Analysis of Encryption Methods to Enhanced Secure data Transmission in Wireless and Cloud Group Communication

Rajnish Choubey[1], Dr. Shiv Shakti Shrivastava[2], Dr. Santosh K. Gandhi[3]
[1]Ph.d. Research Scholar, Department of CSE, RNTU, Raisen M.P. (India)
[2]Associate Professor, Department of CSE, RNTU, Raisen M.P. (India)
[3]OSD, DTE, Govt. of MP, Bhopal (India)

ABSTRACT
Wireless communication has poised to become one of the most predominant area of research in the field of communication engineering. Wireless sensor network (WSN) have limited bandwidth, low computational functions, energy constraints. Inspite of these constraints, WSN is useful where communication happens without infrastructure support. The main concern of WSN is the security as the sensor nodes may be attacked and information may be hacked. The key pre-distribution schemes in wireless networks have attracted researchers' attentions recently in some applications. These researches of key pre-distribution focus on the balance among security, energy overhead and network resilience, because of the low computing ability, small storage and limited energy of nodes in wireless networks. In this paper, a key pre-distribution scheme based on sub-regions is proposed for group communications in wireless networks.

KEYWORDS:- Wireless Networks, Multicast, Key Management, High Leave probability, High Join probability, High Switch probability,

INTRODUCTION

In the age of big data, one of the most important and valuable assets in the world is the data. Almost every business in every field makes most of their decisions after computing and analyzing the available data. Therefore, ensuring the safety and reliability of the data during its transmission and management has become a pressing and important issue. This also includes ensuring the authenticity of data sources and preventing malicious alteration of original data.

As wireless networks have constraints in terms of bandwidth and energy, reducing the communication between base station and sensors plays vital role on power consumption and utilization of bandwidth. Aggregated wireless sensor network serve this purpose. The process of collecting, processing and forwarding the result of the raw sensed data from sensor nodes by intermediary nodes called 'aggregators' is called Data Aggregation. This concept reduces the data transmitted in the network and as a result leads to prolonged life time of network. Without proper security mechanism, it is not possible to perform this operation. Due to the deployment environment of WNs, the physical compromise of sensor nodes and aggregators is possible. It may also lead to false aggregation results. To address these issues, the first option is cryptographic mechanisms using which confidentiality and integrity mechanisms can be achieved [17].

Wireless networks (WNs) collects data from its environment, store and process them, and finally sends the processed data to users, either upon event detection or on demand . They are identified as groups of widely distributed sensors used in monitoring and recording the physical conditions of its environment through organization or collection of data and reporting them to a central point , through wireless links.

This makes it crucial to encrypt sensitive data that are transported from a node to another node in wireless sensor networks so that it will not be modified by or disclosed to any unauthorized party. Data encryption and decryption however, hinges on the cryptography scheme used and the generated key type. Cryptography involves the technique for securing communication in the presence of third parties, which is categorized into public key cryptography, secret key cryptography and hash function (one-way cryptography) based on the keys employed [16].

Various cryptographic protocols/methods are used to solve security concerns by encrypting the data. Cryptography is a technique used for electronic protection over transmission of valuable data which is mainly science for implementing information security. The primary purpose of cryptography is to preserve data by various authentication scheme. During authenticating the data, it is essential to consider that it should cost less than the value of the original data [3].

With the increased use of the Internet that is widely spread in our world, and with the advent of cloud computing technology in recent years, interest in cloud technology is increased and becomes widely used various fields, so security of this technology becomes necessary. Data protection is a very important issue especially in cloud computing because most service providers do not usually have a robust security system to protect data centers, so it is necessary to rely entirely on the lessor to process its basic environment to maintain its data safely. It is mandatory for the organization and multi tenancy to use a suitable data encryption algorithm through cloud computing. Each of encryption algorithms has advantages and disadvantages in term of many security metrics such as throughput, entropy, encryption and decryption time and memory usage and avalanche effect [8].

