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 13, Issue 8, August 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

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

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

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308124|

Pioneering Multi-Key Cryptography for Secure Video Exchange

Dr. M. Selvi, Sahil Guptha, Y Samarth, Rohith PG

Associate Professor, Department of Computer Science Engineering, Rajarajeswari College of Engineering, Bangalore, Karnataka, India

U.G. Student, Department of Computer Science Engineering, Rajarajeswari College of Engineering, Bangalore, Karnataka, India

ABSTRACT: The increasing prevalence of online video streaming in people's daily entertainment habits has brought about a heightened focus on safeguarding copyright and combating piracy within real-time video streaming systems. In response to this pressing concern, a groundbreaking research initiative has introduced a cutting-edge multi-key and hybrid cryptography methodology to enhance security measures. This innovative approach involves the utilization of continuous systems based on Elliptic Curve Cryptography as pseudorandom encryption key generators for the encryption and decryption of video content. By generating multiple keys to encrypt and decrypt small segments of video files dynamically based on the video data, this method ensures robust protection against unauthorized access. The software implementation of this encryption and decryption process has been successfully carried out on the Android platform, with dedicated applications developed for both senders and recipients to facilitate seamless video streaming. Through rigorous testing on various devices and streaming scenarios, the proposed system has demonstrated exceptional performance and security capabilities, underscoring its effectiveness in safeguarding valuable video content.

KEYWORDS: Asymmetric key cryptography, multi-key encryption

I. INTRODUCTION

Real-time media streaming has become increasingly common due to the rapid advancements in Internet infrastructure and the technologies that drive these developments. Streaming media involves the continuous delivery of audio or video data over the Internet, allowing users to access content before it is fully downloaded. The popularity of video conferencing, web-based TV services, e-learning, telemedicine, and platforms like YouTube and Netflix offering live streaming has led to a significant increase in Internet traffic sharing.

With the rise of Over-The-Top (OTT) services and similar applications, concerns regarding security and privacy have become more pronounced. Illegal sharing of media content and pirated videos pose risks to sensitive data, particularly in fields like telemedicine and real-time video streaming. Various security measures, such as forensic watermarking, trusted compute environments, and encryption, are employed to protect content.

As technology evolves and embedded devices become more prevalent for content consumption, new content protection strategies that rely less on hardware are needed. Authentication, encryption, and key management are key challenges in ensuring secure video communication. Cryptography techniques, including symmetric and asymmetric key cryptography, play a crucial role in enhancing security in multimedia communication.

While symmetric key cryptography, such as the Advanced Encryption Standard (AES), is commonly used, challenges in key management persist, especially in decentralized networks. Asymmetric cryptography methods like RSA and Elliptic Curve Cryptography (ECC) are gaining popularity for overcoming these challenges and providing higher security for video content streamed over the Internet.

In video streaming applications, encryption methods using asymmetric key cryptography can offer enhanced security by generating separate keys for each chunk of video data. This approach, combined with automatic key generation techniques, aims to provide dynamic and robust security for video streaming applications. The use of RSA and ECC

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

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308124|

methods, along with multi-key techniques and automatic key generation, contributes to the overall security of video communication.

The conclusion highlights the importance of leveraging advanced cryptography techniques to address the security challenges in video communication effectively.

II. RELATED WORK

Zia et al. [20] introduced a novel method based on chaos theory for generating pseudorandom numbers that can enhance cryptographic techniques. This approach aids in the automatic generation of random numbers.

Kezia and Sudha [21] developed a video encryption scheme utilizing chaotic maps, where the video sequence is encrypted by splitting it into frames and further into macro-blocks for larger frames.

Khan et al. [22] proposed an ECC-based authentication and encryption technique for IoT applications, focusing on analyzing computational costs and processing delays. Imam et al. [23] reviewed RSA-based cryptographic techniques, highlighting their suitability for various applications.

Sen et al. [24] studied ECC-based cryptography techniques on video data, noting the efficiency of ECC in encryption and decryption operations.

Chen and Ye [27] implemented an image encryption method using hash SHA 3, RSA, and compressive sensing to enhance security. Hegde and Jagadeesha [28] designed a crypto technique using ECC with multiple elliptic curves for improved data robustness.

Murad Rahouma [29] explored hybrid cryptography models for cloud security. Ghosh et al. [30] proposed a hybrid method for data confidentiality and security on the Internet.

