iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59335

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

Design of a Hybrid Security Protocol based on Cryptographic Algorithms

Bhanu Sankhyan[1], Anupam Baliyan[2], Abhishek Kumar[3]
[1]*Research Scholar,* [2]*Additional Director,* [3]*Assistant Director, Computer Science and Engineering Chandigarh University Punjab, India*

Abstract: ***With increase in the use of the internet, the need to secure data is also increased. The present symmetric and asymmetric algorithms provide secure systems, but with many limitations. In the emerging world need for rapid accessing the data is increasing, a blend of both efficiency and security is required to cater the day-to-day needs. To ensure efficiency and security of the message hybrid security protocols are developed. Hybrid security protocol combines the advantages of traditional algorithms, such that more secure and efficient systems can be developed. A new hybrid protocol is developed using AES, ECC and ECDH, which in terms increase efficiency of existing protocols and provide a better security by adding an extra layer of security to the traditional AES algorithm.***

Index Terms: Advanced Encryption Standard, Elliptical Curve Cryptography, Elliptical Curve Diffie Hellman, Cryptography, Security, Efficiency

I. INTRODUCTION

Cryptography is an essential part for securing communications over the network. Cryptographic algorithms are used to encrypt and decrypt data. Data encryption and decryption is done on the sender and receiver's end respectively, such that the message can be only accessed by sender and receiver. Cryptographic algorithms are used in combination with keys. The security of a protocol depends on two main factors one is the complexity of the algorithm, how hard is it to break the algorithm and other is secrecy of the key [1]. Cryptographic algorithms are defined to cover four basic principles, which are defined as follows.

1) *Confidentiality:* Confidentiality ensures that information is restricted and cannot be accessed.
2) *Data Integrity:* This principle states that data transferred should be consistent and cannot be tampered or exchanged with other data.
3) *Authentication:* It makes sure that data is claimed by the only user to which it belongs.
4) *Non-repudiation:* It makes sure that the person associated with the data cannot contest the authenticity of sending the message.

Some of the problem arises in the cryptographic algorithms are efficiency and security. It is main the aspect of an algorithm to provide security. With the advancement in technologies, algorithms are being compromised. Thus, more secure and secure algorithms are being developed. With the increase in security algorithms are becoming more complex, which in result uses more resources and decreases efficiency. Therefore, it is important to consider security along with efficiency.

Encryption is the process of protecting information using a mathematical function which is considered an encryption algorithm. A key to alter the plain text into cipher text using an encryption algorithm. Cryptography can be further classified into two parts.

Symmetric key cryptography uses the same secret key in the process of encryption and decryption. Security of symmetric key algorithms depends on key length, algorithmic design. In symmetric key algorithm keys are comparatively short and uses less computational power. Hence much more efficient than asymmetric cryptography methods. Same key is used for encryption and decryption, thus making it difficult to distribute keys among the users.

Asymmetric key cryptography requires a pair of private and public keys in the process of encryption and decryption. In public key encryption, plain text is converted into cipher text using private key and cipher text is converted into plain text using public key or vice-versa. Private key is known to sender and the public key is distributed over the network. The security of these methods lies on the mathematical functions called as the trapdoor functions. These functions are impossible to re- verse for sufficiently large values. Thus, making it impossible to crack the algorithms. [3]

To overcome the limitations of traditional algorithms, hybrid security protocols are developed. More secure, robust and efficient protocols are developed using traditional algorithms. A variety of algorithms are used such that these protocols can combine the advantages of different algorithms.

II. RELATED WORK

Manali J Dubal et al. (2011)[5] proposed a protocol as shown in figure 2.2, developed using ECC, ECDH, Dual- RSA, ECDSA and MD5. Elliptical Curve Cryptography is used to generate keys and Elliptical Curve Diffie Hellman is used to distribute the keys between sender and receiver over the network. Dual-RSA takes the key and plain-text such that cipher-text can be generated. A signature is appended to cipher-text generated using ECDSA. ECDSA servers the purpose of authentication in the protocol. ECDSA certificates are generated and sent along the network and the authentication of the message is verified at the receiver's end. In the final step decryption is done using dual RSA and plaintext is derived. This protocol has some limitations such as, use of two asymmetric algorithms dual RSA and ECC, which lacks speed as compared to symmetric key algorithms. If the private key is compromised, attacker can read the message that is being transmitted.

