message used in interaction
Cipher Text	Encrypted (Unreadable) format of plain text
Encryption	Conversion of plain text to cipher text
Decryption	Conversion of cipher text to plain text
Key	Numeric or Alpha numeric string
Key Size	Length of key in bits
Block Size	Fixed length string of bits
Round	Number of time to execute the encryption process

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Figure 1 shows the cryptographic techniques.

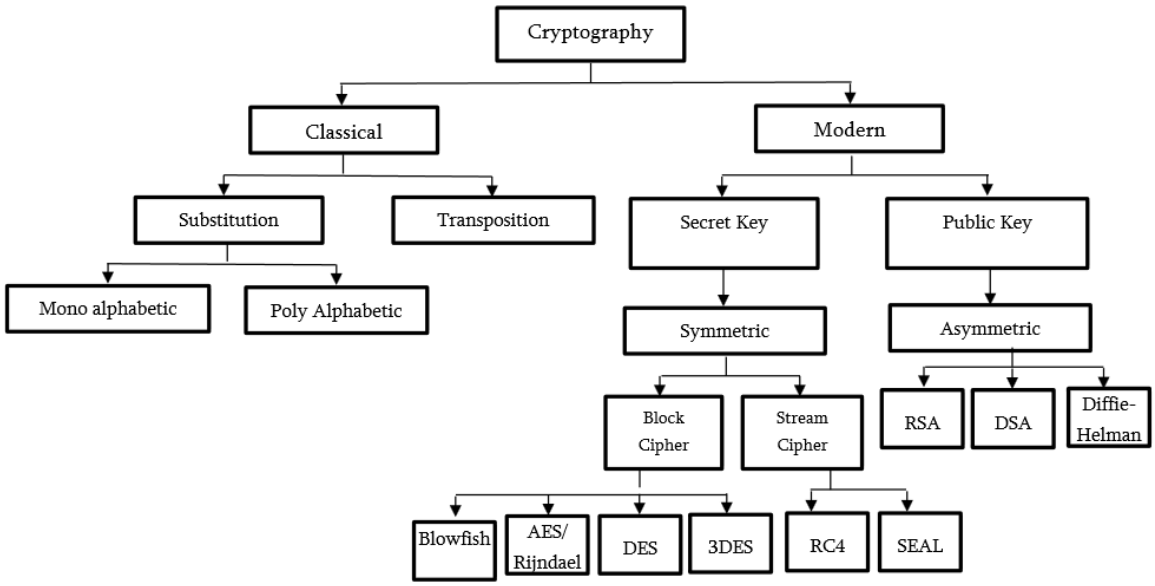

Figure 1 Cryptographic techniques [18]

III. KEYS IN CRYPTOGRAPHY

In cryptography, a key is a piece of information used to modify data by an algorithm. This is aimed at scrambling this data and is only available to individuals who have the necessary key to retrieve the desired information. This section explains some keys used in cryptography.

Secret Key Cryptography

In secret key cryptography the transmitter and recipient must use the same key to encrypt and decrypt a text. This increases security risk as it is necessary to deliver the key in a secure way to decrypt the message to the recipient of the message. If intruders get hold of the key, the hidden message can be decrypted, thereby compromising the entire device. Figure 2 shows the secret key cryptography system.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

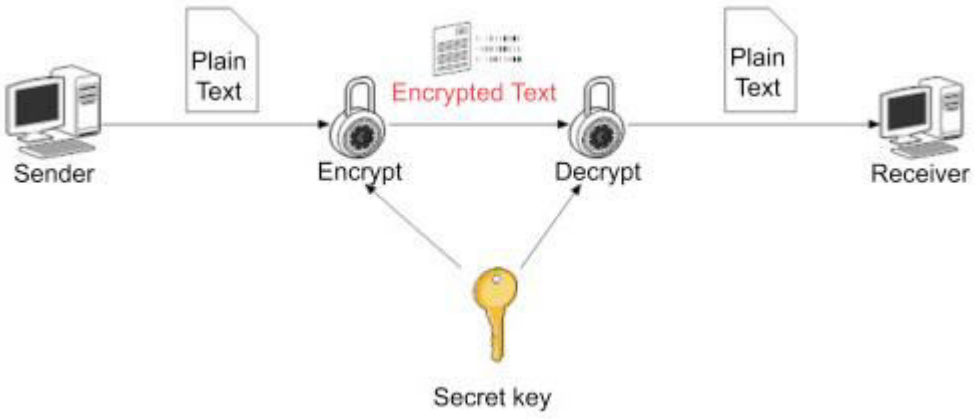

Figure 2 Secret Key cryptography [17]

Public Key Cryptography

Two keys are used in public key cryptography, one for encryption and the second for decryption. Without compromising the private key, the public key is spread everywhere. To encrypt the message, a user will use his friend's public key. To decrypt this message, the recipient will use his/her private key (which should be kept secret).

