Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 9s (2025)

Enhancing IoT Security: A Hybrid IDEA64 ECEG based Cryptographic Approach for Efficient Encryption and Robust Session Key Management

Remegius Praveen Sahayaraj L[1], Jeevitha A[2], Lakshmi Priya V[3], Aishwarya PL[4]

[1,2,3,4] Loyola – ICAM College of Engineering and Technology, Chennai, Tamil Nadu, India.

[1]pravinsahayaraj@gmail.com, [2]jeevitha.a@licet.ac.in, [3]lakshmipriya.23cs@licet.ac.in, [4]aishwaryapl07@gmail.com

Article History:

Received:11-11-2024

Revised:24-12-2024

Accepted:09-01-2025

Abstract:

The Internet of Things (IoT) presents unique challenges for securing sensitive information due to resource-constrained devices and open network environments. This paper proposes a hybrid cryptographic algorithm to address these concerns. The approach leverages the strengths of the IDEA 64 algorithm for efficient data encryption and the Elliptic Curve Exponential-Golomb Coding (ECEG) algorithm for secure session key management. By combining these functionalities, the proposed algorithm aims to achieve a robust security solution for sensitive information transmission in IoT networks. The paper discusses the design of the hybrid algorithm, its advantages over existing methods, and potential areas for further research

Keywords: *Internet of Things (IoT), Security, Sensitive Information, Cryptography, IDEA 64, ECEG Algorithm, Session Key Management.*

1. INTRODUCTION:

IoT uses the embedded sensors with the physical objects and it gathers and acts upon the information from the environment. Low embedded system, cloud computing, availability of big data, networking connection are the four main components of Iot. Some of the recent establishment of IoT includes smart homes, gene therapy, agriculture, smart cities, and medicine. Network layer is handled by IPv6 and application layer is handled by Auto Discovery Remote Control (ADRC). To connect different vehicles IoT uses One Machine to Machine (M2M) service layer. People used the internet just to send messages and call each other before the invention of IoTs, but the invention of IoT makes us to interact with physical objects. Artificial Intelligence and machine learning are used in IoT to collect data. IoT is often used in healthcare to completely monitor patients. Some of the examples of IoT includes home security, activity tracker, self-healing machines, AR glasses, smart contact lenses. The main and basic motto of IoT is to make the world 'smart'. In the Internet of things (IoT) there are many challenges to be solved. Some of the challenges are as follows. In cellular networks, rapid increase in mobile broadband services for video streaming and content sharing. The Europe FP7 project Mobile and wireless communications Enablers for the Twenty-twenty Information Society (METIS) introduces a 5G network. IoT products often lack thorough testing and updates, leading to security issues. Poor connectivity can hinder the reliable operation of IoT sensors, affecting data monitoring and information supply. Balancing hardware and software development is essential to ensure optimal performance, especially with the growing number of devices. The act of securing IoT involves protecting devices

and networks from threats while identifying, monitoring, and addressing vulnerabilities to maintain a robust security posture in the IoT ecosystem. IoT security faces a major obstacle in the form of devices that were not made with security in mind from the beginning, making them susceptible in networks. For optimal IoT operation, a comprehensive solution to protect hardware, software, and communication is required, as the inability to manually install security software on devices increases this risk. In the absence of strong security, connected devices—such as industrial bots—are vulnerable to hacking, which makes it possible for illegal access and data theft. In order to address these issues, an integrated solution that guarantees protection, visibility, and segmentation throughout the network architecture is needed. For the protection of low-end, cost-sensitive devices, embedded software toolkits containing security protocols such as TLS and IPsec are essential. In order to maximize overall system efficiency, there is a growing need for IoT systems that are lightweight and require little power and resources. The metrics used in hardware implementation includes memory consumption, throughput, latency, facility consumption. And for software implementation includes RAM consumption, code size. Since IoT uses a lot of M2M communication, these devices are vulnerable to power consumption. Low power Static RAM (SRAM) may increase the power consumption. To overcome the above problem, one can use extra transistors but this may decrease the performance. Some companies introduce special microcontrollers with a low-power mode of operation called deep power down or deep sleep which can run at full speed during normal operation and drop into low-power modes when not required. By this method IoT devices can reduce power consumption without affecting the performance. The special type of protocol namely Message Queuing Telemetry Transport (MQTT) is used in IoT connectivity to increase the efficiency. It is lightweight protocol which acts uses broker-based system which works on the Transmission control protocol. MQTT is lighter than HTTP 1. 1 protocol. It has more advantage as it offers security and privacy, lightweight protocol, uses minimum packets of data. Our proposed system uses IDEA-64 and ECC and Elgamal algorithms. The above-mentioned algorithms are used due to its lightweight nature. As lightweight algorithm is used in IoT because of the reasons as we previously mentioned.

2. LITERATURE SURVEY

S. M. Riazul Islam et al. [1] investigate how wearable technology can be integrated with IoT in the healthcare industry, highlighting how crucial security upkeep is. Their plan covers a wide range of portable devices, including laptops, tablets, PCs, and mobile phones, in addition to wearables. They skillfully collect and store personal health data on the cloud using a variety of sensors, allowing for on-demand access. This study highlights the possibility for improving security protocols and service quality in this emerging industry in the future.

Zelaing Liu et al. [2] suggest an inventive use of IoT technology for the protection of cultural artifacts. To track the presence of treasures within museum premises, their solution makes use of passive RFID technology. When artifacts escape specified boundaries, alarms are set off via electronic tags attached to the artifacts that connect to a central PC. To maintain this protective framework's effectiveness, the authors emphasize that system upgrades must be made on a regular basis to stay up with RFID technological improvements.

Chin-Teng Lin et al.'s [3] innovative wireless method for remote patient sleep monitoring is presented. Their technology captures patients' important bio signals and safely stores the information in the cloud

so that doctors can access it at any time. The system accurately detects the stages of sleep using EEG and EOG technologies, which reduces expenses and improves diagnostic precision. This creative method marks a major breakthrough in remote healthcare monitoring by prioritizing patient comfort while streamlining diagnosis.

Chalermpong Senarak [4] emphasizes the critical role of strong security measures and pushes for the incorporation of cybersecurity knowledge into port facility operations within seaports. Port systems can be made more resilient to cyberattacks and function better by integrating TNP, CTM, and CSM and ISM experience. However, thorough training for Port Facility Security Officers (PFSOs) is required for the successful implementation, which could result in higher expenses and time commitments. In order to protect vital infrastructure and marine assets, port operations must prioritize cybersecurity, as this proactive strategy emphasizes.