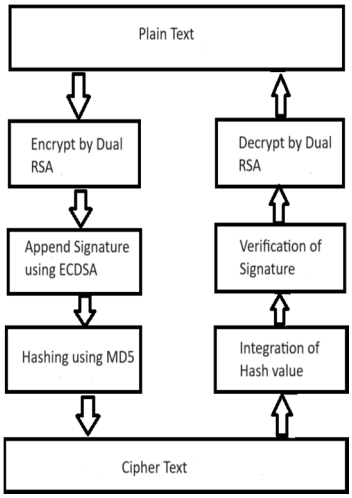


Fig. 1: Dubal Security Protocol Architecture

Sandeep Kumar Namini (2012)[6] proposed a protocol as shown in figure 2.3, which is developed using Advanced Encryption Scheme and Elliptical Curve Cryptography. In this protocol hash value of the message is evaluated using MD5 algorithm. AES and ECC are used to encrypt the plaintext and ciphertext generated is sent over the network. At the receiver's end cipher-text is decrypted using AES, ECC and the hash value of plain-text is calculated and compared with hash received, to check the data integrity. The execution time of the protocol is large due to sequential use of both AES and ECC.

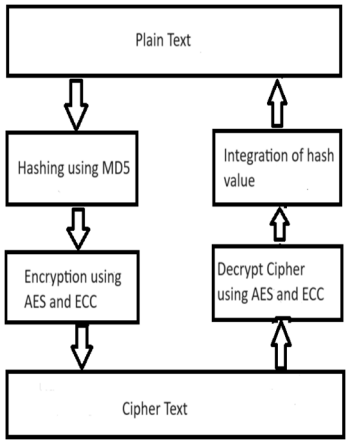


Fig. 2: Kumar Protocol Architecture

Wuling Ren et al (2010)[7] proposes a protocol as shown in fig. 2.4, developed using DES and RSA. Initially, plain- text is encrypted using DES and key used for encryption is encrypted using RSA and sent over the network. RSA is used to compute the key for decryption at the receiver's end and plaintext is evaluated using DES algorithm. This algorithm has a limitation of key management and if key gets exposed whole security is compromised.

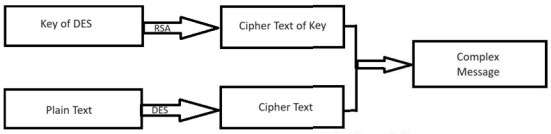


Fig. 3: Ren Protocol Architecture

Sci Hai Zhu (2011)[8] proposed protocol is shown in Fig. 2.5, Zhu's protocol is developed using AES, ECC and digital signature to achieve data confidentiality, integrity and authentication as demonstrated in "Fig. 5". Plaintext is encrypted using AES and cipher of digital signature is computed using ECC. The key used in AES is encrypted using the public key shared by receiver. These are combined to form ciphertext. The ciphertext is sent along the network. Key of AES is decrypted using the private key of receiver and the plain-text is obtained by decryption performed using AES. Public key of sender is used to decipher signature, which in result used to ensure authentication of the sender. The discussed protocol lacks security as it is encrypted using single layer encryption of the AES.