Two parts of this key pair are mathematically related, even though the two keys are different. The public key is used for plain text encryption or digital signature authentication, while the private key is used for cipher text decryption or for digital signature production. Only using the same private key pair will messages encrypted with a public key be decrypted. This technique is much more reliable than symmetric cryptography, as the sender and receiver may use any communication method to share their public keys while keeping their private keys secret to decrypt the received messages. Figure 3 shows the public key cryptography

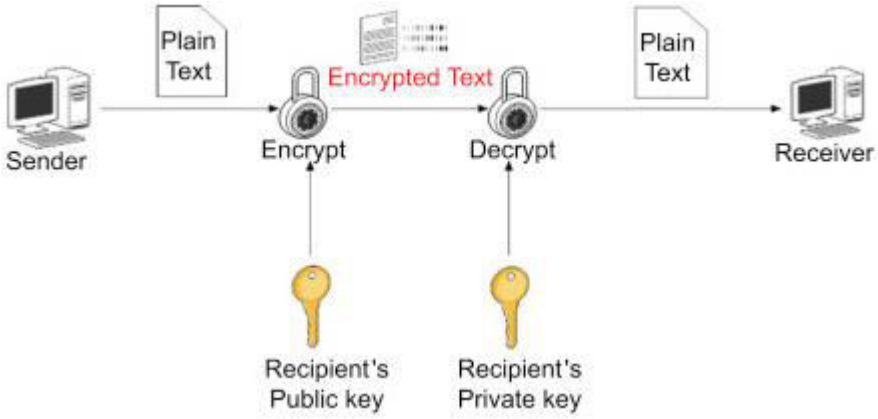

Figure 3 Public key cryptography

Digital Signature

Digital signatures include confirmation of the integrity and originator of the associated records, but go one step further and also provide the notion of non-repudiation, the signatory being unable to legitimately say that the signature has been falsified. Figure 4 shows the digital signature.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

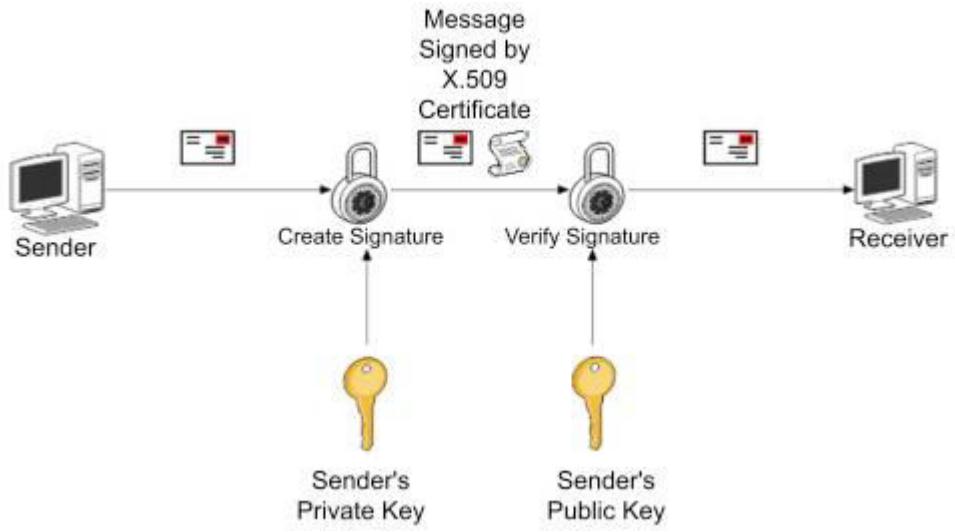

Figure 4 Digital Signature

Cryptographic Hash Function

Another reliable method of encryption is the hash function. Hashing is the process of creating a number out of a text string. The hash is significantly smaller than the text itself and is produced by a formula in such a way that any other text is highly unlikely to produce the same hash value. Hashing is commonly used in the security of information and in forensic systems. If the user wants to submit an encrypted file, the file hash should be determined first. Then the file is encrypted and sent to the recipient along with the created hash number. The file will be decrypted by the receiver and his hash number determined. There is a very high chance that the message has not been compromised if both hashes are the same.