Ramaprabha Jayaram S & Prabakaran [5] suggested an inventive edge-cloud system is in an effort to improve predictive accuracy and data security. Strong privacy protection is provided by them by storing encrypted forms and filtering non-sensitive data at the edge. Their approach reduces prediction and reaction times, minimizes capacity utilization, and provides higher prediction accuracy by incorporating an adaptive weighted probabilistic classifier model. They also support the use of blockchain security features to secure electronic health records, which would strengthen data integrity and confidentiality in medical settings. Using edge-cloud technologies for improved data management and security in healthcare systems has advanced significantly with the adoption of an all-encompassing approach.

In a thorough survey, F. John Dian et al. [6] divided wearable IoT devices into categories for sports, health, daily use, tracking, and location. These gadgets use sensors to track vital and non-vital signs and notify users when there are anomalies in the former. But issues like power consumption and safety worries still exist. Examining substitutes such as Cellular IoT could improve wearable IoT system efficiency.

A unique approach is presented by Nidal Nasser et al. [7] that uses unmanned aerial vehicles to collect data from wearable and ambient sensors of each user equipment and securely store it in the hospital cloud. Using B5G makes it easier to address data privacy concerns in wireless communications with federated machine learning. Nevertheless, the system's memory usage could be a problem.

Brain-computer interface (BCI) privacy is a goal pursued by Shams Ajrawi et al. [8], who also suggest a BCI Identification System for user identification. By connecting the central nervous system (CNS) to the outside world and transforming inputs into artificial output, this system interfaces with the CNS. Authorized clinicians are the only ones with access to securely stored output signals on the cloud. Still, there are obstacles in the way of accomplishing two-way communication.

With an emphasis on the utilization of antecedents' qualities for cybersecurity, Ling Li et al. [9] investigate the Protection Motivational Model as a technique of preventing cyberattacks within businesses. Factors including response cost, self-efficacy, and efficacy are addressed by cognitive mediating processes. Although fundamental methods of gathering data are used, the implementation of sophisticated strategies may improve overall security protocols.

By introducing a system that uses Time-delay Mutual Information to evaluate multi-camera architecture, Keyang Cheng et al. [10] overcome the drawbacks of conventional video surveillance techniques that could miss suspicious patient behaviors. By using re-identification techniques, their proposed system locates and tracks anomalous behaviors in mental health hospitals, improving patient monitoring and guaranteeing prompt intervention.

The importance of control and monitoring apps for customized health services in traditional healthcare systems is highlighted by Najma Taimoor et al. [11]. The authors demonstrate targeted monitoring and control of particular health concerns with examples such as blood pressure monitors and insulin pumps. Their analysis also identifies research gaps that need to be filled in order to create individualized healthcare systems that are trustworthy and long-lasting in the future. Rahul Saha and associates [12] present a ground-breaking e-healthcare architecture that emphasizes electronic medical records (EMRs) and privacy protection. Their framework connects people, things, and processes through the Internet of Things (IoTs) to improve human social life. The authors verify the technology's effectiveness through comparative and experimental investigations, highlighting its noteworthy benefits for e-healthcare in a cloud-fog network.

Narrowband IoT (NBIoT), according to Sudhir K. Routray et al. [13], is a more affordable and straightforward kind of IoT that can manage jobs well, especially in the healthcare industry. NBIoT is a top choice for many healthcare applications due to its low resource needs. Nonetheless, worries about wearable device pain and safety continue to exist, highlighting the need for more research in this field. Roberto O. Andrade and colleagues [14] argue in favor of improved cybersecurity design in residential settings, pointing out differences from enterprise security standards. They draw attention to how attackers take use of social engineering techniques and use COVID-19 worries to make their attacks more potent. The pandemic has altered human behavior, which has increased the attack surface of smart homes. Cybercriminals are taking advantage of psychological characteristics linked to COVID-19 to launch cyberattacks.

An ontology-based system that organizes cybersecurity data and complies with industry standards is introduced by Takeshi Takahashi et al. [15]. Their research explores the useful uses of this knowledge base and ontology in cybersecurity operations. Delineating responsibilities and operational domains, the framework highlights the prevalence of manual handling of operations caused by an absence of well-structured cybersecurity information across enterprises. It provides clarification on the kinds of information used, by whom, and for what particular objectives. According to Mohamed Maazouz et al. [16], putting strong encryption measures in place is essential to protecting the privacy of data that is transferred. This global infrastructure, which builds on information and communication technologies, enables smooth communication and interaction among a vast network of ten billion intelligent physical or virtual items. The security level set by this complex matrix determines how well the suggested algorithm works.

Thumbnail-Preserving Encryption (TPE), which preserves the thumbnail after encryption, is a solution that Yongming Zhang et al. [17] present as balancing privacy and usability. In keeping with people's social characteristics, this method is especially helpful for photos shared on social media, cloud storage, and image hosting platforms. It makes it easier for individuals to record and share their life events. TPE leverages the confusion-diffusion properties of chaotic systems to provide security while

drastically reducing encryption and decryption times. According to Sajitha A. S. et al. [18], encryption is an essential method that hides the true meaning of data by converting it into a secret code. They stress the significance of image data security, which is an essential component of data security. If at least k pieces are obtained, the decryption procedure carried out by the human visual system permits the extraction of secret information. A very safe way to accomplish this is to use direct visual cryptography.

A novel definition of cybersecurity is put out by Ziga Turk et al. [19], who characterize it as the absence of three errors in any one of the four major areas that comprise information and communications technologies (ICT): design, building, operation, and maintenance. Their methodology offers a novel and comprehensive approach to cybersecurity by conceptualizing security as the absence of stealing, lying, and injuring. A system for continually monitoring a patient's bodily signs, such as blood pressure, ECG, SpO2, and pertinent environmental indicators, is introduced by Chao Li [20]. By providing four different ways to transmit data, this system successfully strikes a balance between the needs for computing and communication resources as well as healthcare. It also uses context awareness and data stream mining technologies to provide improved pervasive healthcare services, like real-time patient knowledge assistance and early warning alarms. IoT-generated healthcare data is secured by K. M. Besher, Z. Subah, and M. Z. Ali [21] via a matrix multiplication approach that transmits encrypted data to the cloud. But because their method just uses basic matrix multiplication for encryption, it is open to several kinds of assaults.