Zhang and Gao [31] introduced a method for encoding video data using layered coding. Yu et al. [32] discussed the applications of hybrid encryption algorithms in software securities, particularly in video surveillance software.

Khan et al. [33] studied a Hybrid encryption technique using different encryption methods for message segmentation and authentication.

Chowdhary et al. [34] analyzed image encryption and decryption using hybrid ECC with various ciphers. Dave and Gayathri [35] discussed the pros and cons of storing biometric data on the cloud and proposed a hybrid cloud-based encryption method.

Hamdi et al. [36] proposed a hybrid encryption algorithm based on block and stream ciphers using chaotic systems. Yuet al. [37] explored a unique hybrid model for security tests in video applications. Zhu et al. [38] proposed a hybrid encryption approach based on blockchain technology.

Hosny et al. [39] developed a chaotic logistic map-based encryption method for enhanced security.
Alarifi et al. [40] proposed a cryptosystem combining DNA encoding sequences, Arnold chaotic map, and modified Mandelbrot sets for video streaming applications.

In conclusion, the hybrid model is effective in enhancing data security, with ECC-based techniques being suitable for real-time video streaming applications due to their efficiency in processing.

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

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308124|

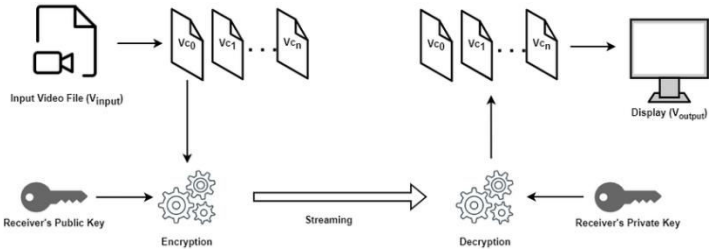

Fig 1. Secure video communication using asymmetric key cryptography

III. PROPOSED METHOD

In our research, we have introduced an innovative approach to enhance security in video communication. The method employs a multi-key cryptographic technique, combining elements of RSA (Rivest–Shamir–Adleman) and ECC (Elliptic Curve Cryptography). By utilizing this hybrid approach, we achieve asymmetric encryption, ensuring robust security for video content. Specifically, our methodology involves generating dynamic keys based on mathematical equations and user attributes. These keys are used for encryption and decryption processes, significantly bolstering the overall security of video material.

3.1. PROBLEM STATEMENT

In video streaming applications, content is transmitted from the media server to client devices on-demand. Ensuring the security of digital video content involves several key aspects, including conditional access, user authentication, content copy control, and video content tracking. Cryptography techniques play a crucial role in achieving these security measures. However, creating a comprehensive solution for digital video security remains a challenging research problem.

Numerous studies have explored the benefits of asymmetric key cryptography methods to address key management challenges. Unfortunately, existing methods do not adequately support dynamic and automatic multi-key techniques, which are essential for enhancing security in video communication applications. Consequently, there is a need for an automatic and dynamic key management approach. This work focuses on a multi-key encryption technique that combines RSA (Rivest–Shamir–Adleman) and ECC (Elliptic Curve Cryptography) to address this gap.

3.2. PROPOSED ALGORITHMS

The proposed method aims to enhance security in video communication by generating multiple dynamic keys using a combination of RSA (Rivest–Shamir–Adleman) and ECC (Elliptic Curve Cryptography) asymmetric key cryptography techniques. The primary goals of these techniques are as follows:

Securing Video Data: The proposed approach ensures the security of video data based on both content characteristics and unique receiver identifications.

Leveraging Hybrid Cryptography Techniques: To maximize security, the proposed method utilizes a hybrid approach that combines RSA, ECC, and AES (Advanced Encryption Standard) techniques.

Improving Security with Multi-Key Encryption: By employing multi-key encryption, the overall security of the system is enhanced.

Enhancing Security for Video Chunks: Each video is divided into smaller chunks (each approximately 1 MB in size), and individual keys are generated for these segments.

Reducing Multi-Key Management Overhead: The proposed method automates key generation, minimizing the complexity of managing multiple keys.

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

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308124|

The key generation process begins by passing video data to the key generation module. This module requires the receiver's Public Key (RPkey) and MAC address (Rmac) to improve the uniqueness of the generated keys. These attributes are stored on the sender's side and are necessary throughout the video communication process.

