Analysis of Hybrid Cryptography for Secure Exchange of Information

Pawan Kumar
Department of Computer Science
Babasaheb Bhimrao Ambedkar University, Lucknow, 226025
Uttar Pradesh, India

Vipin Saxena
Department of Computer Science
Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, Uttar Pradesh, India

Karm Veer Singh
Department of Computer Science
Babasaheb Bhimrao Ambedkar University, Lucknow, 226025
Uttar Pradesh, India

ABSTRACT

Due to rapid growth of digital communication in the recent days, it is important to secure the confidential information in the form of text, audio and video files from the intruders and hackers watching 365x24x7 days around the globe and well connected through high-speed internet facilities. The information which is used for communication over the network is very sensitive and must be shielded from the network attackers. In the present work, a new concept of hybrid cryptographical algorithm is explored by combining the Advance Encryption Standard (AES), Rivest, Shamir, Adleman (RSA) and Elliptic Curve Integrated Scheme (ECIES) for digital communication of information passed from one device to another device. The presented approach shall enhance the security levels at the end of sender as well also receiver. The approach is tested through the object-oriented programming language and computed results are shown in the form of figures and graphs.

Keywords

Information, AES, RSA, ECIES, Hybrid Cryptography, Encryption and Decryption

1. INTRODUCTION

The primary goal of security is to keep the information hidden from the unauthorised public and cyber attackers when it is transferred over the internet. This necessity gave rise to a variety of cryptographic primitives, such as hash functions, digital signatures, and symmetric and asymmetric cryptographical techniques. A key which is exchanged between the sender and receiver must be kept hidden so that unauthorised party could not get the same. The symmetric cipher that uses a fixed 128-bit block, shared a secret key to encrypt and decode the information over the communication channels. Three separate key lengths can be used with Advance Encryption Standard (AES), known as AES-128, AES-192, and AES-256, sequentially 128,192, 256, to denote the key's length in bits while asymmetric cryptography encrypts and decrypts the messages using a pair of keys. The first of the two keys are referred to as a public key because it is shared with everyone, while the other is referred to as the private key because it is kept private. Every message is typically encrypted using a public key, which can only be decoded with the associated secret key. Rivest, Shamir,

Adleman (RSA) algorithm has three parts, key generation, encryption and decryption. It was created in the year 1977 by Ron Rivest, Adi Shamir, and Len Adlemen as a public key encryption technique. The Elliptic Curve Integrated Scheme (ECIES) is one of the most effective elliptic curve-based encryption and decryption methods.

Further, Abdalla, Bellare, and Rogway proposed the public-key cryptosystem known as ECIES which has functions like key agreement, key derivation function and encryption/ decryption. The AES is a private key encryption algorithm, RSA is public key encryption algorithm and ECIES is hybrid cryptography algorithm. The ECIES offers features for key exchange, encryption, and digital signature all at once. In hybrid cryptography, one can merge more than one cryptography algorithm such as symmetric, asymmetric and hashing algorithms. Each type of algorithm has strength and weakness. Hybrid cryptography uses the strength of algorithm. In this proposed work, combinations of above three algorithms are well explained for enhancing the security levels over the internet. Let us explain some of the important research papers available on the hybrid cryptographical techniques. In the year 2018, Lee et al. [1] have implemented Heroku as a cloud infrastructure, and then secured the Heroku's information with AES cryptography. According to the performance evaluation, data security is achieved by AES cryptography. The data encryption process is delayed in calculation that demonstrated the bigger data sizes and obtained the result in the form of delay for longer data. Further, Patel [2] has discussed the performance and evaluation of symmetric algorithm on Blowfish, AES, and Data Encryption Standard (DES). Performance evaluations are based on how much memory and how long it takes for certain algorithms to run. The evaluation shows that DES algorithm is better than other algorithm like AES and Blowfish. According to experimental findings, Blowfish is a superior solution to AES and DES in terms of memory.

In the year 2020, Muttaqin et at. [3] have applied test on all files of various file sizes as well as on the cipher text produced through encryption process. Santoso et al. [4] have discussed the combination of two algorithms i.e. Twofish and AES. The SHA-256 algorithm key generates for AES and Twofish algorithms which is 256-bit long key. Arman et al. [5] have discussed, quick execution time and low memory in AES-128-bit version. In terms of performance, it was great improvement over the conventional AES. Hamza A. and Kumar B. [6] have discussed two symmetric algorithms like AES and DES and another asymmetric algorithm like RSA with weaknesses and strength of each algorithm.