Using antecedent qualities for cybersecurity, Ling Li, Li Xu, and Wu He [22] investigate the Protection Motivational Model as a strategy to stop cyberattacks inside of companies. A cognitive-meditative approach is used to address variables including response cost, self-efficacy, and efficacy of response. Although there are basic data collection mechanisms in place, using more sophisticated techniques could improve overall security measures. A. Bozesan et al.'s analysis of the IDEA NXT encryption algorithm's throughput and execution time [23] showed how effective it is in comparison to other methods. IDEA NXT is a new generation of scalable and adaptable symmetric encryption algorithms that were created in response to the need for increased speed, resilience, and security against assaults.

A new IDEA VLSI realization is presented by S. Wolter et al. [24], who first use the IDEA method with the block cipher VINCI. This chip, which operates at a throughput rate of 177.8 Mb/s (@25 MHz), exceeds the highest data speeds possible for existing DES processors. Although the VINCI chip requires considerably higher data rates for IDEA-based cryptographic devices, it is appropriate for real-time encryption, such as that found in ATMs. The suggested IDEA approach, which has four operational modes and an increased chip area of roughly 16%, is evaluated by online tests that use a mod-3 residue code and encode/decode redundant test words. Radio Frequency Identification (RFID) technology is widely used in asset management, healthcare, anti-counterfeiting, and supply chain management systems. X. Shen et al. [25] utilize IDEA for RFID technology. RFID uses radio frequency signals instead of physical contact to identify electronic tags. Because IDEA has an equivalent key length but less power consumption and delay than AES, it is preferred. Furthermore, IDEA has no known effective linear or algebraic flaws, which makes it more appropriate for RFID applications.

IDEA was used by D. V. Penumetcha, Jiafeng Xie, and Saiyu Ren [26] to implement hardware on FPGA using pipelined architecture with RTL looping. Its resilience to linear cryptanalysis and decreased power consumption are the main factors in this decision. Similar to a CPU, FPGA is used in many areas, such as software-defined radio, medical imaging, video and image processing, military applications, wired and wireless communications, and integrating many basic programmable logic devices. Its capacity to convey data continuously provides it a flexible alternative in various fields. The construction of a safe transmission system for ECG data, including ECG acquisition, diagnosis, visualization, and secure storage, was the goal of M. U. Shaikh et al. [27]. The system places a high priority on ease of use for researchers and medical professionals. They utilized the Fully Homomorphic Encryption (FHE) methodology for secure data transfer and the QRS complex method for ECG signal diagnosis. Only authorized medical professionals will be able to decrypt and comprehend the ECG readings thanks to FHE, which makes it possible to conduct algebraic operations on plaintext directly on the ciphertext, protecting the security and integrity of the sent data.

An improved IDEA technique is presented in [28], where it is used in a framework for USB security keys. Specifically designed for E-commerce applications, this version of IDEA includes a random number feedback mechanism based on double verification technology. Especially, the technique efficiently hides statistical features and improves password security. Furthermore, the implementation of the Low-high-bit algorithm greatly enhances the effectiveness of the IDEA method, mitigating its drawbacks and expediting its execution. Karim Shahbazi et al. [29] introduce a novel architecture for IDEA based on the Application Specific Instruction set Processors (ASIPs) Platform. This approach divides the task into hardware and software components, leveraging ASIPs' specific instructions to execute specialized tasks more efficiently compared to general-purpose processors, thereby reducing programming errors. Their architecture includes a new crypto processor featuring various cryptographic algorithms, including IDEA. Designed to support both general-purpose and specific IDEA instructions, the architecture is validated using VHDL code.

In their discussion of an asynchronous VLSI implementation of IDEA, N. Sklavos and O. Koufopavlou [30] provide a synchronous version of the method for assessment. They describe the algorithm in VHDL, a hardware description language, and use two distinct ASIC designs—synchronous and asynchronous—for hardware implementation. The two designs use distinct clocking methods even if their functionality is comparable. Two implementations of the IDEA core, a key component of ASICs, are available: one uses clock-synchronized processing, while the other uses asynchronous methods to save power. The five cycles of the architecture are implemented asynchronously, which offers lower power consumption in all operation modes (the difference varies from 20-40%). The incorporation of cybersecurity expertise into port facility operations at seaports is investigated by Chalermpong Senarak [31]. In order to improve system performance, this entails combining expertise in Threat and Risk Assessment (TNP), Cybersecurity Technology Management (CTM), and Information Security Management (ISM) with competencies in Cybersecurity Management (CSM) and Information Security Management (ISM). But in order to put this system into place, Port Facility Security Officers (PFSOs) need to have the right training, which could mean spending more money and time.

A method is shown by Nidal Nasser et al. [32] that uses unmanned aerial vehicles to collect data from wearable and ambient sensors on individual user equipment and store it safely in the hospital cloud.

By utilizing B5G for federated machine learning, they solve wireless communications' data privacy issues. However, the system's memory consumption could be a disadvantage. AMI 0.5 process technology standard cells were used in the VLSI implementation of the IDEA block cipher that M. Macchetti and Wenyu Chen [33] presented using VHDL. The implementation makes use of the temporal parallelism included into the IDEA method and optimizes the modulus multiplier. Interestingly, once the original key is acquired, subkeys are produced internally and kept until a fresh key is used for encryption. This design is beneficial because it reduces the requirement for extra RAM to hold subkeys, which is a notable gain in memory efficiency.

Using a commercial technology library, M. Macchetti and Wenyu Chen [34] explore how to implement the IDEA NXT algorithm in bespoke silicon. To satisfy various latency and area occupation requirements while preserving a high degree of security, several optimizations are used. This is the first time the IDEA NXT encryption algorithm—which was initially created by Junod and Vaudenay and is protected by a patent held by MediaCrypt AG—has been implemented on ASIC hardware. Although the design choices are mostly focused on custom silicon processes, they might also be applied to other target technologies, such as programmable hardware such as FPGAs, with potentially very effective results. Ledda et al. [35] investigate improvements to the IDEA algorithm through the combination of the middle square approach and circular shifting. These enhancements include changing the bit shifting, bit manipulation, and number of rounds during the encryption and decryption stages. The suggested method generates the ciphertext in an astoundingly short amount of time—28.83 milliseconds. Notably, its avalanche effect of 50.35% satisfies encryption criteria. IDEA's results on a number of tests, including the frequency (monobit) test (0.789), the frequency test within a block (0.997462), and the run test (0.897437), further demonstrates its improved security.