Algorithm 1 and Figure 3 outline the steps involved in key generation. The process starts by creating a unique video identification (VID) using the first video chunk (Vc0). The module extracts the first 16 bytes from Vc0 before encryption and converts them into a base64 string format. The resulting VID is temporarily stored in a file for quick access. Subsequently, the first video chunk is encrypted using the VID and RSA cryptographic techniques.

Video Chunk Key Generation:
The algorithm generates unique keys for each video chunk.
It uses the Video ID (VID), the receiver's Public Key (RPkey), and the receiver's MAC address (Rmac) in the process.
The key derivation is based on an elliptic curve equation: (y^2 = x^3 + ax + b).
In this context, VID corresponds to (a) and Rmac corresponds to (b).
The modified equation for key generation is: (Keya = x^3 + VID \cdot x + Rmac).

Continuous Key Generation:
For the first video chunk (Vc0), the algorithm uses Equation (2).
Subsequent video chunks (Vc1, Vc2, …) use the previously computed Keya.
The updated equation for subsequent chunks is: (Keya = x^3 + Keya \cdot x + Rmac).

AES Encryption Using Chunk-Specific Keys:
Each video chunk is encrypted using the unique key generated for that chunk.
The proposed method ensures that no keys are shared.
By generating keys dynamically during video communication, maximum security is achieved.
Even if one chunk is compromised, the remaining video data remains secure.

IV. EXPERIMENTATION

Mobile Platform Implementation:
The suggested cryptography technique is implemented on a mobile platform, specifically an Android-based application.
The application handles encryption, decryption, and video streaming.

Sender-Side Process:
Sender devices store video content and video metadata.
When a receiver requests to stream a video file, the sender application verifies the recipient's identity.
Information about the recipient (username, password, public key, MAC address) is retrieved during the sign-up process and stored in the sender's database.

Receiver-Side Tasks:
The receiver module handles decryption and video playback.
Encrypted video chunks are received and decrypted using the proposed module.
Necessary keys are obtained from the receiver's database, eliminating the need for key exchange.
RSA implementation is used to obtain the first video parts.
Video data is displayed on the device's screen via the application, avoiding the need to save received video data.

Database Implementation:
A database is essential for storing video metadata and receiver information.
On the sender side, recipient information (username, MAC address, public key) is stored.
The sender's public key and communication session's video metadata are similarly stored in the receiver-side database.

Dynamic Key Generation:
The proposed approach automatically generates dynamic keys using an elliptic curve equation (ECC).

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

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308124|

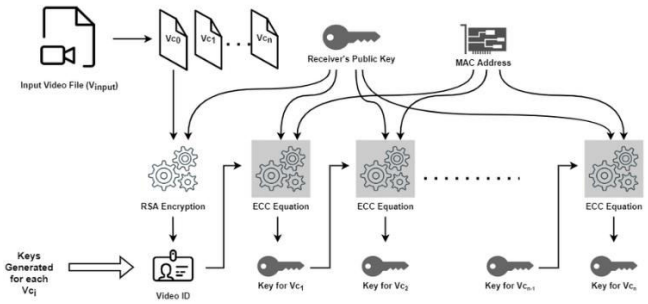

FIG 2. BLOCK DIAGRAM OF PROPOSED KEY GENERATION TECHNIQUE

4.1. DELAY FOR SPLITTING FILE TO CHUNK

The application's performance in creating video chunks from the video file was measured, focusing on the use of video chunk-based encryption. The investigation aimed to understand the processing time within the video processing module. The FFMpeg utility reads the chunk size from the sender, and the chunk is then divided into the nearest full frame based on user input. Figure 4 illustrates the time needed by the video processing module to split the video file into several chunks. As expected, latency gradually increases as the file size grows. While the technique does not unexpectedly lengthen the time, the overall delay results from chunk formation—a necessary trade-off to achieve high security.

4.2. TIME TO GENERATE THE KEYS

In this experiment, the researchers aimed to assess the impact of multi-key encryption and decryption processes. To achieve this, they calculated the time required to generate encryption keys. It's important to note that the method and equation used to derive these keys remain consistent for both encryption and decryption. Therefore, the delay calculated during encryption was applied for analysis purposes in this context.