In the year 2011, Zhou and Tang [7] have discussed encryption/decryption based on RSA algorithm and public key. In the year 2013, Padmavathi et al. [8] have implemented three encryption methods DES, AES, and RSA along with a steganographic method Least Significant Bit (LSB) substitution and compared the effectiveness of these methods based on an analysis of their stimulated times during the encryption and decryption processes. In the year 2006, Cilardo et al. [9] have discussed various factors regarding efficiency, security, speed and memory requirements at the time of execution. Martnez et al. [10] have provided a thorough introduction to ECIES and described the encryption and decryption processes as well as the list of features and unique qualities with standards. Analysis and comparison of the ECIES versions included in the publications from ANSI, IEEE, ISO/IEC, and SECG and emphasizing the important variations [11], [12]. In the year 2016, Abbas et al. [13] have implemented Elliptic curve integrated encryption scheme with the help of identity-based encryption. ECIES cryptographic method was used to discuss the various Vehicular Ad Hoc Network (VANET) security algorithm kinds and workable solutions [14].

In the year 2021, Velmurugadass et al. [16] have built a blockchain architecture that is applied in Infrastructure as a Service (IaaS) cloud for evidence gathering and authenticity preservation. User registration, login, data encryption, storage systems, tracking user actions, and data mining from the controller are the components. The results of the trial showed that the suggested system performed better in terms of response time and overall change rate. In the year 2022, Khalid et al. [17] have implemented, the innovative picture encryption method and described user identification, secrecy and secure key exchange between the sender and receiver. The users first applied Diffie-Hellman across the elliptic curve to communicate a secret parameter before passing it via Secure Hash Algorithm-256 (SHA) then employed the first 128 bits for the data's secrecy and the latter 128 bits for verification. Alkady et al. [18] have implemented a hybrid encryption technique that combined AES with Elliptic-Curve Cryptography (ECC) to offer node encryption. For verification, the XOR DUAL RSA algorithm is used, and also message digest version-5 for integrity. Further, Abbas et al. [19] have implemented hybrid cryptography alongwith use of stenography for cloud data security. For encryption, RSA and AES algorithms are used. The LSB method is used to mask the encrypted data within a picture and the SHA hashing method throughout the data validation stage. Gupta et al. [20] have implemented hybrid cryptography to protect data in web applications. In the hybrid algorithm, AES and ECC algorithms were replaced by Blowfish and RSA, respectively. For original data authentication, authors used message digest version-5 hash algorithm. Hamza et al. [21] have discussed functions of symmetric algorithm and asymmetric algorithm in terms of number of keys, encryption/decryption speed, and complexity of process, security/strength factoring primes and other functions.

2. PROPOSED WORK

Symmetric and asymmetric cryptographical techniques have some advantages and disadvantages. When a single algorithm is used then there will chance of security threats but when the concept of hybrid cryptographical techniques is used, then definitely it will decrease the security threats. So, the proposed algorithm provides more security and more reliable than the existing algorithms available in the literature. The proposed work is a combination of three cryptography algorithms. Let us first introduce the basics of the three algorithms used in the present work.

2.1 AES

AES algorithm is of three types which depends on key size and number of rounds. AES-128 represents key size of 128 and takes number of rounds as 10, AES-192 represents key size of 192 and takes number of rounds as 12 and AES-256 represents key size of 256 and takes number of rounds as 14. In each round, AES divides into four sub parts such that Sub Bytes, Shift Rows, Mix Columns and Add Round Key. In the last round, it divides into three sub parts such that Sub bytes, Shift Rows, and Add Round Key as shown below in the following figure 1.