In order to improve the safe transmission of graphic-text used in mobile phones, W.-X. Zhang, S.-Y. Xiao, and Y. Zhang [36] make use of the extremely effective and lightweight properties of the X-IDEA encryption algorithm, an upgraded version of IDEA. The method is optimized for 3G transmission, supporting photographs of varying sizes and a higher probability of recurring patterns. The software smoothly integrates into mobile phone operations and successfully encrypts and decrypts image files, guaranteeing transmission security. The IDEA algorithm, a block cipher created by James L. Massey and Xuejia Lai at ETH-Zürich, is discussed by V. S. Prajwal and K. V. Prema [37]. It is a minor variation on the DES cipher, utilizing a 128-bit key length to encrypt a 64-bit block of plaintext into a 64-bit block of ciphertext. The authors draw attention to the use of four different keys, two distinct bit blocks, and an increase in the number of rounds from eight to ten. For less sensitive data, they recommend reducing the encryption time; for extremely sensitive data, they recommend enhancing security. Increasing the use of the brute force method can also improve system security.

The system [38] highlights important factors to make sure cloud environments are secure .The authors provide an advanced security architecture that uses controlled access methods, elliptic curve cryptography (ECC), and location-based data storage and access (LDSA). The addition of LDSA improves the security architecture by adding a geographic component to data storage and access. Through the integration of these components, the article seeks to address the growing issues of cloud computing privacy and confidentiality by offering a comprehensive solution for protecting communication as well as data storage in cloud environments. The elliptic curve Diffie-Hellman

(ECDH) technique is enhanced in [39] by genetic algorithms and fuzzy logic. Genetic algorithms optimize important parameters to strengthen security, while fuzzy logic is used to improve the algorithm's adaptation to dynamic and unexpected network settings. The paper explores the possible usefulness of this hybrid strategy in reducing security concerns and ensuring the reliable transfer of cryptographic keys in wireless communication contexts.

In [40], elliptic key encryption combined with beta gamma functions is used to improve the confidentiality and integrity of data exchanged in Wireless Sensor Networks (WSNs). The paper explores the mathematical underpinnings of the Beta Gamma functions used in cryptography and shows how effective they are at protecting WSN routing systems. By offering a fresh method for cryptographic applications in WSNs, this research considerably advances network security and may have an effect on how secure different IoT and wireless communication systems.

3. SYSTEM ARCHITECTURE:

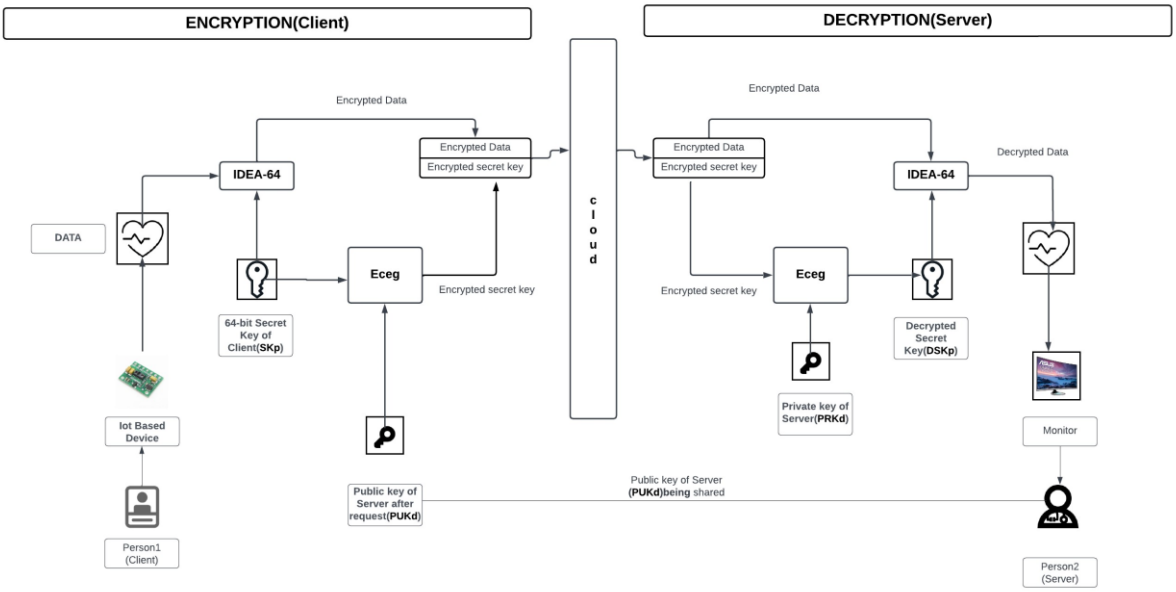

Fig 3. 1 The model architecture

3.1 Collecting data from pulse oximeter sensor module(MAX30100)

As depicted in the Figure 3.1, the public key and private key of the server are generated using the ECC and Elgamal algorithms. Our suggested algorithm comprises an encryption and decryption system where the data is encoded at the sender's end with a specific session key and transferred to the receiver. First of all, the message to be encrypted is received from the client. In our case, the message in the form of heart beat rate and oxygen saturation is generated by the hardware device which consist of MAX30100 sensor and given as an input to our system. This input is given to the IDEA-64 algorithm.

3.2 Encryption of data using IDEA-64 Algorithm

This encryption algorithm operates on a 64-bit input with a 28-bit key as shown in figure 3.2, executing 8 rounds utilizing 6 subkeys each, and employing four keys for output transformation. The 64-bit session key is used for encryption. This session key can either be generated by a random function or

given by the client. In our system, we have created a random function to generate the 64-bit session key. This 64-bit key is split into four blocks of 16-bit data. In the IDEA-64 algorithm, the plaintext of size 32 bits is given as input. This input is split into four blocks. Each block consists of 8-bit data. It uses 52 subkeys for encryption. The subkeys for further rounds are generated by shifting the parent 64-bit session key. These 52 subkeys are used in 8 rounds. Each round uses six subkeys, and for the last round, it uses ten subkeys. So totally (8*6)+4=52 subkeys are used. Since it uses 52 subkeys and 8 rounds, linear cryptanalysis is difficult. The low-cost operations modulo addition, modulo subtraction, and XOR are used. The output is the encrypted message.