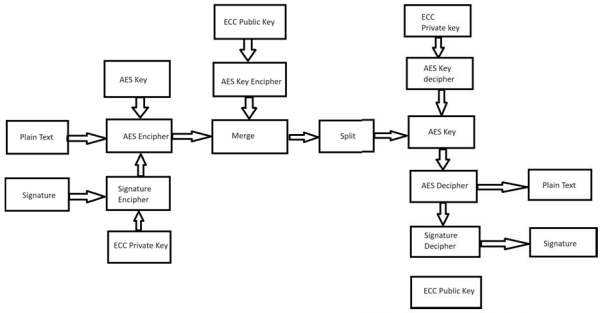


Fig. 4: Zhu Protocol Architecture

Yasmin Alkady et al. (2013)[10] proposed protocol as shown in Fig. 2.6. This protocol uses AES, ECC XOR Dual RSA and MD5. Plaintext is divided into two equal sized blocks for encryption. Key is generated using ECC and AES is used to encrypt the first block of code. Sequentially second block of plaintext is converted into ciphertext using XOR Dual RSA. Hash values for both are calculated using MD5 and appended with final cipher-text. In the decryption phase, hash value is compared with received cipher-text, if the value matches the message is accepted otherwise dropped. Cipher-text is split into two halves and decrypted by utilizing AES, ECC and XOR Dual RSA to obtain the plain-text. The proposed algorithm requires heavy mathematical computations, thus has more execution time.

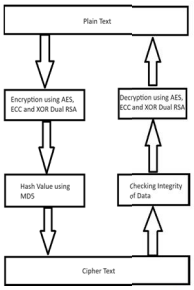


Fig. 5: Yasmin Protocol Architecture

Khalid M. Abdullah et al. (2018) [9] proposed a protocol as shown in Fig. 2.7, Hybrid Cryptography Algorithm developed using AES, RSA, LZW compression and modification of algorithm. This algorithm is based on conversion of plain text into two sub parts and both parts are encrypted using AES and RSA. The messages encrypted are compressed using LZW compression. Further another layer of security is added by applying an algorithm on previously encrypted data and ap- pended to cipher-text. Simultaneously, key in encrypted using RSA and added to cipher-text. At the receiver's end cipher- text is divided into two parts, to obtain key and the cipher text. Thus, decrypting the cipher-text using key, following the encryption process algorithm in reverse order. Finally, decrypting the obtained text using AES and RSA to obtain plain-text. This protocol has a limitation of using the asymmetric key algorithm, which involves heavy mathematical calculations, thus increasing time of encryption and decryption.

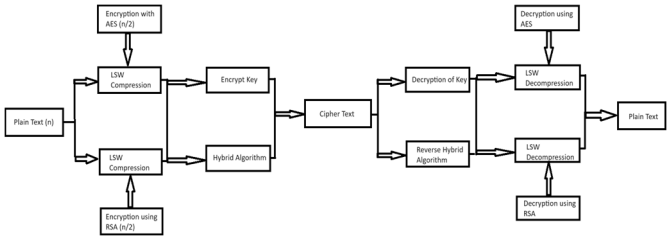


Fig. 6: Khalid Protocol Architecture

III. RESEARCH FINDINGS

All the previously developed protocols are analyzed and their limitations are discussed based on efficiency and security. Efficiency of the discussed protocols is backed by the experimental results obtained from encryption and decryption performed using different protocols. Security of protocols is determined using type of algorithms used to develop protocol, ciphertext length. The major findings are represented in a tabular form discussed in TABLE I.