Figure 5 illustrates the time needed to generate each key. Initially, the receiver's public key and partial video data serve as the foundation for the key used to encrypt the first video chunk. Subsequent keys are obtained using the receiver's MAC address, public key, and previously computed key. Importantly, the parameters' lengths remain consistent throughout this procedure, resulting in minimal variation in the time between each key generation.

4.3. TIME TO ENCRYPT VIDEO CHUNKS

The researchers aimed to assess the impact of multi-key encryption and decryption processes. To achieve this, they calculated the time required to generate encryption keys. It's important to note that the method and equation used to derive these keys remain consistent for both encryption and decryption. Therefore, the delay calculated during encryption was applied for analysis purposes in this context.

Figure 5 illustrates the time needed to generate each key. Initially, the receiver's public key and partial video data serve as the foundation for the key used to encrypt the first video chunk. Subsequent keys are obtained using the receiver's MAC address, public key, and previously computed key. Importantly, the parameters' lengths remain consistent throughout this procedure, resulting in minimal variation in the time between each key generation.

4.4. TIME TO ENCRYPT THE VIDEO FILES

This section discusses the overall execution time for the video processing pipeline, which encompasses the entire journey from producing video chunks to generating encrypted video segments. The end-to-end latency of this process is visualized in Figure 7.

The research findings reveal a consistent trend: as the file size increases, the time required for processing also grows proportionally. This behavior is typical across various applications. Importantly, Figure 7 specifically highlights the additional delay introduced by each individual video chunk within the clip. Notably, this delay does not impact video streaming or playback on the receiver's side.

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

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308124|

4.5. NUMBER OF KEYS GENERATED

The quantity of keys generated corresponds to the number of video chunks produced. This aspect is crucial for the study, as the proposed solution leverages multiple key technologies to enhance security. Interestingly, the use of multiple keys does not significantly impact memory usage. These keys are only temporarily stored at both the transmitter and receiver sides. Furthermore, since each key is employed only once, an increase in the number of keys does not affect the fetching delay.

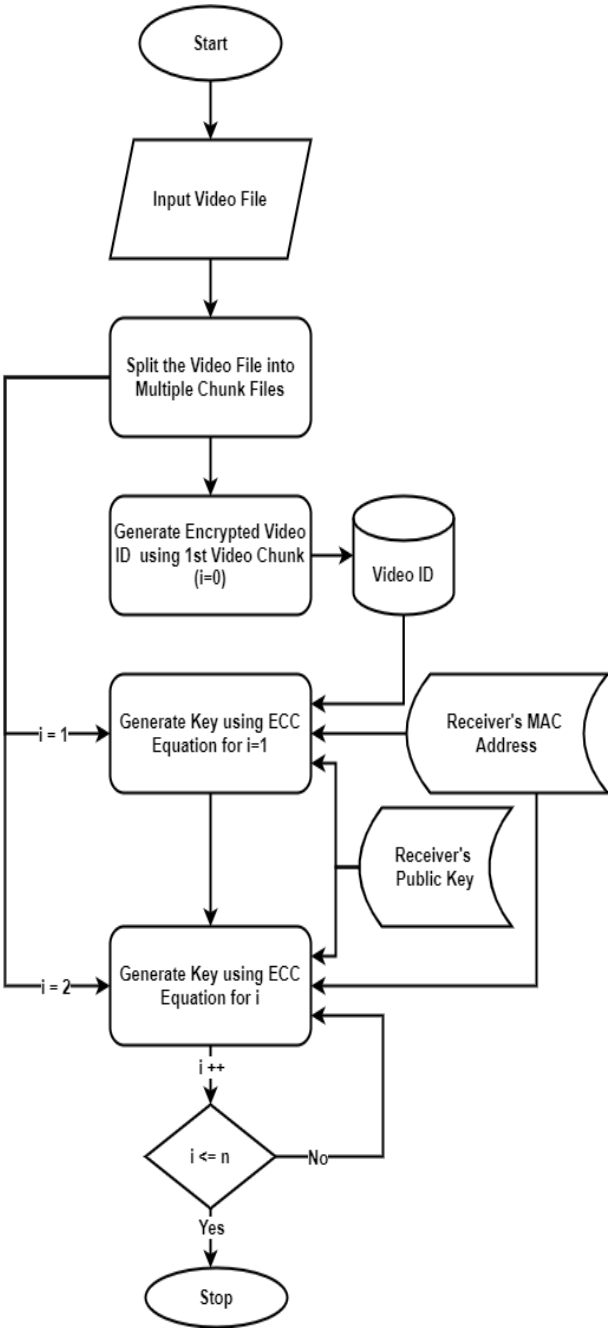

FIG 3. BLOCK DIAGRAM OF PROPOSED KEY GENERATION TECHNIQUE.