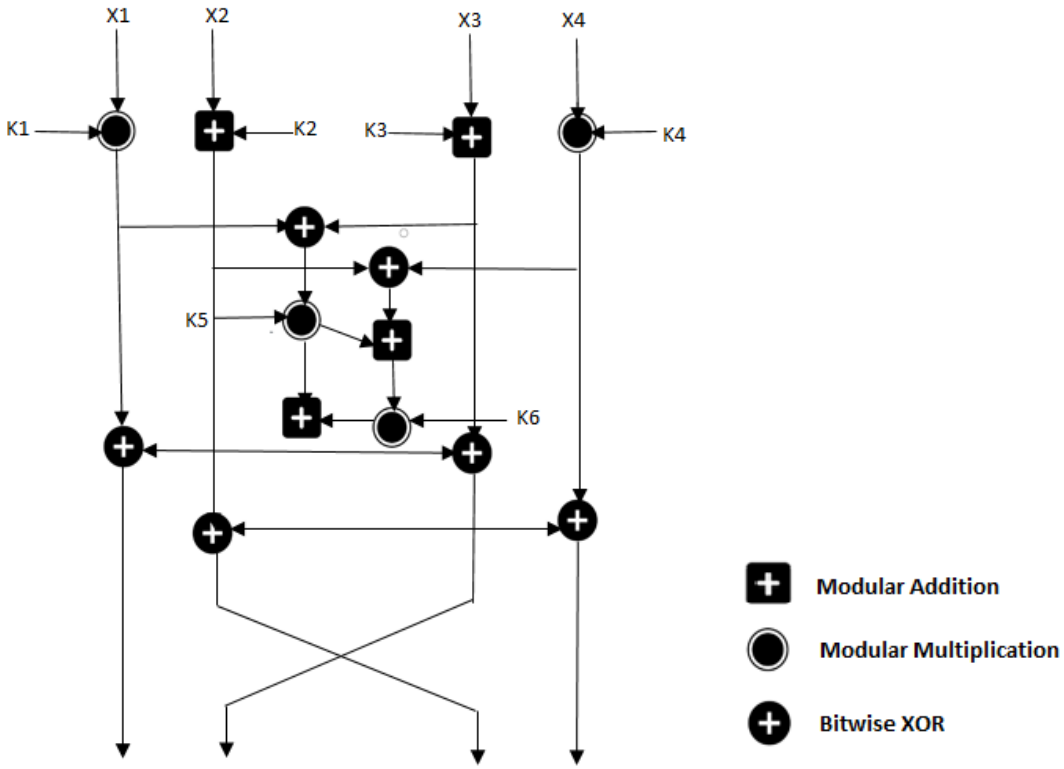

Figure 3.2 Process of Encryption

3.3 Encryption of session key using Eceg Algorithm

The session key used for encryption of messages is given as an input to Eceg algorithm. The public key will be further used to encrypt the session key of the client, which will be delivered after a request from the client side to the server side. The encrypted session key is in the form of c1, c3. In each of the above (x, y) coordinates, information is encoded using the P-256 curve. The encrypted message, along with the encrypted session key, is released from the router to the cloud. Here we have used a socket connection for sending and receiving the encrypted and decrypted data. The private key is generated using the random function and curve P-256, which is also used to generate the public key. The size of the private key is 256-bit. The public key is in the form of (x, y) coordinates.

3. 4 Decryption of session key and data

When the packet of encrypted message and encrypted session key is received at the server side, first the session key is decrypted using Eceg algorithm. The decryption process takes place using the private

key of the server. The output of this process is the 64-bit session key of sender. This 64-bit session key is used for the decryption of the encrypted message, and the original message is displayed to the receiver.

3.5 Proposed IDEA and Eceg based Encryption and Decryption Algorithm

Encryption :

Input: Plain Text [Pulse and Oxygen rate]

Output: Cipher Text [Encrypted Pulse and Oxygen rate]

Step 1: Get the input from the pulse oximeter.

Step 2: Perform the encryption of input using the 64-bit IDEA key as follows:

a. Split the input into 4 blocks of 8-bit.

b. The 64-bit Session key is divided into four 16-bit subkeys.

c. Each of the 8 round consists of the following operations:

i. XOR the 16-bit subkey, K_i for the current round with the 16-bit plaintext block, P_i and store in cipher text , C_i

C_i = P_i XOR K_i

ii.substitute the 16-bit block using a predefined S-Box,S(P_i)

C_i = S(P_i)

iii. Permutation, P of the bits within the 64-bit block is taken place and the output is again stored in cipher text, C_i

C_i = P(C_i)

iv. Perform modular addition of C_i block with 2^16 (65536)

C_i = C_i + 2^16

d. After 8 rounds, a final permutation is applied to the block and the result obtained is 32-bit block of cipher text, C.

Step 3: The Session Key S used for encryption of input data is being encrypted as follows:

a. The public key K is received from the receiver by using socket connection.

b. Random point k, G is generated from the P-256 curve.

c. Cipher text C1 is generated as, C1 = k * G.

d. Cipher text C2 is generated as, C2 = S + k * K.

Step 4: The encrypted input, C and the Session Key, C1,C2 is sent to the receiver.

Decryption:

Input: Plain Text [Pulse and Oxygen rate]

Output: Cipher Text [Encrypted Pulse and Oxygen rate]

Step 1:Receive the Cipher text, C and Encrypted session key (C1,C2).

Step 2: The Decryption of Session Key using the private key, Kr of receiver is as follows:

a. Random point l, G is generated from the P-256 curve.

b. The final Cipher text S is generated as, S = C2 + (l – Kr) * C1.

Step 3: The Decryption of input is as follows:

a.Split the Cipher text,C into 4 blocks of 8-bit.

b. The 64-bit decrypted Session key is divided into four 16-bit subkeys.

c.Each of the 8 round consists of the following operations:

i. XOR the 16-bit subkey, K_i for the current round with the 16-bit Cipher text, C_i i and store in plain text for current round in , P_i

C_i = P_i XOR K_i

ii. perform the inverse substitution using the inverse of the same S-Box with cipher text, C_i

P_i = S^(-1)(C_i)

iii. Perform inverse permutation

C_i=P^(-1)(C_i)

iv. Perform modular subtraction of C_i block with 2^16 (65536)

C_i = C_i - 2^16

d. After 8 rounds, a final permutation is applied to the block and the result obtained is 32-bit block of plain text, P.

5. Results and Performance evaluation:

The Table 5.1 below infers that the number of subkeys is higher in the proposed system when compared to all other existing algorithms, and hence the brute force attack is difficult. And also, the number of rounds is lower, which eventually lowers the overall execution time of the system.