Cryptography is the science based on maintaining the confidentiality of data by converting it to the unreadable form by certain algorithms. It is utilizing science of mathematics for converting plaintext data (P) into format of an ambiguous cipher text (C), this process is known as "Encryption", with using one or more of encryption algorithms (E). While the process of returning the cipher text back to plaintext known as "Decryption", with using one or more of decryption algorithms (D). For encryption and decryption utilizing encryption keys (k1and /or K2).

Cryptography algorithms are classified according to the encryption key used. These algorithms are Symmetric-key algorithms, Asymmetric-key algorithms, hybrid algorithms and Hashing algorithms. In symmetric key algorithm, process of encryption and decryption of the data utilize one key called private key . While in asymmetric key algorithm cryptographic two keys are used, private key (used for decrypting data) and public key (used for encrypting data). In hashing algorithms, data will compress for signing to standard fixed size. Whereas in hybrid encryption two or more algorithms of the same type or more than one type are used.

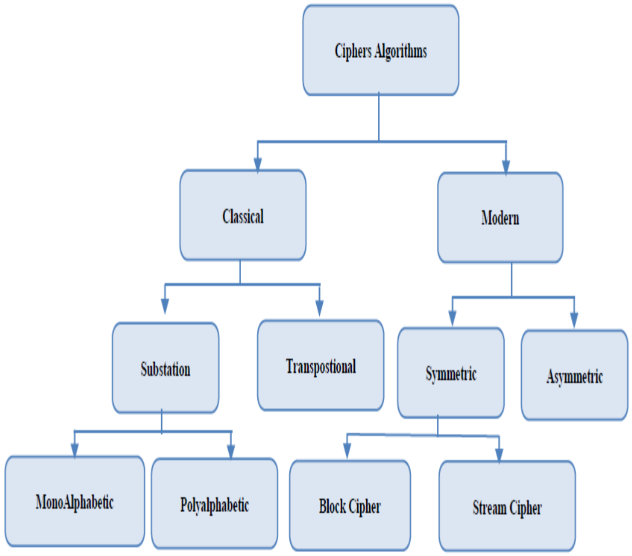


Fig 1: Classification of cipher algorithms [8].

In wireless group communications, each node is an intelligent unit to collect, process and forward data.

When two nodes need exchange packets securely, they need keys to encrypt and decrypt packets. Key schemes for encryption and decryption include symmetric key, asymmetric key and hybrid key schemes. The two later key schemes are not suitable for wireless communications for their high complexities, so current key schemes for wireless communications incline to the symmetric key schemes. The simplest method to get symmetric keys is the centralized key distribution scheme, in which the nodes have to apply session keys from the key distribution center (KDC). Although it has a high security and reliability, too much energy is consumed to obtain session keys from the remote KDC in wireless group communications [11]. Data flows in communication networks and they are always at risk to more vulnerabilities or security breaches. These security threats may include breach of confidentiality, data integrity problems, authenticity problem by impersonation, man-in-the-middle-attack, and insider attacks. In order to overcome these breaches, some algorithms have been developed [13].

RSA
RSA algorithm exhibits key generation, encryption, and
decryption.

Key Generation
1: Select p, and q; where, p and q both are primes, $p \neq q$.
2: Calculate n = pxq.
3: Calculate $\Phi(n) = (p-1)x(q-1)$:
4: Select encryption exponent e;
gcd(Φ(n), e) = 1 and ($1 < e < \Phi(n)$).
5: Calculate decryption exponent d;
$d\text{-}e^{-1}$(mod Φ(n)).
6: Public key PU = (e, n).
7: Private key PR = (d, n).
Encryption
1: Plaintext: M < n.
2: Ciphertext: $C = M^{e}$ mod n.
Decryption
1: Ciphertext: C.
2: Plaintext: $M=C^{d}$ mod n.