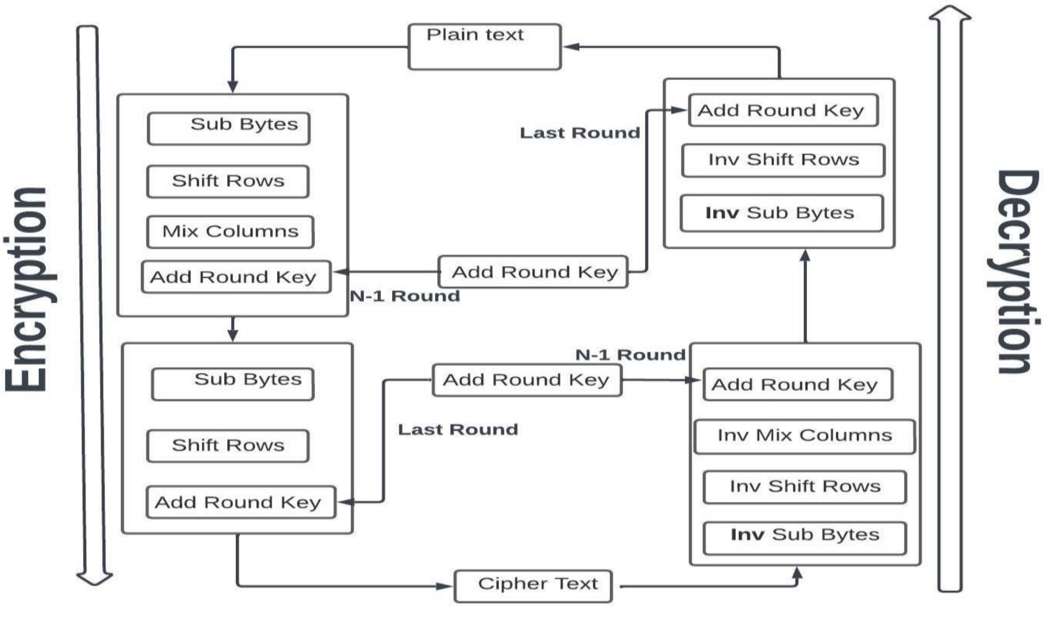


Fig. 1. Flow diagram of AES algorithm

2.2 RSA

The RSA algorithm is one of the important security algorithms based on the asymmetric keys by considering the two huge prime numbers and furthers computations are too long and due to long computations, intruders are not able to crack the algorithm. It contains three-parts like key generation, encryption and decryption described below in brief:

Key_generation()

```
Step 1. choose two distinct prime number prime_number1, prime_number2 with equal size;

Step 2. n= ( prime_nummber1 * prime_number2);
Step 3. ∅ (n)= ( prime_number1 -1) * ( prime_number2-1);
Step 4. Generate encryption key e which must be co-prime of ∅ (n) and 1 < e < $\emptyset(n)$;
Step 5. Calculate $d \cong e^{-1}(mod\emptyset(n))$;
Step 6. public_Key = (e, n);
        private_key= (d, n).
```

Encryption()

```
Step 1.  Message for encryption Message;
Step2.   The ciphertext of a message $Cipher\_text = (Message)^{e}$ mod n.
```

Decryption()

```
Step 1. Cipher Text at receiver end $Cipher\_text$;
Step 2. Message Message =$(Cipher\_text)^{d}$ mod n.
```

2.3 ECIES

ECIES generates public key and private key with random private key *pri_key* and take a point on elliptic curve as *ec_point* , then determine the public key as *pub_key*.

$$pub\_key = pri\_key * ec\_point$$

Ram sends *pub_key* to Shyam. Shyam generates *rndm_num* a large random number, then computes

$$R = rndm\_num * ec\_point$$
$$S = rndm\_num * pub\_key$$

Using key derivation function which generates symmetric key

$$Shyam\_KEY = KDF(S)$$

Message is encrypted with the help of *Shyam_KEY*

Ram receives *R* and encrypted the Message as

$$S = pri\_key * R$$
$$S = pri\_key *(rndm\_num * ec\_point)$$
$$S = rndm\_num *(pri\_key * ec\_point)$$
$$S = rndm\_num * pub\_key$$
$$Shyam\_KEY = KDF(S)$$

In the above, both sides keys are same.