Table 5. 1 Basic comparison of different encryption algorithms

FACTORS	**AES**	**TRIPLE-DES**	**IDEA**	**Proposed System**
Key-size	128	168	64	64
No.of rounds	10	48	8	9
Operations	Substitution and permutation	Shift and permutation	Shifting and Modulo	Shifting, modulo, Encoding and Decoding

No.of subkeys	11(round keys)	48	52	52
Mathematical Operation	Substitution and permutation	XOR and fixed S-boxes	XOR,Addition, Multiplication(modulo)	XOR,Addition, Multiplication(modulo)

The insights from **Table 5.2**, shows that the encryption time and decryption time are less than all other compared algorithms. And also, the encryption time of our proposed system is 98.06% less than AES and 99.081% less than Triple-Des. The decryption time of our proposed algorithm is 80.17 % less than AES and 90.25 % less than Triple-DES. The shorter execution time eventually lowers battery consumption.

Table 5. 2 Execution time of different encryption algorithms excluding hardware properties

FACTORS	AES	TRIPLE-DES	IEceg
Encryption Time	248147 microseconds	264138 microseconds	87091 Microseconds
Decryption Time	206532 microseconds	234047 microseconds	88495 microseconds
Overall Execution (with Eceg)	296532 microseconds	294047 microseconds	148488 Microseconds

Below **Table 5.3** clearly demonstrates the strong correlation between our system's increased throughput and its significantly shorter execution time, demonstrating a higher degree of effectiveness and efficiency.

Table 5. 3 Execution time of different encryption algorithms including hardware properties

FACTORS	AES	TRIPLE-DES	IEceg
Encryption Time (in ms)	45474018	53074225	2462510
Decryption Time (in ms)	49074528	58147011	2474088
Overall Execution (in ms)	51074528	60147011	38474528

In the table 5.4 below, various algorithms are compared on two different system configurations, and proves that our system works better and consumes less energy and memory, demonstrating increased efficiency.

Table 5.4 Memory Usage and Battery consumption of the proposed hybrid model

Configurations	Intel Core i5 Processor, 2.50GHz, RAM:8.00 GB, Windows 10 OS				Intel Core i3 Processor, 2.50GHz, RAM:4.00 GB, Windows 11 OS			
Parameter / Algorithm	**AES**	**3DES**	**DES**	**Proposed Hybrid Model**	**AES**	**3DES**	**DES**	**Proposed Hybrid Model**
Battery consumption (%)	3.4	5.5	4.8	2.60	4.2	5.6	4.8	2.98
Memory Usage	32.5	46.3	39.2	38.9	40.5	49.3	43.2	3.94

We examine the time complexities of various algorithms in this table 5.5 and demonstrated that our system's effectiveness and efficiency in handling computational tasks is high and precise.

Table 5.5 Time complexity analysis

Algorithm/Complexity	**ECC**	**[38]**	**[39]**	**[40]**	**MTECSR**	**Proposed Hybrid Model**
Best case	O(n3)	O(n2 log n)	O(n2 log n)	O(n3)	O(n log n)	O(n log n)
Average case	O(n3)	O(n2 log n)	O(n2 log n)	O(n3)	O(n2)	O(n log n)
Worst case	O(n4)	O(n3)	O(n3)	O(n4)	O(n2)	O(n2)

We provide a thorough comparison examination of the security levels offered by various algorithms in the table 5.6 below . Our research shows that our system performs better in terms of security and provides a higher level of protection.

Table 5.6 Security level analysis

Experiments	[38]	[39]	[40]	MTECSR	Proposed Hybrid Model
E1	85.76	89.84	91.56	96.87	97.52
E2	87.65	90.43	93.23	97.54	97.52
E3	88.13	91.35	93.78	98.45	99.65
E4	88.52	92.23	94.72	98.75	99.55
E5	89.02	93.65	94.92	98.92	99.32
Average	87.81	91.5	93.64	98.10	98.71

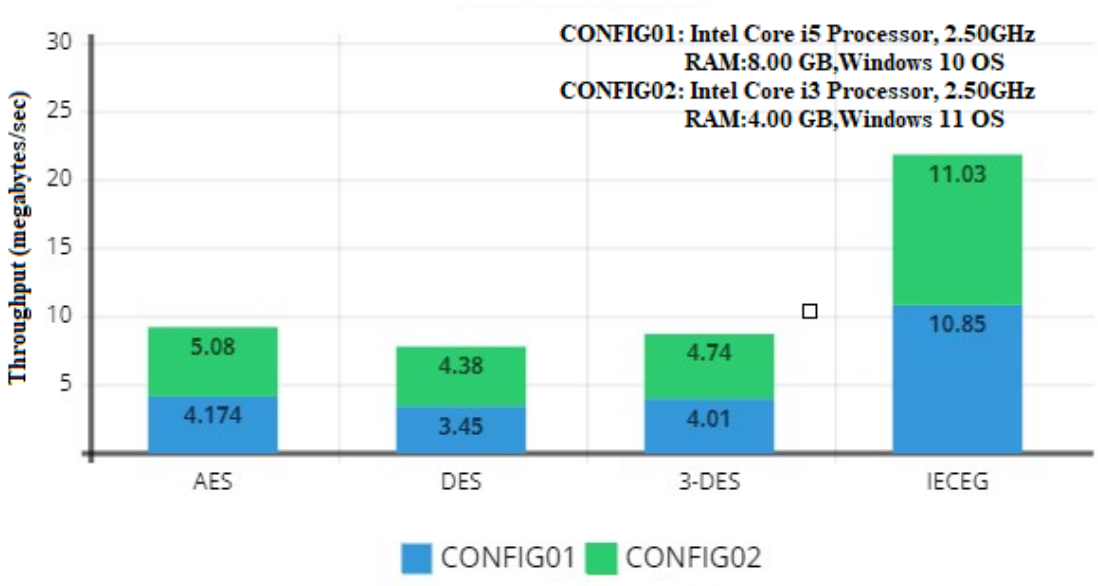

Figure 5. 1 Execution time of AES, Triple-DES, Our Proposed system.

Figure 5.1 illustrates the execution time of AES, Triple-DES, and our proposed system. Notably, our proposed system demonstrates significantly superior efficiency compared to AES and Triple-DES. Furthermore, the potential for even faster execution in hardware translates to reduced power consumption, highlighting the enhanced efficiency of our system.