RELATED WORK

[1] Security is an important issue in the digital world, in this paper author presents the comparative experimental study between the RSA and ECC algorithm, here author compare the both techniques for the time taken during the encryption and decryption using the both techniques for a specific key pattern like 8 bits, 64 bits and 356 bits. They suggest that the ECC algorithm performs better than the RSA algorithm in the terms of operational efficiency and resource constraints devices.

[2] Data is very important parts of the current business system and we have to keep them secret, cryptographic is a techniques where we can secret our data or information from the outside user, here they present the comparative study for the asymmetric cryptographic techniques with security algorithm like ECC, ECNR, ECIES and RSA. As we know that the ECC algorithm is very robust equivalent with the RSA with shorter key length.

[8] Cryptographic is the science of protecting data by converting data (plain text) into an incomprehensible format (cipher text) for unauthorized individuals through the use of mathematical techniques. This paper provides work for the most common encryption algorithms that are utilized to encryption of data in cloud computing and presented some of papers that based on the most common cryptographic techniques such as DES, 3DES, Blowfish, AES, RSA, D-H, ECC and others.

[12] This paper presents a performance study and analysis of two popular public-key cryptosystems: RSA with its two variants, and ECC (Elliptic Curve Cryptography). RSA is considered as the first generation public-key cryptography, which is very popular since its inception while ECC is gaining its popularity recently. The paper shows the result of the experimentation performed using these cryptosystems with the different modulus/key sizes recommended by the NIST. The modulus/key sizes are used such as 1024/2048/3072-bit for RSA and 160/224/256-bit for ECC.

[16] From this study, it is observe from the output of the elliptic curve cryptographic key generation code that, for each attempt to send or transfer information from a sender to a receiver,

a new private key is generated. This is as a result of the random private key (integer) which is chosen to generate the shared private key for the two parties. The variant shared private key generated for each communication in the elliptic curve cryptography makes the network protocol less predictive by attackers during communication.

EXPERIMENT RESULT

In this section we present the improve master key encryption scheme with using elliptic curve cryptography was originally suggested by Neal Koblitz and Victor S. Miller (1985). This techniques is more flexible with the user requirements and provide the enhance security key management and reduce the storage space in cloud computing environment. Elliptic curve cryptography uses the less power and very fast and secure then compare to RSA and DSA algorithm. The proposed scheme simulated with the network simulator 2.34, And analysis the performance of proposed and existing scheme for the storage overhead communication I.e. requirement of memory capacity for the key management with present and previous techniques.

The continuous application of various transactions in the security increasingly demands smaller transaction size and higher transaction efficiency. All these requirements are closely related to the encryption algorithms used during the transaction. Small key size will occupy less memory. Good key generation performance will spend less time and provide a higher speed of producing a transaction. Outstanding key verification performance will spend less time and provide higher speed for verifying the
transaction. In this paper in our model, we use network simulator to do the calculation. We have picked the following three aspects namely; key size, key generation performance, and signature verification performance to make the comparison between RSA and ECC algorithms.

In this study, the application of elliptic curves in cryptography for the construction of public and secret keys is carried out. To analyze the strength and feasibility of elliptic curves in cryptography, data encryption/decryption process is studied in line with elliptic curves. The Elliptic Curve cryptography technique identified as most robust technique for key generation is then employed to construct secured public and private keys.

ECC (Elliptic Curve Cryptography)

ECC cryptography is promising asymmetric cryptography, this type of system is most suitable for memory constraint devices such as Smartphone etc. To encrypt and decrypt the data, an ECC requires comparatively less or smaller parameters than RSA, but with equivalent levels of security.

ECC Algorithm

ECC algorithm exhibits key generation, encryption and decryption

Global Public Elements

Step I. Chooses an elliptic curve Eq(a, b) with parameters
a, b, and q, where q is a prime and > 3, or an integer of the form 2m.
Step II. Selects G(x, y) - a global point on elliptic curve whose order is large value n.

User Alice Key Generation

Step I. Selects a private key, VA; where, VA < n
Step II. Calculates the public key, PA(x, y)
$PA(x, y) = VA \times G(x, y)$.