There are four key properties of the ideal cryptographic hash function:

- For any given message, it is easy to calculate the hash value.
- A message from a given hash is almost impossible to produce.
- Without changing the hash, it is impossible to change a message.
- Finding two separate messages with the same hash is unlikely.

There are several different algorithms for hashing, such as MD2, MD5, SHA, and SHA-1.

IV. DYNAMIC KEYS – REVIEW

This section reviews related work on dynamic key based cryptographic techniques.

4.1 Dynamic key based Authentication

Users that attempt to access network services need to be authenticated. Authenticated key agreement protocols authenticate the identity of users to ensure that a session in which the group members can communicate with each other can be formed only by the intended group members. A novel community key agreement protocol was proposed in [23] with disprovable authentication against insider attack. The community participants are unable to disclose the source of the messages to any party, and the entire transcript process can still be simulated by any subgroup participants. In [29] an

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

authenticated asymmetric community key agreement protocol is suggested; without relying on the trusted dealer to transmit the secret key, which provides protection against active and passive attacks.

A one-round affiliation-hiding authenticated asymmetric group key agreement was proposed in [30] with semi-trusted group authority, which can preserve individual privacy, but the calculation of this protocol is very high, not suitable for use in wireless network power-limited mobile devices. A one-round authenticated dynamic protocol was proposed by Li et al. [24] for symmetric group key agreement. They used public-key cryptography based on identity to authenticate users rather than public key infrastructure and public-key cryptography without certificates. A dynamic and cross-domain authenticated asymmetric community key agreement is proposed by Qikun et al., [14]. To mitigate the potential risks of key issuer and the difficulty of certificate management, the protocol establishes cross-domain authentication mechanisms. It allows the dynamic group key update of nodes for group key forward confidentiality and backward protection, and also achieving the key self-certified, the group key agreement participated by the participant will self-certify if the group keys measured are correct.

A new post-quantum constant-round dynamic GKE protocol from Ring Learning with Errors without a trust authority is proposed in [1]. Traditional GKE dynamic protocols rely on number-theoretical problems that are vulnerable to quantum computing attacks, such as the Diffie-Hellman problem. For heterogeneous WSNs, an effective dynamic authentication and key management system is suggested in [6]. The key idea is to provide both authentication and key establishment with a single lightweight protocol while optimizing the level of security. The key distribution algorithm is based on pre-existing dynamic key generation information and does not require a secure channel and sharing process that improves protection, energy efficiency and memory usage. A group-based authentication key agreement protocol with dynamic policy updating proposed in [25]. In particular, choose an asynchronous secret sharing scheme to enforce distributed authentication and session key establishment in the long term evaluation advanced networks in combination with the Diffie-Hellman key exchange scheme and to achieve dynamic updating of the communication system access authority.

A protocol for a complex privacy-preserving and lightweight dynamic key agreement proposed in [10] for vehicles to grid in social IoT. This protocol resists numerous threats, including impersonation, offline password guessing, man-in-the-middle, replay, and trace attacks, maintaining anonymity, perfect forward confidentiality, protection of the session key, and stable shared authentication. A new lightweight technique Protean Authentication Scheme proposed in [11]. This method constantly change the authentication keys at regular intervals thereby reducing the attack span due to the pressing fact that the edge nodes are exposed to direct physical attacks while deployed in the open. A novel dynamic ID-based anonymous two-factor authentication key exchange protocol proposed in [22].

4.2 Dynamic key based Encryption

Nowadays, data and information transfers are typically carried out by means of unreliable public networks. The use of insecure communication networks, such as social media, is very vulnerable to third parties' misuse of information. It is therefore necessary to preserve the confidentiality of data sent through unsecured networks, including text, images and video. Encryption is the one of the way to secure the data. This section reviews dynamic key based encryption for text and image.

Dynamic public-key threshold encryption, suggested by Delerablée and Pointcheval [32], is an extension of ordinary threshold encryption that allows decryption servers to engage the system even after the setup stage and dynamically choose the authorized set and decryption threshold. Dynamic TPKE (threshold public-key encryption) schemes proposed in [27] that prevent the use of random oracles and q-type assumptions with decryption consistency. Two dynamic TPKE constructions are proposed by the author, both of which use public key encryption with non-interactive opening.