5. 2 CONCLUSION AND FUTURE WORK:

The proposed system ensures secure healthcare data flow, building customer trust amidst evolving cyber threats. It facilitates practical and user-friendly data transmission from patient IoT devices to a doctor's monitor, emphasizing the integrity and confidentiality of personal medical information, thereby supporting the overall security and efficiency of healthcare systems. The use of the Pretty Good Privacy (PGP) enhancement for the IDEA encryption algorithm provides a robust safeguard for

healthcare data during transmission and storage, with seamless adaptability to both hardware and software settings. Furthermore, our system employs the ECC and ElGamal algorithms for secret key encryption and data integrity, adding an extra layer of security to the system. In conclusion, the proposed algorithm, initially designed for IoT-based oximeters, offers a sturdy framework for data security in healthcare. Its adaptability extends to ECG and blood glucose monitoring devices, preserving data reliability and fortifying these systems against potential external attacks. Additionally, our proposed system boasts impressive performance metrics, being approximately 17% faster at encryption than AES and 33% more efficient than Triple-DES. In practical terms, this means our model processes data more quickly, with a 70% boost in throughput compared to AES, DES, and our proposed system on average, ensuring better overall performance. Its versatile capabilities position it as a promising solution for safeguarding classified information in evolving security landscapes across various sectors.

REFERENCES:

[1]S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain and K. -S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey, " in IEEE Access, vol. 3, pp. 678-708, 2015, doi: 10. 1109/ACCESS. 2015. 2437951.

[2]Z. Liu, M. Wang, S. Qi and C. Yang, "Study on the Anti-Theft Technology of Museum Cultural Relics Based on Internet of Things, " in IEEE Access, vol. 7, pp. 111387-111395, 2019, doi: 10. 1109/ACCESS. 2019. 2933236.

[3]C. -T. Lin et al., "IoT-Based Wireless Polysomnography Intelligent System for Sleep Monitoring, " in IEEE Access, vol. 6, pp. 405-414, 2018, doi: 10. 1109/ACCESS. 2017. 2765702.

[4]Chalermpong Senarak, Cybersecurity knowledge and skills for port facility security officers of international seaports: Perspectives of IT and security personnel, The Asian Journal of Shipping and Logistics, Volume 37, Issue 4, 2021, Pages 345-360, ISSN 2092-5212, https://doi. org/10. 1016/j. ajsl. 2021. 10. 002.

[5]Ramaprabha Jayaram, S. Prabakaran, Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system, Egyptian Informatics Journal, Volume 22, Issue 4, 2021, Pages 401-410, ISSN 1110-8665, https://doi. org/10. 1016/j. eij. 2020. 12. 003.

[6]F. John Dian, R. Vahidnia and A. Rahmati, "Wearables and the Internet of Things (IoT), Applications, Opportunities, and Challenges: A Survey, " in IEEE Access, vol. 8, pp. 69200-69211, 2020, doi: 10. 1109/ACCESS. 2020. 2986329.

[7]Nidal Nasser, Zubair Md Fadlullah, Mostafa M. Fouda, Asmaa Ali, Muhammad Imran, A lightweight federated learning based privacy preserving B5G pandemic response network using unmanned aerial vehicles: A proof-of-concept, Computer Networks, Volume 205, 2022, 108672, ISSN 1389-1286, https://doi. org/10. 1016/j. comnet. 2021. 108672.

[8]Shams Ajrawi, Ramesh Rao, Mahasweta Sarkar, Cybersecurity in Brain-Computer Interfaces: RFID-based design-theoretical framework, Informatics in Medicine Unlocked, Volume 22, 2021, 100489, ISSN 2352-9148, https://doi. org/10. 1016/j. imu. 2020. 100489.

[9]Ling Li, Li Xu, Wu He, The effects of antecedents and mediating factors on cybersecurity protection behavior, Computers in Human Behavior Reports, Volume 5, 2022, 100165, ISSN 2451-9588, https://doi. org/10. 1016/j. chbr. 2021. 100165.

[10]K. Cheng, M. S. Khokhar, Q. Liu, R. Tahir and M. Li, "Data-Driven Logical Topology Inference for Managing Safety and Re-Identification of Patients Through Multi-Cameras IoT, " in IEEE Access, vol. 7, pp. 159466-159478, 2019, doi: 10. 1109/ACCESS. 2019. 2951164.

[11]N. Taimoor and S. Rehman, "Reliable and Resilient AI and IoT-Based Personalised Healthcare Services: A Survey, " in IEEE Access, vol. 10, pp. 535-563, 2022, doi: 10. 1109/ACCESS. 2021. 3137364.

[12]R. Saha, G. Kumar, M. K. Rai, R. Thomas and S. -J. Lim, "Privacy Ensured ${e}$ -Healthcare for Fog-Enhanced IoT Based Applications, " in IEEE Access, vol. 7, pp. 44536-44543, 2019, doi: 10. 1109/ACCESS. 2019. 2908664.

[13]S. K. Routray and S. Anand, "Narrowband IoT for healthcare, " 2017 International Conference on Information Communication and Embedded Systems (ICICES), 2017, pp. 1-4, doi: 10. 1109/ICICES. 2017. 8070747.

[14]R. O. Andrade, I. Ortiz-Garcés and M. Cazares, "Cybersecurity Attacks on Smart Home During Covid-19 Pandemic, " 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 2020, pp. 398-404, doi: 10. 1109/WorldS450073. 2020. 9210363.

[15]T. Takahashi and Y. Kadobayashi, "Reference Ontology for Cybersecurity Operational Information, " in The Computer Journal, vol. 58, no. 10, pp. 2297-2312, Oct. 2015, doi: 10. 1093/comjnl/bxu101.

[16]Mohamed Maazouz, Abdelmoughni Toubal, Billel Bengherbia, Oussama Houhou, Noureddine Batel, FPGA implementation of a chaos-based image encryption algorithm, Journal of King Saud University - Computer and Information Sciences, 2022, ISSN 1319-1578, https://doi. org/10. 1016/j. jksuci. 2021. 12. 022.

[17]Yongming Zhang, Ruoyu Zhao, Yushu Zhang, Rushi Lan, Xiuli Chai, High-efficiency and visual-usability image encryption based on thumbnail preserving and chaotic system, Journal of King Saud University - Computer and Information Sciences, 2022, ISSN 1319-1578, https://doi. org/10. 1016/j. jksuci. 2022. 04. 001.

[18]A. S. Sajitha, A. Shobha Rekh, Review on various image encryption schemes, Materials Today: Proceedings, 2022, ISSN 2214-7853, https://doi. org/10. 1016/j. matpr. 2022. 03. 058.

[19]Žiga Turk, Borja García de Soto, Bharadwaj R. K. Mantha, Abel Maciel, Alexandru Georgescu, A systemic framework for addressing cybersecurity in construction, Automation in Construction, Volume 133, 2022, 103988, ISSN 0926-5805, https://doi. org/10. 1016/j. autcon. 2021. 103988.