2.4 Present Methodology

On the basis of above three algorithms, the combination of algorithms is given below:

```
RSA_AES_ECIES(Message)

#Key_generation()

        prime_num1, prime_num2 ← large_prime_number
        n= ( prime_num1 * prime_num2)
        ∅ (n)= ( prime_num1 -1) * ( prime_num2-1)
        Generate encryption key e which must be co-prime of ∅ (n) and 1 < e < $\emptyset(n)$
        $d \cong e^{-1}(mod\emptyset(n))$
        pub_Key = (e, n)
        priv_key= (d, n)
        Priv_key_aes = key_aes

        ecies_priv_key, Ec_point ← ECC( )

        pub_key = pri_key * ec_point

#Encryption()

        RSA_encryption , AES_encryption,
        ECIES_encryption ← (Message/3)

        rndm_num ← gen_random_number

        R= rndm_num * ec_point

        S= rndm_num * pub_key
        Sender_ECIES_Key=KDF(S)

        RSA_Cipher ← $ENC_{RSA,\ pub\_Key}$(RSA_encryption)

        AES_Cipher ← $ENC_{AES,Pri\_key\_aes}$(AES_encryption,)

        ECIES_Cipher ← $ENC_{ECIES,\ Sender\_ECIES\_Key}$(ECIES_encryption)

#Decryption()

        S= pri_key * R
        S= pri_key *( rndm_num * ec_point )
        S= rndm_num *( pri_key * ec_point )
        S= rndm_num * pub_key
        Receiver_ECIES_Key= KDF(S)

        IF (Receiver_ECIES_Key == Sender_ECIES_Key)

                RSA_Message ← $DEC_{RSA,\ priv\_Key}$(RSA_Cipher)

                AES_ Message ← $DEC_{AES,Pri\_key\_aes}$(AES_Cipher

                ECIES_ Message ← $DEC_{ECIES,\ Receiver\_ECIES\_Key}$(ECIES_Cipher)

                Original_Message= RSA_Message+
                AES_ Message + ECIES_ Message

        Else

                Failed( )
```

For the use of above algorithm, the message is divided into three parts and in each part is encrypted in hybrid mode and thereafter cipher text is floated over the network and it is represented below in the figure 2.

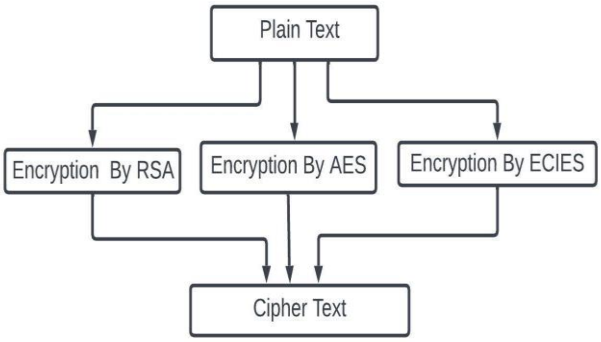


Fig. 2. Encryption of plain text by hybrid cryptography

Further, the decryption is also shown below in the figure 3 in which each part of cipher text is decrypted through decryption keys through hybrid decryption and later on all the plain texts are combined to get the original message.

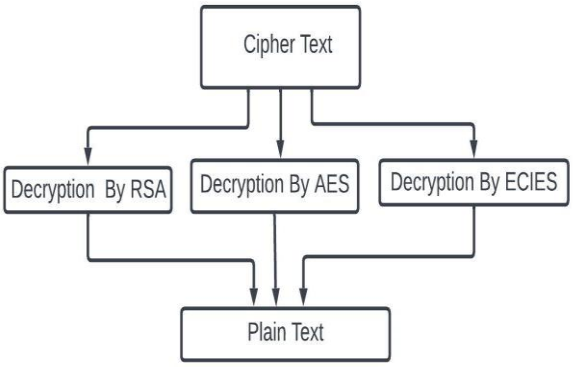


Fig. 3. Decryption of cipher text by hybrid cryptography

3. RESULTS AND DISCUSSION

The above concept is tested through python programming language by considering the various parameters. It is tested by considering the average of three run time and performance is evaluated through execution time computed in milliseconds. The computed results are shown below in the table 1 in which first column represents the size of transfer message in Kilobytes, the second column represents time in milliseconds through ECIES algorithm while the third column represents the time in milliseconds for the hybrid cryptography algorithm. The same results are also depicted in the figure 4.

Table 1. Performance evaluation of ECIES and proposed work (in milliseconds)

Size (in KB)	**ECIES**	**Proposed Work**
1	99.40775235	98.22924932
2	100.2163887	99.67796008
3	104.4425964	103.0866305
4	106.4364115	104.4103305
5	108.6775462	105.1533222
6	110.6043657	107.4786981
7	111.1205419	108.6012522
8	108.0915133	101.6322772
9	107.9964638	105.9719721
10	209.5348835	108.9668274
20	219.5947965	127.4317106
40	245.9483941	143.5027917
80	263.7557983	187.9731814
160	339.5132224	238.5372321
320	505.0186316	405.1672618

In the following figure 4, comparison between ECIES represented through blue dots and the proposed technique represented through green dots, is shown and it is observed that the security level of the proposed technique is much better than the algorithms available in the literature and the presented technique is compared with ECIES and observed that the computation time of the presented approach to transmit the information started from 1 kb to 320 kb is much lesser than the ECIES as depicted in the table and also in the figure 4.

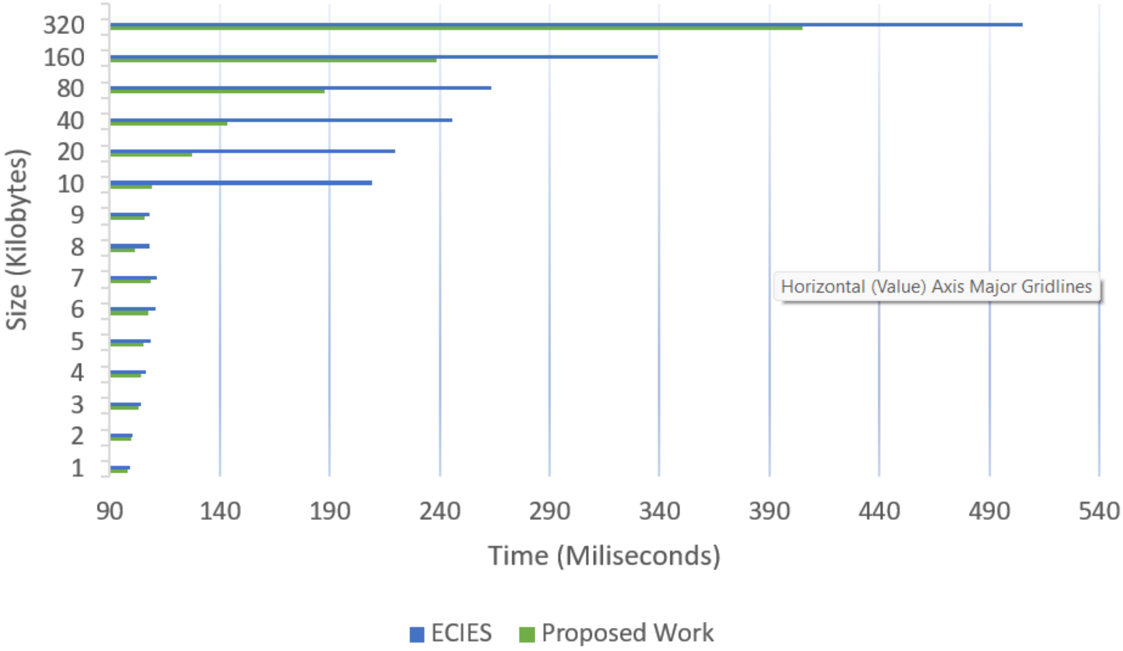
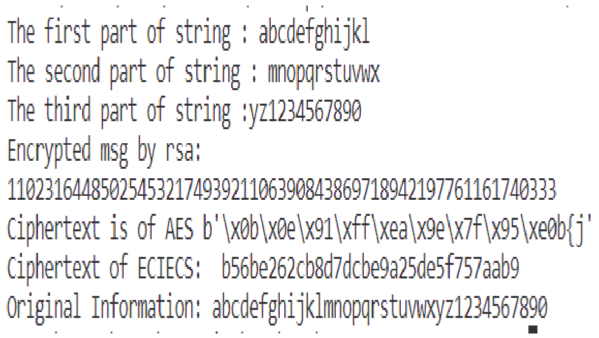


Fig. 4. Time complexity of ECIES versus present method



```
The first part of string : abcdefghijkl
The second part of string : mnopqrstuvwx
The third part of string :yz1234567890
Encrypted msg by rsa:
110231644850254532174939211063908438697189421977611617403333
Ciphertext is of AES b'\x0b\x0e\x91\xff\xea\x9e\x7f\x95\xe0b{j'
Ciphertext of ECIECS:  b56be262cb8d7dcbe9a25de5f757aab9
Original Information: abcdefghijklmnopqrstuvwxyz1234567890
```

Fig. 5. Encryption and decryption through hybrid cryptography

The above figure 5 shows that the original information is "***abcdefghijklmnopqrstuvwxyz1234567890***" which is divided into three sub parts, the first part is *abcdefghijkl*, second is *mnopqrstuvwx* and third part is *yz1234567890*. First part is encrypted by RSA, second part is encrypted by AES and third part is encrypted by ECIES and the cipher texts are sent over the internet. At the receiver side, these cipher texts are decrypted in the similar manner and further complete plain text is received after combining all the three parts.