Securing color image transmission using a dynamic key generator compression-encryption model and effective symmetric key distribution is suggested in [2]. It includes a stable key generation model that for each communication

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

session always produces different keys; a cryptosystem model that uses a selective compression-cryptographic approach, which is followed by implementing the principle of multiple encryptions to enhance data confidentiality; and a model that safely and efficiently distributes symmetric keys.

Orthogonal frequency-division multiplexing (OFDM) based encryption systems at the physical layer are tested, evaluated and vulnerabilities are found in [7]. Encryption in the frequency domain is shown to slightly reduce the effects of channel fading and increase the efficiency of the bit error rate. Time-domain encryption, on the other hand, is shown to be more stable. In addition to a new method for updating cipher primitives for input OFDM symbols or frames, a dynamic secret key approach that improves the security level of OFDM-based encryption schemes is suggested.

A dynamic key generation scheme is proposed in [8] which integrate a pre-shared/stored secret key with a dynamic nonce extracted from channel information. The primary benefit of this technique is that it ensures a degree of high security with reduced overhead. In addition, upon any change in channel parameters, the obtained dynamic key can be changed frequently. To avoid unauthorized synchronization or channel measurement by invalid users, a preamble encryption scheme is also proposed. The security level of the cipher scheme proposed depends primarily on the secret key and the dynamicity of the channel used for each frame symbol to update the cipher primitives.

A lightweight cipher algorithm based on a dynamic structure with a single round consisting of simple operations is proposed in [13]. A dynamic key is generated in this algorithm and then used to build two robust tables of substitution (dynamic permutation table, and two pseudo-random matrices.). This complex cipher structure reduces the number of rounds to a single one while retaining a high degree of randomness and protection. A good balance between security and performance levels can be achieved by dynamic key-based cryptography algorithms. A set of cryptographic primitives are generated and modified using a dynamic key. This implies that for the same plaintext, distinct cipher text can be obtained since different cryptographic primitives are used. The algorithms explained in [8] [13] [9] need only one round iteration and, in addition to avoiding diffusion operations, make use of simple operations. The new generation of these cryptographic algorithms reduces the latency, resources and overhead of computing needed.

In [16], a new chaos-based image encryption algorithm is implemented with dynamic key selection mechanisms. It introduces a dynamic selection mechanism for keystream selection and sequence group selection that extends the key selection range and allows us to dynamically picks the keys using the corresponding plaintext pixels. This method increases the security level. For reliable image transmission, a Secure Dynamic Decision based Permutation and Butterfly Network Topology based Diffusion model is proposed in [4]. For creating initial vectors of Henon map, two separate models are implemented, which in turn used to generate the random key sequence for each encryption to achieve high sensitivity to the plain image. The digital image encryption scheme [5] is proposed based on the chaotic method of Lorenz. The hash value of the plain image is embedded in the cryptosystem during the process of creating chaotic key streams to dynamically alter the initial secret keys to increase the level of security. Because a single replacement box (s-box) is used to encrypt digital files, it does not function well for both higher and lower grey levels. A new substitution technique using multiple S-boxes with dynamic substitution is proposed in [3] to solve this problem. Table 2 and Table 3 shows the comparison of dynamic key methods based on different domain and key size with future suggestions.

Table 2 Comparison of Dynamic key methods based on different domain

Method	Domain	Description	Drawback / Future Suggestion
Protean Authentication [11]	IoT	This method provides secure authentication between gateway node and edge node. It uses AES algorithm to encrypt the authentication credentials	Use lightweight hash based biometric authentication scheme
EDAK [6]	Heterogeneous WSNs	To provide both authentication and key establishment with a	This scheme does not consider replay attack

		single lightweight protocol while enhancing the level of security. The key algorithm for distribution is based on preexisting data to produce dynamic keys and does not need any secure channel.	and insider attack.
Image compression-encryption model with dynamic key generator[2]	Social media	A new cryptosystem model that is capable of solving key management problems and preserving the data protection of the images transmitted.	This model can be extended to video files, which, by enhancing the compression system, has a much larger data size.