User Bob Key Generation

Step I. Selects a private key, VB; where, VB < n.
Step II. Calculates the public key, PB(x, y);
$PB(x, y) = VB \times G(x, y)$.

Calculation of Secret Key by User Alice

Step I. $SK(x, y) = VA \times PB(x, y)$

Calculation of Secret Key by User Bob

Step I. $SK(x, y) = VB \times PA(x, y)$.

Encryption by Alice using Bob’s Public Key

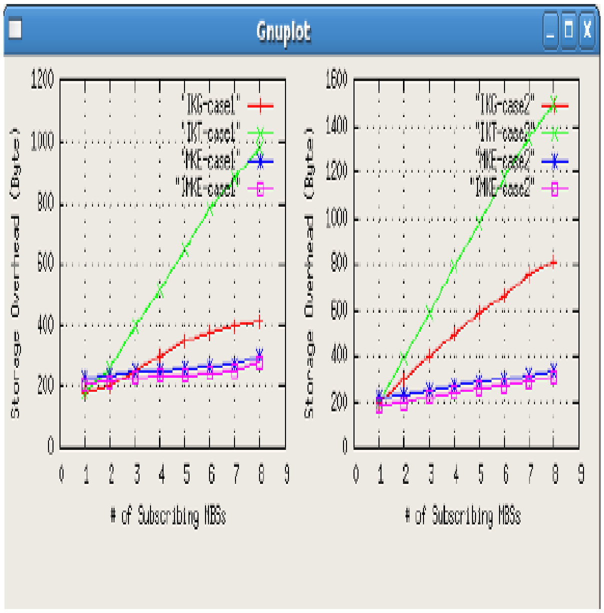
Step I. Alice chosen message Pm(x, y) and a random positive integer ‟k‟ and $1 < k < q$
,tep II. Ciphertext, Cm((x, y),(x, y)); = ((k × G(x, y)),
(Pm(x, y) + k × PB(x, y))).

Decryption by Bob using his own Private Key

Step I. Ciphertext, Cm((x, y),(x, y))
Step II. Plaintext, Pm(x, y);
= (Pm(x, y) + k × PB(x, y)) - (k × VB × G(x, y))
= Pm(x, y).

Here, first coordinate of Cm gets multiplied with the private key of the Bob i.e, VB, which in turns becomes similar to Bob‟s public key. Finally, due to substation of resultant coordinate with the second coordinate of the ciphertext Cm, all get canceled and only Pm(x, y) gets left.

This section evaluates the communication overhead (CO) of the new IMKE-MGKM scheme through numerical analysis and simulations. In the MGKM, the membership change of a user can be regarded as the switching from one SG to another SG. For example, if user1, seen in Fig. 2, quits subscribing to both MBS2 and MBS3, it becomes one of SG4 members. This paper analyzes the number of rekeying messages transmitted by the KDC, denoted by COi;j, when a user moves from SGi to SGj, because the number of rekeying messages determines the CO. To represent a user who leaves all the MBSs, SG0 is defined as the group that does not subscribe to any MBSs.



(a) (b)

Fig 2: Analysis of storage overhead as number of subscribing MSBs for case 1 and case 2.

It is assumed that there are three events in the simulation model: The joining of a new user with probability a, the leaving with probability b, and the switching of a SG with probability c, and we assume that two or more events cannot occur simultaneously in a single time slot. In below figure we shows the number of rekeying messages against the number of users in a SG for three scenarios: 1) high joining probability (a = 0:5, b =c =0:1), 2) high leaving probability (b = 0:5, a = c ¼=0:1), and 3) high switching probability (c = 0:5, a = b = 0:1). Here, the number of users ranges from 500 to 5,000. The results are averaged over 1,000 iterations, each of which has 5,000 simulation time slots. The number of the MBSs is set to 8 and the results are used to compare the three schemes relatively rather than absolutely.