TABLE I: Research Findings

Title of Paper with Author details and year of publication	Algorithms Used	Major Findings
Design of a new security protocol using hybrid cryptography algorithms by S. Subhasree and N.K. Sakthivel(2010)	ECC, Dual RSA and MD5	The proposed uses two asymmetric key algorithms and not considered efficient. The security of the protocol is compromised if the key is exposed.
A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication by Wuling Ren, Zhiqian Miao(2010)	ECC, ECDH, Dual RSA, ECDSA and MD5.	The proposed protocol in the study lacks speed as it uses various asymmetric techniques to encrypt the data.
Design of a new security protocol using hybrid cryptography architecture by M.J. Dubal, Mahesh T.R., Pinaki A Ghosh(2011)	ECC, ECDH, Dual RSA, ECDSA and MD5.	This protocol lacks security as it is encrypted using single layer of encryption.
Research of Hybrid Cipher Algorithm Application to Hydraulic Information Transmission by Shi-hai Zhu(2011)	AES, ECC and ECDSA.	The proposed protocol lacks security as it is encrypted using single layer of encryption.
A New Security Protocol Using Hybrid Cryptography Algorithms by Yasmin Alkady, Mohmed I. Habib, Rawya Y. Rizk(2013)	AES, ECC XOR Dual RSA and MD5.	The research work lacks efficiency due use of algorithms which leads to heavy mathematical calculations.
New Security Protocol using Hybrid Cryptography Algorithm for WSN by Khalid M. Abdullah, Essam H. Houssein and Hala H. Zayed(2018)	AES, RSA and LZW compression.	Proposed protocol uses RSA, which uses heavy mathematical calculations, thus decreasing efficiency of the algorithm.

IV. PROPOSED HYBRID SECURITY PROTOCOL

"Fig. 7" shows the proposed protocol, developed using AES, ECC and ECDH. In this algorithm ECC is used to generate efficient keys and ECDH is used to transfer the keys over the network securely. AES is modified by adding a second encryption layer and insertion of plain text with random text followed by base64 encoding. In the proposed protocol insertions are appended to the plain text and encrypted with the encoding method. In the next step this text is passed to AES algorithm for encryption. AES uses key generated using ECC. At the receiver's end data is decrypted using AES and second encryption layer is decrypted, such that insertion of text can be removed.

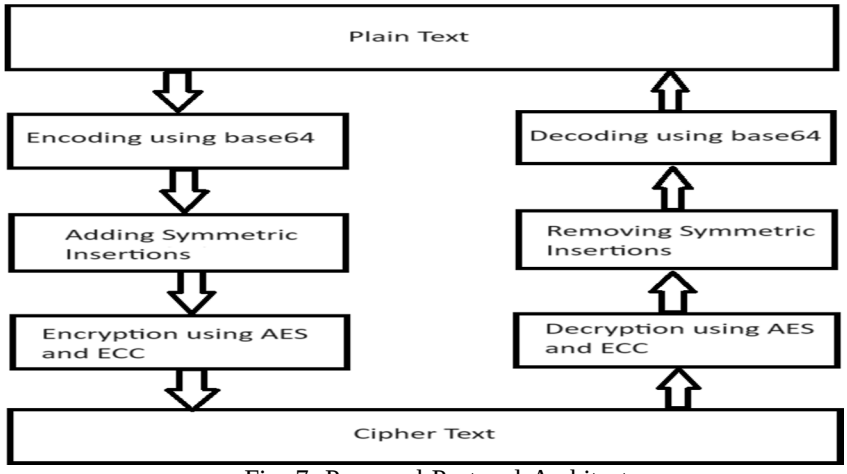


Fig. 7: Proposed Protocol Architecture

A. Encryption process

AES is used for encryption process. AES uses a key of three different sizes, determining the security of the algorithm. AES is one of the most secure symmetric algorithm known till date, which is only vulnerable to handful of attacks such as brute-force attack, side channel attacks, know key attack.

[12] A new layer of encryption is used with AES, such that AES is not vulnerable to traditional attacks. Elliptical Curve Cryptography is used to generate keys for AES. ECC generate keys in efficient and secure manner. ECC uses a one-way trapdoor function to generate keys, which is hard to reverse thus, providing secure keys and have less computational overhead than RSA algorithm. [11] ECC generates keys using mathematical function of polynomial equation of the form

$$y^2 = x^3 + ax + b$$

Point multiplication, doubling or adding is used to generate keys using ECC. [13] These keys are distributed over the network using ECDH termed as shared secret keys. Encryption process can be discussed below:

I: Get the generator point (G) for the brainpool curve having prime field 256.

II: Compute a random number K_a, K_b private key for user *A* and *B*.

III: Compute a point on curve $P = K_a*G$, public key for user A.