[20]Chao Li, Xiangpei Hu, Lili Zhang, The IoT-based heart disease monitoring system for pervasive healthcare service, Procedia Computer Science, Volume 112, 2017, Pages 2328-2334, ISSN 1877-0509, https://doi. org/10. 1016/j. procs. 2017. 08. 265.

[21]K. M. Besher, Z. Subah and M. Z. Ali, "IoT Sensor Initiated Healthcare Data Security, " in IEEE Sensors Journal, vol. 21, no. 10, pp. 11977-11982, 15 May15, 2021, doi: 10. 1109/JSEN. 2020. 3013634.

[22]Ling Li, Li Xu, Wu He, The effects of antecedents and mediating factors on cybersecurity protection behavior, Computers in Human Behavior Reports, Volume 5, 2022, 100165, ISSN 2451-9588, https://doi. org/10. 1016/j. chbr. 2021. 100165.

[23]A. Bozesan, F. Opritoiu and M. Vladutiu, "Hardware implementation of the IDEA NXT crypto-algorithm, " 2013 IEEE 19th International Symposium for Design and Technology in Electronic Packaging (SIITME), Galati, Romania, 2013, pp. 35-38, doi: 10. 1109/SIITME. 2013. 6743640.

[24]S. Wolter, H. Matz, A. Schubert and R. Laur, "On the VLSI implementation of the international data encryption algorithm IDEA, " Proceedings of ISCAS'95 - International Symposium on Circuits and Systems, Seattle, WA, USA, 1995, pp. 397-400 vol. 1, doi: 10. 1109/ISCAS. 1995. 521534.

[25]X. Shen, D. Liu, Y. Yang and J. Wang, "A low-cost UHF RFID tag baseband with an IDEA cryptography engine, " 2010 Internet of Things (IOT), Tokyo, Japan, 2010, pp. 1-5, doi: 10. 1109/IOT. 2010. 5678440.

[26]D. V. Penumetcha, Jiafeng Xie and Saiyu Ren, "FPGA design space exploration of IDEA cryptography IP core, " 2015 IEEE 58th International Midwest Symposium on Circuits and Systems (MWSCAS), Fort Collins, CO, USA, 2015, pp. 1-4, doi: 10. 1109/MWSCAS. 2015. 7282150.

[27]M. U. Shaikh, S. Anom Ahmad and W. A. Wan Adnan, "Investigation of Data Encryption Algorithm for Secured Transmission of Electrocardiograph (ECG) Signal, " 2018 IEEE-EMBS Conference on Biomedical Engineering and Sciences (IECBES), Sarawak, Malaysia, 2018, pp. 274-278, doi: 10. 1109/IECBES. 2018. 8626640.

[28]. An Improved IDEA Algorithm Based on USB Security Key | IEEE Conference Publication | IEEE Xplore

[29]Karim Shahbazi, Mohammad Eshghi, Reza Faghih Mirzaee, Design and implementation of an ASIP-based cryptography processor for AES, IDEA, and MD5, Engineering Science and Technology, an International Journal, Volume 20, Issue 4, 2017, Pages 1308-1317, ISSN 2215-0986, https://doi. org/10. 1016/j. jestch. 2017. 07. 002.

[30]N. Sklavos and O. Koufopavlou, "Asynchronous low power VLSI implementation of the International Data Encryption Algorithm, " ICECS 2001. 8th IEEE International Conference on Electronics, Circuits and Systems (Cat. No. 01EX483), Malta, Malta, 2001, pp. 1425-1428 vol. 3, doi: 10. 1109/ICECS. 2001. 957482.

[31]Chalermpong Senarak, Cybersecurity knowledge and skills for port facility security officers of international seaports: Perspectives of IT and security personnel, The Asian Journal of Shipping

and Logistics, Volume 37, Issue 4, 2021, Pages 345-360, ISSN 2092-5212, https://doi. org/10. 1016/j. ajsl. 2021. 10. 002.

[32]Nidal Nasser, Zubair Md Fadlullah, Mostafa M. Fouda, Asmaa Ali, Muhammad Imran, A lightweight federated learning based privacy preserving B5G pandemic response network using unmanned aerial vehicles: A proof-of-concept, Computer Networks, Volume 205, 2022, 108672, ISSN 1389-1286, https://doi. org/10. 1016/j. comnet. 2021. 108672.

[33]M. Macchetti and Wenyu Chen, "ASIC hardware implementation of the IDEA NXT encryption algorithm, " 2006 IEEE International Symposium on Circuits and Systems (ISCAS), Island of Kos, 2006, pp. 4 pp. -4846, doi: 10. 1109/ISCAS. 2006. 1693715.

[34]M. Macchetti and Wenyu Chen, "ASIC hardware implementation of the IDEA NXT encryption algorithm, " 2006 IEEE International Symposium on Circuits and Systems (ISCAS), Island of Kos, 2006, pp. 4 pp. -4846, doi: 10. 1109/ISCAS. 2006. 1693715.

[35]M. K. C. Ledda, B. D. Gerardo and A. A. Hernandez, "Security Evaluation of the Enhanced IDEA Algorithm, " 2019 2nd World Symposium on Communication Engineering (WSCE), Nagoya, Japan, 2019, pp. 6-10, doi: 10. 1109/WSCE49000. 2019. 9041086.

[36]W. -X. Zhang, S. -Y. Xiao and Y. Zhang, "Research on Image-Text Encryption Techniques in Mobile Communications, " 2010 Second WRI Global Congress on Intelligent Systems, Wuhan, China, 2010, pp. 115-118, doi: 10. 1109/GCIS. 2010. 184.

[37]V. S. Prajwal and K. V. Prema, "User Defined Encryption Procedure For IDEA Algorithm, " 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, India, 2018, pp. 1668-1671, doi: 10. 1109/ICACCI. 2018. 8554699.

[38] Kavin, B. P., Ganapathy, S., Kanimozhi, U., & Kannan, A. (2020). An enhanced secu-rity frameworkfor secured data storage and communications in cloud using ECC, access control and LDSA. WirelessPersonal Communications, 115(2), 1107–1135.

[39]Sethuraman, P., Tamizharasan, P. S., & Kannan, A. (2019). Fuzzy genetic elliptic curve dife hell-man algorithm for secured communication in networks. Wireless Per-sonal Communications,105(3),993–1007.

[40]Viswanathan, S., & Kannan, A. (2019). “Elliptic key cryptography with Beta Gamma functionsfor secure routing in wireless sensor networks.” Wireless Networks, 25, 4903–4914.