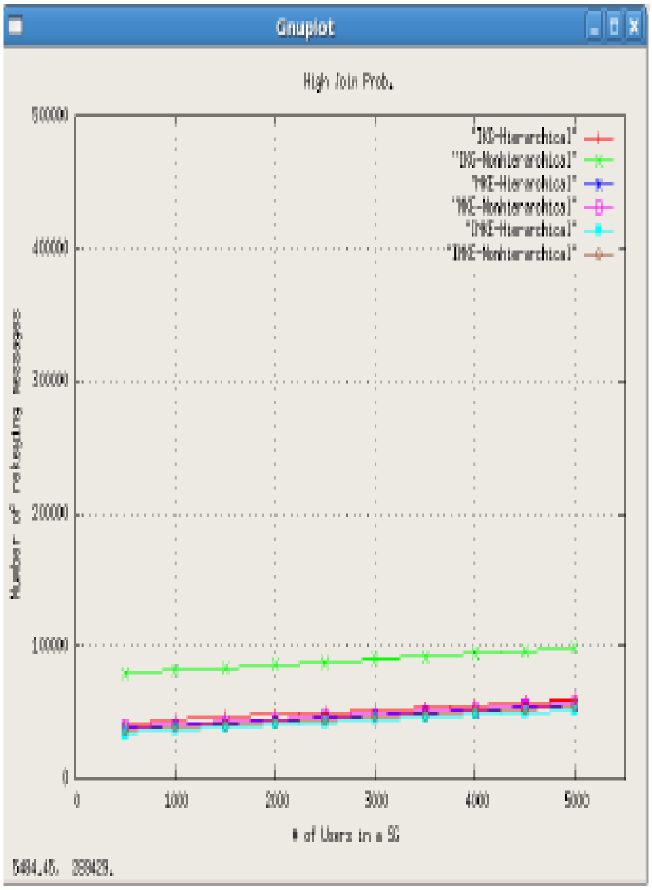


Fig 3: Comparisons between the previous and proposed techniques for the high join probability with no, of rekeying message generation.

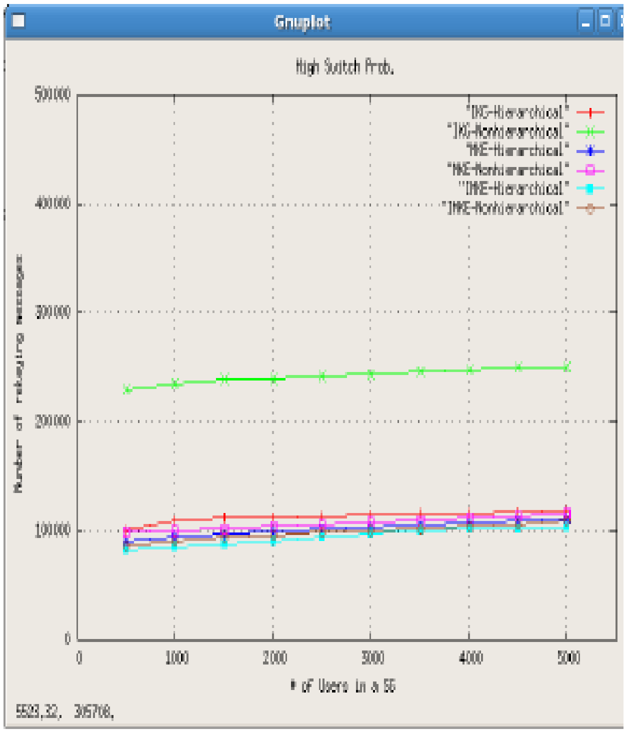


Fig 4: Comparisons between the previous and proposed techniques for the high switch probability with no, of rekeying message generation.