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

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308124|

V. CONCLUSION

This work introduces an innovative and secure platform that leverages a suggested cryptographic method for video file encryption and decryption. The approach combines hybrid and multi-key cryptography, enhancing the security of video content. Specifically, the platform employs RSA, the ECC equation, and AES to safeguard the video data.

Here are the key points:

Multi-Key Solution: The proposed method divides the video into multiple chunks and encrypts each chunk with a distinct key. Importantly, receivers do not have direct access to these keys. Instead, the receiver application generates the necessary keys based on the encrypted chunks it receives. This dynamic and automatic process ensures efficient decryption.

Implementation Details: The application is developed for the Android platform on the receiver side. A Java-based server-side program is created to implement and test the suggested method. Distinct modules are designed based on the identified tasks.

Consistent Delay and Real-Time Communication: Testing with video files of various sizes demonstrates that the application maintains consistent delay and supports real-time video communication. This reliability is crucial for seamless user experience.

Hybrid Approach: The platform combines well-established algorithms—AES, RSA, and ECC—to enhance video content security. By leveraging these cryptographic techniques, the system ensures robust protection.

Advantages for Video-on-Demand Applications: The proposed platform is particularly advantageous for video-on-demand services. It encrypts and streams video content across the network while dynamically protecting it using recipient credentials and device information. Additionally, program settings allow temporary local storage of generated keys and encrypted material on the destination device. This approach effectively safeguards copyright and encourages more users to subscribe to video services, ultimately boosting revenue.

REFERENCES

[1] O. El Marai, T. Taleb, M. Menacer, and M. Koudil, ‘‘On improveing video streaming efficiency, fairness, stability, and convergence time through client–server cooperation,’’ IEEE Trans. Broadcast., vol. 64, no. 1, pp. 11–25, Mar. 2018.

[2] Z.LuandI.Nam,‘‘Research on the influence of new media technology on internet short video content production under artificial intelligence background,’’ Complexity, vol. 2021, pp. 1–14, Jan. 2021. [Online]. Available: https://ideas.repec.org/a/hin/complx/8875700.html

[3] F. Loh, F. Wamser, F. Poignée, S. Geißler, and T. Hoßfeld, network ‘‘YouTube dataset on mobile streaming for internet traffic modeling, management, Sci. and streaming analysis,’’ Data, vol. 9, p.293, Apr. 2022. [Online]. Available: https://figshare.com/articles/dataset/YouTube_Dataset_on_Mobile_Streaming_for_Internet_Traffic_Modeling_Network_Management_and_ Streaming_Analysis/19096823

[4] D. Shamsimukhametov, M. Liubogoshchev, E. Khorov, and I. F. Akyildiz, ‘‘Youtube, netflix,webdatasetforencryptedtrafficclassification,’’inProc. Int. Conf. Eng. Telecommun., 2021, pp. 1–5, doi: 10.21227/s7x7-wd58.

[5] CiscoAnnualInternetReport—CiscoAnnualInternetReport(2018–2023) White Paper. Accessed: Feb. 15, 2023. [Online]. Available: https://www. cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[6] Cisco Annual Internet Report—Cisco Annual Internet Report Highlights Tool. Accessed: Feb. 15, 2023. [Online]. Available: https://www.cisco. com/c/en/us/solutions/executive-perspectives/annual-internet-report/air highlights.html

[7] A. Rao, A. Legout, Y.-S. Lim, D. Towsley, C. Barakat, and W. Dabbous, ‘‘Network characteristics of video streaming traffic,’’ in Proc. 7th Conf. Emerg. Netw. Exp. Technol., Dec. 2011, pp. 1–12.

[8] X. Huang, D. Arnold, T. Fang, and J. Saniie, ‘‘A chaotic-based encryption/decryption system for secure video transmission,’’ in Proc. IEEE Int. Conf. Electro Inf. Technol. (EIT), May 2021, pp. 369–373.