IV: Similarly compute Point for second user $P = K_b*G$, public key for user *B*.

V: Public keys of both users are shared and multiplied with their respective private keys to obtain the secret key for encryption and decryption, which will be

$$Secert_a = Secret_b = K_a*K_b*G.$$

VI: Plaintext is encoded using base64 encoding method.

VII: After every 4th element four random insertions are made having ASCII value from 33 to 127.

VIII: The text is passed to AES along with the shared secret key and encryption is performed and ciphertext is obtained.

B. Decryption process

Decryption of the cipher-text is done in the reverse order which can be shown in the algorithm below:

I: Cipher-text obtained is passed to the AES along with the shared secret key.

II: Random insertions are removed from the text obtained from the previous step.

III: Text is decoded using base64 decoding method. IV: Plaintext is obtained.

C. Strength of Proposed Protocol

The algorithm proposed uses both symmetric and asymmetric algorithms ECC and AES followed by base64 encoding and random insertions of text to add an extra layer of security to the traditional AES algorithm. Secure and Efficient keys are generated using ECC, the plain text is encoded using base64 and encrypted using AES. This protocol combines both symmetric and asymmetric algorithms, such that a balance of speed and security can be maintained. Symmetric algorithms are faster and asymmetric algorithm are much more secure as they require heavy mathematical calculations and depends on the trapdoor functions. This protocol overcomes the limitation of traditional attacks on AES such as side channel attacks, brute force attacks and known key attack. [12]

V. RESULTS

A. Cipher Text

As shown in TABLE II the size of the cipher text generated after encryption of the data. As shown in the table proposed protocol has cipher text is longer as compared to other proto- cols. The length of cipher-text generally dictates the security of the algorithm, as it makes difficult to remove extra-padded bits. Thus, the proposed algorithm is more secure and improves the securities lies in the traditional algorithms.

B. Encryption and Decryption Time

The time taken by an algorithm to convert the plain-text into cipher-text is considered encryption time. Similarly, decryption time is described as time required to convert cipher-text into plain-text. TABLE III and TABLE IV shows encryption and decryption time respectively. Proposed hybrid protocol is considered as the fastest algorithm as it takes less time for both encryption and decryption processes.

C. Throughput

TABLE V shows throughput calculated for each algorithm for different text sizes. Throughput helps us determine the efficiency of the algorithm. In other terms throughput, is defined as encryption of bytes per millisecond. Throughput can be calculated using

$$\text{Throughput} = T_p \text{ (bytes)} / E_t \text{ (ms)}$$

where size of the plaintext in bytes is denoted by T_p and time taken to encrypt the message in milliseconds is denoted by E_t. Table 4 shows throughput of the existing protocols, proposed hybrid protocol has the fastest encryption speed as they have higher throughput value. The proposed hybrid protocol have highest throughput value and hence is considered most efficient algorithm among all the algorithms. [10]

TABLE II: Size of Ciphertext

Plain Text (bytes)	Dubal Protocol	Kumar Protocol	Ren Protocol	Zhu Protocol	Khalid Protocol	Proposed Protocol
609	673	846	602	609	648	1632
25615	25645	35142	25610	25647	25647	68320
35080	35192	48226	35070	35080	35116	93568
61386	61486	84340	61369	61386	61421	163712
184162	184262	253008	184143	184162	184201	491120

TABLE III: Encryption Time(ms)

Plain Text (bytes)	Dubal Protocol	Kumar Protocol	Ren Protocol	Zhu Protocol	Khalid Protocol	Proposed Protocol
609	2032	1500	1432	998	548	277
25615	6305	1518	1490	1022	990	401
35080	6805	1526	1468	1059	1037	438
61386	7203	3019	3143	2345	2345	697
184162	8904	5752	4970	3814	3187	1139

TABLE IV: Decryption Time(ms)

Plain Text (bytes)	Dubal Protocol	Kumar Protocol	Ren Protocol	Zhu Protocol	Khalid Protocol	Proposed Protocol
609	1016	966	756	562	221	269
25615	4053	972	821	713	636	309
35080	4897	980	953	824	762	310
61386	5134	991	864	891	795	345
184162	6478	1099	1075	907	856	490