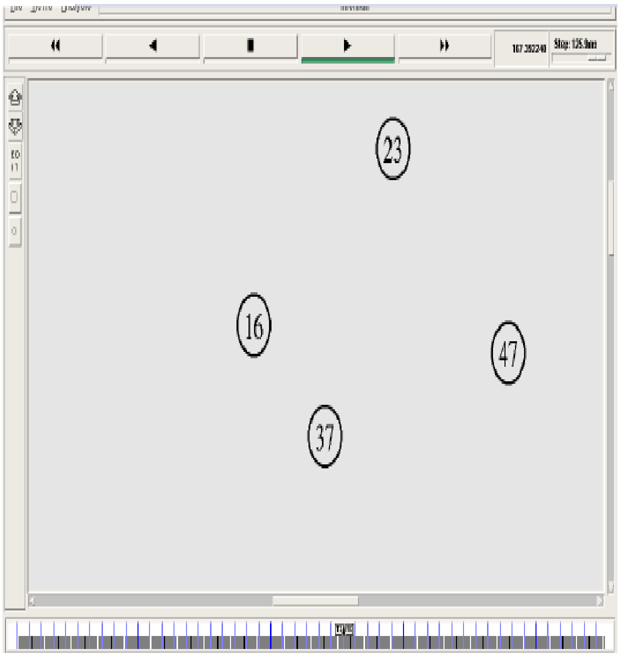


Fig 5: The above figure shows the node positions in a group communication.

Name of method	High leave prob. (no. of rekeying message)	High switch prob. (no. of rekeying message)	High join prob. (no. of rekeying message)
Previous method	13000	12000	6000
Proposed method	11000	10000	5000

Table 1: The above table shows the comparative study between the previous and proposed techniques with no. of rekeying message generation.

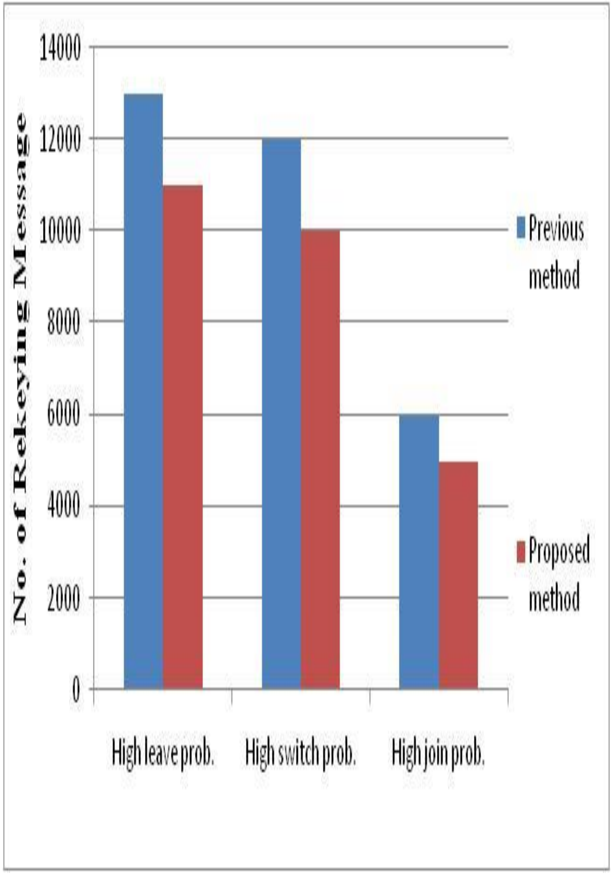


Fig 6: Comparisons between the previous and proposed techniques of the high join probability, high leave probability and high switch probability for the user, with no. of rekeying message generation.

CONCLUSION

The proposed method ECC is a suitable choice to achieve wireless network communication security. The proposed enhanced version of ECC provides a good choice for asymmetric cryptography. The RSA key with 1024 bit key provides the secured environment as that of 160 bit elliptic curve key. By using speed, storage, power and bandwidth several advantages can be achieved by smaller key sizes. The shorter key means less storage space and reduced arithmetic operations. In total, enhanced ECC based algorithm can be easily included into currently used protocols to achieve security with smaller resources.

REFERENCES

[1] Dindayal Mahto, Dilip Kumar Yadav, “RSA and ECC: A Comparative Analysis”, International Journal of Applied Engineering Research, Volume 12, 2017, pp. 9053-9061.