Table 3 Comparison of methods based on dynamic key size

Algorithm	KeySize	KeyGen Time	Future Suggestion
AES-ECC [26]	192 bit	140e(ms)+20d(ms)	encryption times that change according to the input text and the key used for encryption
HMAC-SHA-512 [9]	64 bytes	232.726(ms)-189.4(ms)	Include Authentication-Encryption operation mode with one single pass
DLSeF [28]	32, 64, and 128 bit	7.301e+09, 3.136e+19, 5.7848e+35 ns	This method take more time to generate the key. In future, reduce the key generation time.
DC-AAGKA [14]	160 bits	3.886ms	Apply other security group applications
DRAG [1]	128 bit	3 msec	Check key reuse attack
Image Encryption algorithm [5]	256 bit(512X512)	86e(ms)-71d(ms)	High security and avoid large key space
EDAK [6]	16 bytes	0.77 ms	highly dynamic, with roaming nodes and multiple network .

V. CONCLUSION

Key management has become an essential security concern considered by industrial researchers with the comprehensive and extensive application of wireless sensor networks in which many techniques have been proposed so far. The aim of key management is to dynamically create and maintain reliable channels between nodes that communicate. To reduce the crypt analysis attack risk, a dynamic key is developed. Dynamic keys are once-used cryptographic keys that enhance the security of cryptographic systems dramatically. This paper survey, dynamic key based authentication, encryption and decryption for different types of document like text and images. Most of the paper uses hybrid method for key generation, which increases the computation overhead and also take more time to generate the key. In the future, reduce

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

the computational overhead and key generation time. In addition to this develop a framework which includes, authentication, encryption, decryption, data integrity verification using dynamic keys.

REFERENCES

[1] R. Choi, D. Hong, S. Han, S. Baek, W. Kang and K. Kim, "Design and Implementation of Constant-Round Dynamic Group Key Exchange from RLWE," in IEEE Access, vol. 8, pp. 94610-94630, 2020
[2] E. Setyaningsih, R. Wardoyo, A. K. Sari, "Securing color image transmission using compression-encryption model with dynamic key generator and efficient symmetric key distribution", Digital Communications and Networks, vol. 6, no. 4, pp. 486-503, 2020
[3] A. Shafique, F. Ahmed, "Image Encryption Using Dynamic S-Box Substitution in the Wavelet Domain", Wireless Pers Commun, vol. 115, pp. 2243–2268, 2020
[4] R. Vidhya, M. Brindha, "A novel dynamic chaotic image encryption using butterfly network topology based diffusion and decision based permutation", Multimed Tools Appl, vol. 79, pp. 30281–30310, 2020
[5] O.M. Al-Hazaimeh, M.F. Al-Jamal, N. Alhindawi, et al, "Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys", Neural Comput & Applic, vol. 31, pp. 2395–2405, 2019
[6] S. Athmani, A. Bilami, D. E. Boubiche, "EDAK: An Efficient Dynamic Authentication and Key Management Mechanism for heterogeneous WSNs", Future Generation Computer Systems, vol. 92, pp. 789-799, 2019
[7] R. Melki, H. N. Noura, M. M. Mansour and A. Chehab, "An Efficient OFDM-Based Encryption Scheme Using a Dynamic Key Approach," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 361-378, 2019
[8] H.N. Noura, R. Melki, A. Chehab and M. Mansour, "A Physical Encryption Scheme for Low-Power Wireless M2M Devices: a Dynamic Key Approach", Mobile Netw Appl, vol. 24, pp. 447–463, 2019.
[9] H. N. Noura, A. Chehab, R. Couturier, "Efficient and secure cipher scheme with dynamic key-dependent mode of operation", Signal Processing: Image Communication, vol. 78, pp. 448-464, 2019
[10] K. Park, Y. Park, A. K. Das, S. Yu, J. Lee and Y. Park, "A Dynamic Privacy-Preserving Key Management Protocol for V2G in Social Internet of Things," in IEEE Access, vol. 7, pp. 76812-76832, 2019
[11] S. Sathyadevan, K. Achuthan, R. Doss and L. Pan, "Protean Authentication Scheme – A Time-Bound Dynamic KeyGen Authentication Technique for IoT Edge Nodes in Outdoor Deployments," in IEEE Access, vol. 7, pp. 92419-92435, 2019
[12] S. R. Nabavi and S. M. Mousavi, "A review of distributed dynamic key management schemes in wireless sensor networks", JCP, vol. 13, no. 1, pp. 77-89, 2018.
[13] H. Noura, A. Chehab, L. Sleem, M. Noura, R. Couturier, M.M. Mansour, "One round cipher algorithm for multimedia IoT devices", Multimed Tools Appl, vol. 77, pp. 18383–18413, 2018
[14] Z. Qikun, G. Yong, Z. Quanxin, W. Ruifang, T. Yu-An, "A Dynamic and Cross-Domain Authentication Asymmetric Group Key Agreement in Telemedicine Application", Access IEEE, vol. 6, pp. 24064-24074, 2018.
[15] Y. Zhang, Y. Xiang, T. Wang, W. Wu, J. Shen, "An over-the-air key establishment protocol using keyless cryptography", Future Generation Computer Systems, vol. 79, no. 1, pp. 284-294, 2018
[16] X. Chai, K. Yang, Z. Gan, "A new chaos-based image encryption algorithm with dynamic key selection mechanisms", Multimed Tools Appl, vol. 76, pp. 9907–9927, 2017
[17] N.A Hassan, R Hijazi, "Chapter 5 - Data Hiding Using Encryption Techniques", Editor(s): Nihad Ahmad Hassan, Rami Hijazi, Data Hiding Techniques in Windows OS, Syngress, pp. 133-205, 2017
[18] E. Jincharadze, "Critical Analysis Of Some Cryptography Algorithms", Scientific and Practical Cyber Security Journal, vol. 1, no. 2, pp. 60-68, 2017.
[19] T. Limbong, P.D.P. Silitonga, "Testing the Classic Caesar Cipher Cryptography using of Matlab", International Journal of Engineering Research & Technology (IJERT), vol. 6 no. 2, 2017
[20] F. Maqsood, M. M. Ali, M. Ahmed, and M. A. Shah, "Cryptography: A comparative analysis for modern techniques," International Journal of Advanced Computer Science and Applications, vol. 8, no. 6, pp. 442–448, 2017.
[21] M. F. Mushtaq, S. Jamel, A. H. Disina, Z. A.Pindar,N. S. Ahmad Shakir,M. Mat Deris, "A Survey on the Cryptographic Encryption Algorithms", International Journal of Advanced Computer Science and Applications, vol. 8, no. 11, 2017