TABLE V: Throughput

Plain Text (bytes)	Dubal Protocol	Kumar Protocol	Ren Protocol	Zhu Protocol	Khalid Protocol	Proposed Protocol
609	.29	.40	.42	.61	1.1	2.1
25615	4	6.8	17.1	12	25.8	63.7
35080	2.2	22.9	23.8	33.1	33.8	80
61386	8.5	14.5	20.3	19.5	26.1	87.9
184162	20.6	32	37	48.2	57.7	161.6

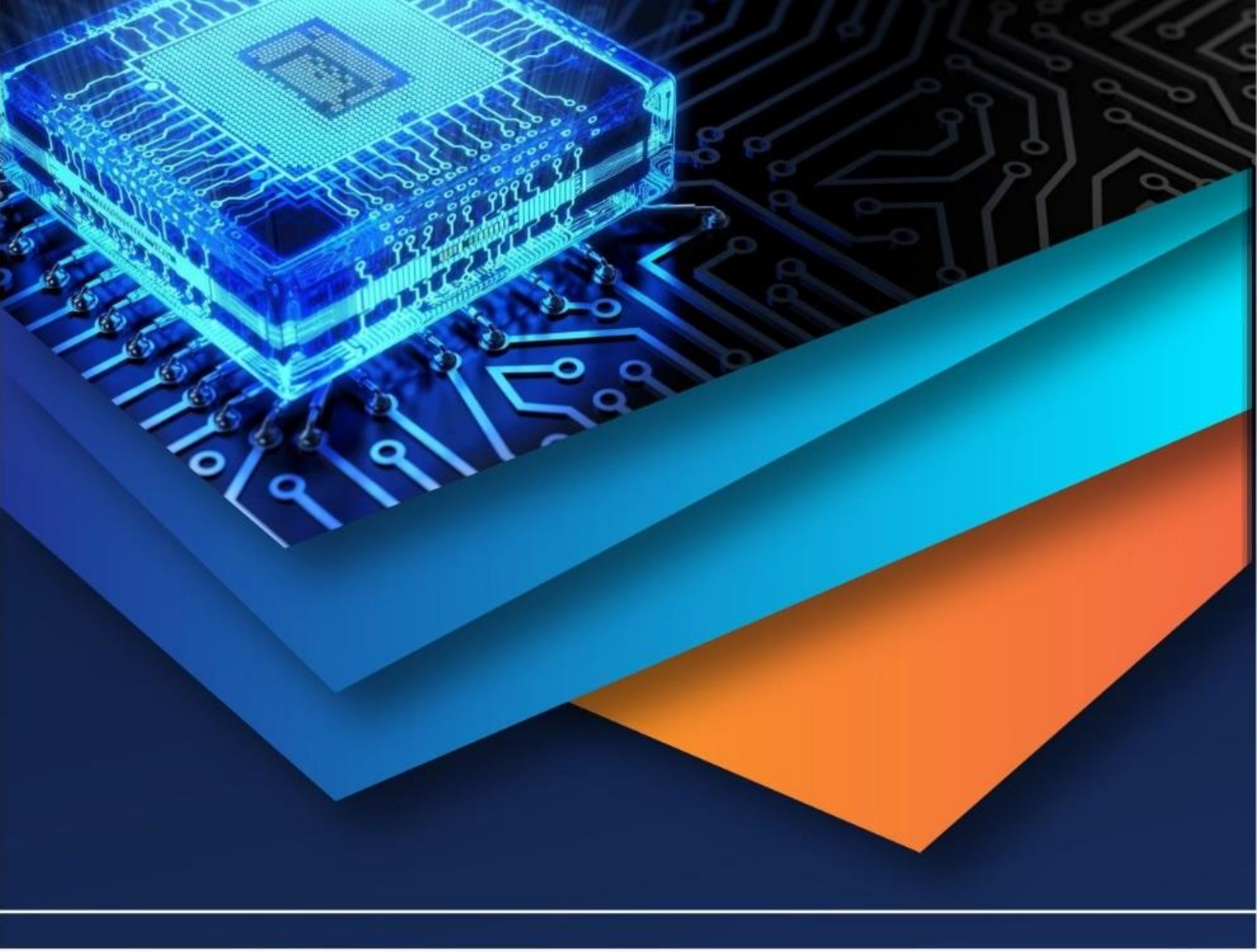
VI. CONCLUSION

Various hybrid security protocols are analyzed and com- pared based on efficiency and security. These protocols are being developed to solve the problems like large response time, efficiency, security and larger computational overhead. According to the analysis performed proposed protocol is more secure than other protocols as it uses both AES and ECC followed by the second layer of encryption and plain text manipulation to encrypt the message. Experimental research is conducted to analyze the efficiency of the protocols, which points that proposed protocol achieved better results than previously developed protocols. Thus, it can be stated that proposed protocol has the highest encryption speed among other protocols and is considered as most secure and efficient among other protocols.

REFERENCES

[1] Stony Brook University, “An Introduction to Cryptography,” pp. 11-13, 2000.
[2] Q. M. Shallal, M. U. Bokhari, “A Review on Symmetric Key Encryp- tion Techniques in Cryptography”, International Journal of Computer Applications pp. 43-47 , 2016.
[3] J. N. Gaithuru, M. Bakhtiari, M. Salleh and A. M. Muteb “A Comprehen- sive Literature Review of Asymmetric Key Cryptography Algorithms for Establishment of the Existing Gap”, 9th Malaysian Software Engineering Conference, 2015, pp. 236–239.
[4] S. Subasree and N. K. Sakthivel, “DESIGN OF A NEW SECURITY PROTOCOL USING HYBRID CRYPTOGRAPHY ALGORITHMS”,International Journal of Recent Research and Applied Studies, 2010,pp. 95-102.