[2] Nelson Josias Gbètoho Saho, Eugène C. Ezin, “Comparative Study on the Performance of Elliptic Curve Cryptography Algorithms with Cryptography through RSA Algorithm”, CARI 2020 – Colloque Africain sur la Recherche en Informatique.pp. 1-15.

[3] Zeinab Vahdati, Sharifah Md Yasin, Ali Ghasempour, Mohammad Salehi, “Comparison of ECC and RSA Algorithms in IoT Devices”, Journal of Theoretical and Applied Information Technology, 2019, pp. 4293-4308.

[4] Mashrufee Alam, Israt Jahan, Liton Jude Rozario, Israt Jerin, “A Comparative Study of RSA and ECC and Implementation of ECC on Embedded Systems”, International Journal of Innovative Research in Advanced Engineering, 2016, pp. 86-89.

[5] Kumari Archana, Vibhuti Sikri, “Comparative Analysis of RSA and ECC”, International Journal of Innovative Research in Computer and Communication Engineering, 2015, pp. 7299-7303.

[6] P.Rajesh Kannan, Dr. R.Mala, “Analysis of Encryption Methods to Enhance Secure Data Transmission”, INFOKARA RESEARCH, 2019, pp. 1197-1210.

[7] Ahmed Othman Khalaf, Shaimaa Khudhair Salah, Hind Jumaa Sartep, Zainab Khyioon Abdalrdha, “Subject Review: Comparison between RSA, ECC & NTRU Algorithms”, International Journal of Engineering Research and Advanced Technology, 2019, pp. 11-15.

[8] Ali Kadhim Bermani, Mehdi Ebady Manaa , Ahmed Al-Salih, “Efficient cryptography techniques for image encryption in cloud storage”, Periodicals of Engineering and Natural Sciences, 2020, pp. 1359-1373.

[9] Sonali Chandel, Wenxuan Cao, Zijing Sun, Jiayi Yang, Bailu Zhang, Tian-Yi Ni, “A Multi-dimensional Adversary Analysis of RSA and ECC in Blockchain Encryption”, Springer Nature Switzerland, 2020, pp. 988-1003.

[10] Priyanka Durge, Hirendra Hajare, “ Countering Drawbacks of RSA and Its Replacement By ECC Algorithm” International Research Journal of Modernization in Engineering Technology and Science, 2020, pp. 1062-1068.

[11] Yinghong Liu, Yuanming Wu, “A Key Pre-distribution Scheme based on Sub-regions for Multi-Hop Wireless Sensor Networks”, Wireless Personal Communications, Springer 2019, pp. 1-20.

[12] Dindayal Mahto, Dilip Kumar Yadav, “Performance Analysis of RSA and Elliptic Curve Cryptography”, International Journal of Network Security,, 2018, pp. 625-635.

[13] O Sri Nagesh, Vankamamidi S Naresh, “Comparative Analysis of MOD-ECDH Algorithm and Various Algorithms”, International Journal of Industrial Engineering & Production Research, 2020, pp. 301-308.

[14] Ashima Narang, Deepali Gupta, “Comparative Analysis of Various Cloud Security Frameworks”, International Conference

on cyber security and privacy in communication networks, 2018, pp. 379-386.

[15] Notom Ajay kumar, Mrinal Sarvagya, Parag Parandkar, "A novel security algorithm ECC-L for wireless sensor network", Internet Technology Letters. 2020, pp. 1-6.

[16] Stephen Aikins-Bekoe, James Ben Hayfron-Acquah, "Elliptic Curve Diffie-Hellman (ECDH) Analogy for Secured Wireless Sensor Networks", International Journal of Computer Applications, 2020, pp. 1-9.

[17] Jyothi R, Nagaraj G Cholli, "An efficient approach for secured communication in wireless sensor networks", International Journal of Electrical and Computer Engineering, 2020, pp. 1641-1647.