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

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308124|

[9] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.-J. Quisquater, ''Overview on selective encryption of image and video: Challenges and perspectives,'' EURASIP J. Inf. Secur., vol. 2008, pp. 1–18, Jan. 2008.
[10] A. Murtaza, S. J. H. Pirzada, and L. Jianwei, ''A new symmetric key encryption algorithm with higher performance,'' in Proc. 2nd Int. Conf. Comput., Math. Eng. Technol. (iCoMET), Jan. 2019, pp. 1–7.
[11] S. Kansal and M. Mittal, ''Performance evaluation of various symmetric encryption algorithms,'' in Proc. Int. Conf. Parallel, Distrib. Grid Comput., Dec. 2014, pp. 105–109.
[12] S. Kumar, M. S. Gaur, P. S. Sharma, and D. Munjal, ''A novel approach of symmetric key cryptography,'' in Proc. 2nd Int. Conf. Intell. Eng. Manag. (ICIEM), Apr. 2021, pp. 593–598.
[13] M. Dworkin, E. Barker, J. Nechvatal, J. Foti, L. Bassham, E. Roback, and J. Dray, ''Advanced encryption standard (AES),'' Federal Inf.
Process. Standard, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 197, 2001. Accessed: Feb. 15, 2023, doi: 10.6028/NIST.FIPS.197.
[14] Y. Shen, Z. Sun, and T. Zhou, ''Survey on asymmetric cryptography algorithms,'' in Proc. Int. Conf. Electron. Inf. Eng. Comput. Sci. (EIECS), Sep. 2021, pp. 464–469.
[15] S. Kumar, B. K. Singh, S. Pundir, S. Batra, and R. Joshi, ''A survey on symmetric and asymmetric key based image encryption,'' in Proc. 2nd Int. Conf. Data, Eng. Appl. (IDEA), Feb. 2020, pp. 1–5.
[16] R. L. Rivest, A. Shamir, and L. Adleman, ''A method for obtaining digital signatures and public-key cryptosystems,'' Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.
[17] N. Koblitz, ''Elliptic curve cryptosystems,'' Math. Comput., vol. 48, no. 177, pp. 203–209, 1987.
[18] A. J. Menezes and S. A. Vanstone, ''Elliptic curve cryptosystems and their implementation,'' J. Cryptol., vol. 6, no. 4, pp. 209–224, 1993. [Online]. Available: https://link.springer.com/article/10.1007/BF00203817
[19] N. Koblitz, A. Menezes, and S. Vanstone, ''The state of elliptic curve cryptography,'' Designs, Codes Cryptogr., vol.19,nos.2–3,pp173–193, Mar. 2000. [Online]. Available: https://link.springer.com/article/10.1023/A:1008354106356
[20] U. Zia, M. McCartney, B. Scotney, J. Martinez, and A. Sajjad, ''A novel pseudo-random number generator for IoT based on a coupled map lattice system using the generalised symmetric map,'' Social Netw. Appl. Sci., vol. 4, no. 2, pp. 1–17, Feb. 2022. [Online]. Available: https://link.springer.com/article/10.1007/s42452-021-04919-4
[21] H. Kezia and G. F. Sudha, ''Encryption of digital video based on Lorenz chaotic system,'' in Proc. 16th Int. Conf. Adv. Comput. Commun., Dec. 2008, pp. 40–45. [22] M. A. Khan, M. T. Quasim, N. S. Alghamdi, and M. Y. Khan, ''A secure framework for authentication and encryption using improved ECC for IoTbased medical sensor data,'' IEEE Access, vol. 8, pp. 52018–52027, 2020.
[23] R. Imam, Q. M. Areeb, A. Alturki, and F. Anwer, ''Systematic and critical review of RSA based public key cryptographic schemes: Past and present status,'' IEEE Access, vol. 9, pp. 155949–155976, 2021.
[24] N.Sen,R.Dantu,J.Vempati,andM.Thompson,''Performanceanalysisof elliptic curves for real-time video encryption,'' in Proc. Nat. Cyber Summit (NCS), Jun. 2018, pp. 64–71.
[25] S. C. Iyer, R. R. Sedamkar, and S. Gupta, ''A novel idea on multimedia encryption using hybrid crypto approach,'' Proc.Comput.Sci.,vol.79,pp.293–298,Jan.2016.[Online].Available:
https://www.sciencedirect.com/science/article/pii/S1877050916001691
[26] P. R. Vijayalakshmi and K. B. Raja, ''Performance analysis of RSA and ECCin identity-based authenticated new multiparty key agreement protocol,'' in Proc. Int. Conf. Comput., Commun. Appl., Feb. 2012, pp. 1–5.
[27] Z. Chen and G. Ye, ''An asymmetric image encryption scheme based on hash SHA-3, RSA and compressive sensing,'' Optik, vol. 267, Oct. 2022, Art. no. 169676. [Online]. Available:
https://www.sciencedirect.com/science/article/pii/S0030402622009627
[28] R. Hegde and S. Jagadeesha, ''An optimal modified matrix encoding technique for secret writing in MPEG video using ECC,'' Comput. Standards Interfaces, vol. 48, pp. 173–182, Nov. 2016.
[29] S. H. Murad and K. H. Rahouma, ''Implementation and performance analysis applied in of hybrid cryptographic schemes cloud computing environment,'' Proc. Comput. Sci., vol. 194, pp. 165–172, Jan. 2021. [Online]. Available:
https://www.sciencedirect.com/science/article/pii/S1877050921021116
[30] S. K. Ghosh, S. Rana, A. Pansari, J. Hazra, and S. Biswas, ''Hybrid cryptography algorithm for secure and low cost communication,'' in Proc. Int. Conf. Comput. Sci., Eng. Appl. (ICCSEA), Mar. 2020, pp. 1–5.
[31] J. Zhang and X. Gao, ''A hybrid encryption scheme for scalable video coding based on H.264,'' in Proc. 5th Int. Conf. Intell. Netw. Collaborative Syst., Sep. 2013, pp. 708–711.
[32] L. Yu, Z. Wang, and W. Wang, ''The application of hybrid encryption algorithm in software security,'' in Proc. 4th Int. Conf. Comput. Intell. Commun. Netw., Nov. 2012, pp. 762–765.