4. CONCLUSIONS AND FUTURE SCOPE

From the above work, it is concluded that as per digital communication is increasing day by day, hence there is need of the various security levels to keep the information safe from the intruders. In the present method, three combinations of the algorithms are proposed by considering AES, RSA and ECIES which can be applied over the various parts of the information transmitted between two linked devices that are interacting via internet. The combination of symmetric, asymmetric and integrated encryption schemes makes the system more reliable and robust and even when the time complexity of the presented approach is compared with ECIES, then observed that the time complexity of the present approach is much lesser than the ECIES. The present approach can be further extended by taking combinations of the various kinds of cryptographical techniques available in the literature. In future, the proposed method may be used for multimedia data such that containing images, audio's and video's.

5. REFERENCES

[1] Lee, B. H., Dewi, E. K. and Wajdi, M. F. (2018, April), Data Security in Cloud Computing Using AES Under HEROKU Cloud, In *2018 27th Wireless and Optical Communication Conference (WOCC)*, pp. 1-5, IEEE, **DOI:** 10.1109/WOCC.2018.8372705

[2] Patel, K. (2019), Performance Analysis of AES, DES and Blowfish Cryptographic Algorithms on Small and Large Data Files, *International Journal of Information Technology*, Vol. 11, pp. 813-819. https://doi.org/10.1007/s41870-018-0271-4

[3] Muttaqin, K. and Rahmadoni, J. (2020), Analysis and Design of File Security System AES (Advanced Encryption Standard) Cryptography Based, *Journal of Applied Engineering and Technological Science (JAETS)*, Vol. 1, No. 2, pp. 113-123. https://journal.yrpipku.com/index.php/jaets/article/view/78

[4] Santoso, K. I., Muin, M. A. and Mahmudi, M. A. (2020, April), Implementation of AES Cryptography and Twofish Hybrid Algorithms for Cloud, In *Journal of Physics: Conference Series*, Vol. 1517, No. 1, pp. 012099, IOP Publishing. doi:10.1088/1742-6596/1517/1/012099

[5] Arman, S., Rehnuma, T. and Rahman, M. (2020), Design and Implementation of a Modified AES Cryptography with Fast Key Generation Technique. In *2020 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE)* pp. 191-195, **DOI:** 10.1109/WIECON-ECE52138.2020.9397992

[6] Hamza, A. and Kumar, B. (2020, December), A Review Paper On DES, AES, RSA Encryption Standards, In *2020 9th International Conference System Modelling and Advancement in Research Trends (SMART)*, pp. 333-338, IEEE, **DOI:** 10.1109/SMART50582.2020.9336800

[7] Zhou, X. and Tang, X. (2011, August), Research and Implementation of RSA Algorithm for Encryption and Decryption, In *Proceedings of 2011 6th International Forum on Strategic Technology*, Vol. 2, pp. 1118-1121, IEEE. **DOI:** 10.1109/IFOST.2011.6021216

[8] Padmavathi, B. and Kumari, S. R. (2013), A Survey on Performance Analysis of DES, AES and RSA Algorithm Along with LSB Substitution, *International Journal of Science and Research, India*, *2*, 2319-7064. http://www.ijsr.net/archive/v2i4/IJSRON120134.pdf

[9] Cilardo, A., Coppolino, L., Mazzocca, N. and Romano, L. (2006), Elliptic Curve Cryptography Engineering, *Proceedings of the IEEE*, Vol. *94*, No. 2, pp. 395-406, **DOI:** 10.1109/JPROC.2005.862438

[10] Martínez, V. G., Encinas, L. H. and Ávila, C. S., (2010), A Survey of The Elliptic Curve Integrated Encryption Scheme, *Journal of Computer Science and Engineering, Vol.* 2, No.2, pp. 7-13 http://hdl.handle.net/10261/32671

[11] Martínez, V. G. and Encinas, L. H. (2010, August), A Comparison of The Standardized Versions of ECIES, In *2010 Sixth International Conference on Information Assurance and Security* (pp. 1-4), IEEE, **DOI** 10.1109/ISIAS.2010.5604194