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

[22] Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen and L. Fang, "Provably Secure Dynamic ID-Based Anonymous Two-Factor Authenticated Key Exchange Protocol With Extended Security Model," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 6, pp. 1382-1392, June 2017

[23] H. Zhu and Y. Zhang, "An efficient chaotic maps-based deniable authentication group key agreement protocol", Wireless Pers. Commun., vol. 96, no. 1, pp. 217–229, 2017.

[24] M. Li, X. Xu, C. Guo, and X. Tan, "AD-ASGKA—Authenticated dynamic protocols for asymmetric group key agreement," Secur. Commun. Netw.,vol. 9, no. 11, pp. 1340–1352, Jul. 2016.

[25] J. Li, M. Wen and T. Zhang, "Group-Based Authentication and Key Agreement With Dynamic Policy Updating for MTC in LTE-A Networks," in IEEE Internet of Things Journal, vol. 3, no. 3, pp. 408-417, June 2016

[26] N. Mathur and R. Bansode, "AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection," Procedia Comput. Sci., vol. 79, pp. 1036–1043, 2016

[27] Y. Sakai, K. Emura, J.C.N. Schuldt, G. Hanaoka, K. Ohta, "Constructions of dynamic and non-dynamic threshold public-key encryption schemes with decryption consistency", Theoretical Computer Science, vol. 630, pp. 95-116, 2016

[28] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "A dynamic key lengthbased approach for real-time security verification of big sensingdata stream," inInternational conference on web information systems engineering, Springer, pp. 93–108, 2015

[29] R.S. Ranjani, D.L. Bhaskari, and P.S. Avadhani, "An extended identity based authenticated asymmetric group key agreement protocol," Int.J. Netw. Secur., vol. 17, no. 5, pp. 510–516, 2015.

[30] C. Xu, L. Zhu, Z. Li, and F. Wang, "One-round affiliation-hiding authenticated asymmetric group key agreement with semi-trusted group authority," Comput. J., vol. 58, no. 10, pp. 2509–2519, Oct. 2015.

[31] X. He, M. Niedermeier, H. de Meer, "Dynamic key management in wireless sensor networks: A survey", Journal of Network and Computer Applications, vol. 36, no. 2, pp. 611-622, 2013

[32] C. Delerablée, D. Pointcheval, "Dynamic threshold public-key encryption", D. Wagner (Ed.), CRYPTO 2008, Lecture Notes in Comput. Sci., vol. 5157, Springer, pp. 317-334, 2008

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

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

Scan to save the contact details