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

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308124|

[33] M. A. Khan, K. K. Mishra, N. Santhi, and J. Jayakumari, ''A new hybrid technique for data encryption,'' in Proc. Global Conf. Commun. Technol. (GCCT), Apr. 2015, pp. 925–929.

[34] C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, K. Perumal, and M. F. Ijaz, ''Analytical study of hybrid techniques for image encryption and decryption,'' Sensors, vol. 20, no. 18, p. 5162, Sep. 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/18/5162

[35] J. Dave and M. Gayathri, ''Hybrid encryption algorithm for storing unimodal biometric templates in cloud,'' in Inventive Communication and Computational Technologies, G. Ranganathan, X. Fernando, and F. Shi, Eds. Singapore: Springer, 2022, pp. 251–266.

[36] M. Hamdi, J. Miri, and B. Moalla, ''Hybrid encryption algorithm (HEA) based on chaotic system,'' Soft Comput., vol. 25, no. 3, pp. 1847–1858, Feb. 2021, doi: 10.1007/s00500-020-05258-z.

[37] P. Yu, N. Zhang, S. Zhang, and Q. Wang, ''Security mechanism of video content integrated broadcast control platform under triple play,'' in Proc. 10th Int. Congr. Image Signal Process., Biomed. Eng. Informat. (CISPBMEI), Oct. 2017, pp. 1–5.

[38] D. Zhu, J. Zheng, H. Zhou, J. Wu, N. Li, and L. Song, ''A hybrid encryption scheme for quantum secure video conferencing combined with blockchain,'' Mathematics, vol. 10, no. 17, p. 3037, Aug. 2022. [Online]. Available: https://www.mdpi.com/2227-7390/10/17/3037

[39] K. M. Hosny, M. A. Zaki, N. A. Lashin, and H. M. Hamza, ''Fast colored video encryption using block scrambling and multi-key generation,'' Vis. Comput., pp. 1–32, Nov. 2022. [Online]. Available: https://link.springer.com/article/10.1007/s00371-022-02711-y

[40] A.Alarifi,S.Sankar,T.Altameem,K.Jithin,M.Amoon,andW.El-Shafai, ''A novel hybrid cryptosystem for secure streaming of high efficiency H.265 compressed videos in IoT multimedia ap

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

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