[12] Martínez, V. G., Encinas, L. H. and Dios, A. Q. (2015), Security and Practical Considerations When Implementing the Elliptic Curve Integrated Encryption Scheme, *Cryptologia*, Vol.*39*, *No*.3, pp. 244-269, https://doi.org/10.1080/01611194.2014.988363

[13] Abbas, S. A. and Maryoosh, A. A. B. (2016), Data Security for Cloud Computing Based on Elliptic Curve Integrated Encryption Scheme (ECIES) and Modified Identity Based Cryptography (MIBC), *International Journal of Applied Information Systems (IJAIS)*, Vol. *10*, *No*.6, pp. 7-13, https://www.ijais.org/research/volume10/number6/abbas-2016-ijais-451517.pdf

[14] Patel, P., Patel, R. and Patel, N. (2016), Integrated ECC and Blowfish for Smartphone Security, *Procedia Computer Science*, Vol. *78*, pp. 210-216. https://doi.org/10.1016/j.procs.2016.02.035

[15] Balamurugan, E. (2016), Elliptic Curve Integrated Encryption Scheme Using Analysis Vehicular Ad-Hoc Network, *International Journal of Innovations in Scientific and Engineering Research (IJISER)*, Vol.*3*,

No.5, pp. 47-50. http://www.ijiser.com/paper/2016/vol3issue5/May2016p101.1.pdf

[16] Velmurugadass, P., Dhanasekaran, S., Anand, S. S. and Vasudevan, V. (2021), Enhancing Blockchain Security in Cloud Computing with IoT Environment Using ECIES and Cryptography Hash Algorithm. *Materials Today: Proceedings*, Vol. *37*, pp.2653-2659, https://doi.org/10.1016/j.matpr.2020.08.519.

[17] Khalid, I., Shah, T., Eldin, S. M., Shah, D., Asif, M. and Saddique, I. (2022), An Integrated Image Encryption Scheme Based on Elliptic Curve, *IEEE Access*, doi: 10.1109/ACCESS.2022.3230096.

[18] Alkady, Y., Habib, M. I. and Rizk, R. Y. (2013, December), A New Security Protocol Using Hybrid Cryptography Algorithms, In *2013 9th International Computer Engineering Conference (ICENCO)*, pp. 109-115, IEEE, doi: 10.1109/ICENCO.2013.6736485.

[19] Abbas, M. S., Mahdi, S. S. and Hussien, S. A. (2020, April), Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography, In *2020 International Conference on Computer Science and Software Engineering (CSASE)* (pp. 123-127), IEEE, doi: 10.1109/CSASE48920.2020.9142072.

[20] Gupta, N. and Kapoor, V. (2020), Hybrid Cryptographic Technique to Secure Data in Web Application, *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 23, No.1, pp. 125-135, https://doi.org/10.1080/09720529.2020.1721872

[21] A. Hamza and B. Kumar, "A Review Paper on DES, AES, RSA Encryption Standards," *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, Moradabad, India, 2020, pp. 333-338, doi: 10.1109/SMART50582.2020.9336800.

6. AUTHOR'S PROFILES

Pawan Kumar received Post Graduate Degree in Computer Application (M.C.A.) and Master of Technology (M.Tech) from Babasaheb Bhimrao Ambedkar University, Lucknow, India in respectively 2016 and 2018. Currently research scholar in the Department of Computer Science, Babasaheb Bhimrao Ambedkar University. He is solving the research problems related to security of cloud data and data security in the Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow, Utter Pradesh, India under fellowship program of University Grant Commission (UGC), New Delhi.

Prof. Vipin Saxena received his Ph.D. degree from Indian Institute of Technology, Roorkee, Uttarakhand, India. Presently, he is working as Professor in Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow, India. He has published more than 190 research articles in the International and National Journals and Conferences, authored 05 books in the field of Computer Science and Scientific Computing, attended 55 International and National Conferences and received three National Awards for meritorious research work in the field of Computer Science and other details are available on www.profvipinsaxena.com. His research interests are Scientific Computing, Computer Networking and Software Engineering.

Karm Veer Singh received his Ph.D. degree from Indian Institute of Technology (BHU), Varanasi, India. He is working as Assistant Professor in Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow, India. His research interests include Multimedia Information Retrieval, Pattern Recognition, Mathematical Modeling, Data Science, Medical Imaging, Quantum Neural Networks, Reliability, Cyber Security and Artificial Intelligence.