[5] Manali J Dubal, Mahesh T R, Pinaki A Ghosh, “DESIGN OF NEW SECURITY ALGORITHM USING HYBRID CRYPTOGRAPHY AR-CHITECTURE ” International Conference on Electronics Computer Technology, 2011, pp. 99-101.
[6] N. Kumar, “A secure communication wireless sensor networks through hybrid (aes+ecc) algorithm”, LAP Lambert Academic Publishing, vol. 386, 2012.
[7] Wuling Ren, Zhiqian Miao “A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication”, Second International Conference on Modeling, Simulation and Visualization Methods, 2010.
[8] Shi-hai Zhu “Research of hybrid cipher algorithm application to hy- draulic information transmission”, In Proceedings of International Con- ference on Electronics, Communications and Control (ICECC), 2011.
[9] Khalid M. Abdullah, Essam H. Houssein and Hala H. Zayed “New secu- rity protocol using hybrid cryptography algorithm for wsn”, International Conference on Computer Applications Information Security(ICCAIS), 2018.
[10] Yasmin Alkady, Mohmed I. Habib, Rawya Y. Rizk, “A New Security Protocol Using Hybrid Cryptography Algorithms”, International Com- puter Engineering Conference(ICENCO), 2013.
[11] N. Sullivan, “A (Relatively Easy To Understand) Primer on Ellip- tic Curve Cryptography”, https://blog.cloudflare.com/a-relatively-easy- to-understand-primer-on-elliptic-curve-cryptography, 2013

[12] J. Kaur, S.Lamba and P. Saini, " Advanced encryption standard: Attacks and current research trends", International Conference on Advance Computing and Innovative Technologies in Engineering, 2021.
[13] N. Sullivan, "A (Relatively Easy To Understand) Primer on Ellip- tic Curve Cryptography", https://blog.cloudflare.com/a-relatively-easy- to-understand-primer-on-elliptic-curve-cryptography.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY