International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Available online at: www.jrrset.com

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395

Volume 9, Issue 1 - January 2020-2021 - Pages 101-108

USING A COMBINATION OF ECC AND CEASER CIPHER CRYPTOGRAPHY, A NEW APPROACH TOWARDS IOT SYSTEM SECURITY

C N RAVI, LINU PAULOSE, S K MOULEESWARAN, PREMA MANI
Department of Computer Science and Engineering, Indira Gandhi Institute Of Engineering And Technology, Nellikuzhi P.O ,Kothamangalam, Ernakulam (Dist) Pincode 686691

Abstract
The Internet of Things (IoT) is a burgeoning technology that has captivated the interest of academics in academia and business. In the near future, it is anticipated that the Internet of Things (IoT) will be smoothly incorporated into our surroundings, and humans will become completely reliant on this technology for convenience and a more comfortable lifestyle. The system's security breach will have a direct impact on human existence. The domain of privacy and security in IoT has been widely acknowledged as one of the most formidable domains. IoT devices are known to have limitations such as low power and limited processing performance, making typical encryption algorithms impractical for use on these devices. Therefore, it is necessary to provide a lightweight encryption algorithm specifically designed for IoT devices to ensure safe communication and data transfer in the IoT environment. The existing cryptographic models and security systems rely on generally accepted encryption algorithms and privacy standards. Advanced Encryption Standard (AES) is often used to provide confidentiality in the majority of circumstances. Alternatively, Diffie-Hellman (DH) and Multi Curve Elliptic Curve encryption (ECC) enhance the privacy approaches, namely in the field of asymmetric encryption. Given the ambiguity surrounding the suitability of these cryptographic models and security methods, a thorough investigation is necessary to verify their feasibility for implementation in the designated resources of IoT. When handheld and portable devices have limited capabilities, a very significant and effective cryptographic approach that may be utilised is the Novel Caesar cypher method, which falls under the category of public key cryptography. This approach consists of two static operations, namely encryption and decryption.
Encryption using the Caesar cypher algorithm involves substituting each word in the text with a different word, thereby replacing the original text with a new one. Subsequently, the encrypted text may be produced. Continual research is being conducted to develop more adaptable cryptography suites with the aim of attaining superior outcomes. The security mechanisms of mixed mode, which likely include encryption and authentication, have generated significant attention.

Keywords: Cryptography, Internet of Things, Multi Curve ECC, Elliptic Curve Cryptography, Caesar Cypher

Introduction
The Internet of Things (IoT) is a rapidly growing technology that has captured the interest of academics in both academia and business. The concept behind the Internet of Things (IoT) is to establish connectivity or provide internet access to all objects or devices. The IoT ecosystem enables both Human to Machine communication and Machine to Machine interaction. In the future, the majority of devices will be interconnected via the Internet of Things (IoT), and human beings will primarily rely on electronic gadgets. The IoT industry has shown rapid growth during the last five years. The Internet of Things (IoT) is poised to become a major technological advancement in the future. Given that IoT technologies are interconnected with many day-to-day activities, such as personal and company management, in one way or another. IoT technology

International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Available online at: www.jrrset.com
ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395
Volume 9, Issue 1 - January 2020-2021 - Pages 101-108

will facilitate several crucial transactions. Any breach in the system's security will have a direct impact on human life. Privacy and security in the Internet of Things (IoT) have been identified as one of the most difficult and complex issues to address. IoT devices are known to have limitations such as low power and limited processing performance, making typical encryption algorithms impractical for use on these devices. Our objective is to create a lightweight encryption method specifically designed for IoT devices. This algorithm will provide safe communication and data transfer inside the IoT ecosystem.

Literature Review

Existing cryptographic models and security approaches rely on generally accepted encryption algorithms and privacy standards. Advanced Encryption Standard (AES) is often used to provide confidentiality in the majority of circumstances.
Alternatively, Diffie-Hellman (DH) and Multi Curve Elliptic Curve encryption (ECC) enhance the privacy approaches, namely in the field of asymmetric encryption. Given the uncertainty surrounding the suitability of various cryptographic models and security methods, a thorough examination is required to verify their feasibility for implementation within the designated resources of the Internet of Things (IoT). Particularly when considering the limited functionality of handheld and portable devices. Elliptic Curve Cryptography is an advanced kind of asymmetric cryptographic technique that utilises the algebraic structure of elliptic curves over finite fields for public-key cryptography [1].
Ramakrishna Hegde [2] suggested a cryptographic method that combines a multi-bend ECC algorithm with an optimised modified grid encoding steganography technique to encrypt the user's confidential data. The artificial bee colony algorithm was used to conceal the cipher-text inside an H.264 movie. The results of this approach were compared to those of LSB steganography and a regular FMO system.
The security of ECC relies on the capability to calculate point multiplication and the impossibility to calculate the multiplicand when given the original and product points [3]. The ECC standards are defined in SEC, which stands for Standards for Efficient Cryptography [4]. Elliptic curve encryption was separately introduced in the mid-1980s by Koblitz and Miller [5]. This study presents a very promising alternative to cryptographic protocols that rely on the discrete logarithm problem in the multiplicative group of a finite field. Examples of such protocols are Diffie-Hellman key exchange and ElGamal encryption/signature.

Security challenges by the Internet of Things (IoT)

Inadequate testing and upgrading

The main cause of the majority of IoT security vulnerabilities is from manufacturers' inadequate allocation of time and money towards security measures. The equipment, which was first seen as safe at the time of purchase, later becomes vulnerable to hackers and other security threats.
Many fitness monitors that use Bluetooth may still be seen by other devices even after they have been paired. A smart refrigerator can unintentionally reveal the login details for a Gmail account. Additionally, a smart fingerprint locks can be unlocked using a Bluetooth key that has the same MAC address as the padlock itself. One of the most significant security concerns with IoT is just this.

There are many security issues associated with IoT devices that are produced by manufacturers:
Weak, easily predictable, or statically embedded passwords
Hardware malfunctions
The absence of a reliable method for updating and ensuring security.

International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Available online at: www.jrrset.com
ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395
Volume 9, Issue 1 - January 2020-2021 - Pages 101-108

Some of the main vulnerabilities include outdated and unpatched embedded operating systems and software, as well as insecure methods of transferring and storing data.

Reason:

IoT manufacturers prioritise speed of production and delivery above security considerations.
Many manufacturers provide firmware upgrades for a limited duration, ceasing them as soon as they begin developing their next attention-grabbing device. They use outdated Linux kernels that are neither backed nor maintained.
The absence of universally accepted security standards for the Internet of Things (IoT) means that manufacturers will persist in producing devices with inadequate security measures.
Manufacturers that have begun integrating Internet connectivity into their gadgets often do not prioritise the "security" aspect as a critical factor in their product design process.
As a consequence of using old technology and software, their loyal consumers are left vulnerable to possible assaults.
Solution: To safeguard consumers against such assaults, each gadget must be thoroughly tested before being made available to the public, and organisations must consistently upgrade them.

Lack of User Knowledge & Awareness.

There is no text provided. A major security concern and obstacle in the realm of IoT is the user's lack of knowledge and awareness about the operation of IoT devices. Consequently, the safety of everyone is jeopardised.
Deceiving a person is often the most straightforward method to get entry into a network. There is no information provided. An frequently neglected IoT security problem is the vulnerability to social engineering attacks. Rather of focusing on exploiting hardware, a hacker directs their attention towards manipulating a person by using the Internet of Things (IoT).
Social engineering was used as a tactic in the 2010 Stuxnet assault on an Iranian nuclear facility. The assault targeted industrial programmable logic controllers (PLCs), which are also classified as IoT devices. The assault compromised 1,000 centrifuges, resulting in a catastrophic explosion at the facility. It is hypothesised that the internal network was segregated from the public network as a precaution against assaults. However, this precaution proved futile when a worker simply inserted a USB flash drive into one of the internal machines.

Challenges in maintaining the accuracy and reliability of data in healthcare IoT security

With the Internet of Things (IoT), data is always in motion. The data is being transferred, stored, and processed. Most Internet of Things (IoT) devices gather and collect data from the surrounding environment. They can function as smart thermostats, HVAC systems, televisions, and medical equipment. Occasionally, these gadgets transmit the gathered data to the cloud without using any encryption. Consequently, a hacker may infiltrate a medical IoT device, seizing command of it and having the ability to manipulate the data it gathers.

International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Available online at: www.jrrset.com
ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395
Volume 9, Issue 1 - January 2020-2021 - Pages 101-108

A regulated medical Internet of Things (IoT) device has the potential to transmit inaccurate signals, leading healthcare professionals to take decisions that might harm their patients' well-being. For instance, a compromised medical IoT device might falsely indicate to the maintenance station that its battery is completely charged, even when the battery is really on the verge of running out of power. Furthermore, healthcare equipment such as pacemakers or insulin injection devices are susceptible to significant dangers in terms of IoT security.

Home Invasions

One of the most alarming risks associated with IoT is the potential for home invasion. Currently, there is a widespread usage of IoT devices in both residential and commercial settings, leading to the emergence of home automation.
The security of these Internet of Things (IoT) devices is a significant cause for worry, since it might potentially reveal your IP address, which can be used to identify your home address. Hackers may sell this crucial information to underground websites that serve as safe havens for criminal organisations. If you include IoT devices into your security systems, there is a risk that they may be compromised, posing a significant danger to the security of your home.

Doubtful Communication

There are several Internet of Things (IoT) devices that transmit messages to the network without using any kind of encryption. Companies must assure the use of the most advanced encryption protocols for their cloud services and devices. The optimal approach is to use transport encryption and adhere to established standards such as TLS. An alternative approach involves using distinct networks that segregate individual devices. In October 2016, a hacker discovered a weakness in a particular type of security cameras. Approximately 300,000 Internet of Things (IoT) video recorders initiated a coordinated assault on several social network websites, resulting in the temporary shutdown of Twitter and other prominent platforms for a duration of almost two hours. There is no information provided. This assault serves as a mere illustration of the potential consequences that might befall IoT devices without adequate security measures. There is no text provided. Not just video cameras, but any device that has an internet connection, such as refrigerators, smart locks, thermostats, lightbulbs, automobiles, and even smart toys. Utilising IoT devices consistently presents issues and hazards that must be addressed in terms of security.

Revised Caesar Cypher Cryptography for Encrypting Confidential Message

One of the most effective techniques for public key cryptography is the Modified Caesar Cypher Method. In our study, we use this approach to encrypt the control message sent by the user to the appropriate IoT devices. This approach consists of two static operations, namely encryption and decryption. Encryption using the Ceaser cypher method involves replacing each word in the text with a different term. The original text, denoted as 'n', is substituted with another word. The cypher text may be derived using equation (1).

$$CI = PI + t \quad (1)$$

International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Available online at: www.jrrset.com
ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395
Volume 9, Issue 1 - January 2020-2021 - Pages 101-108

The equation above represents the relationship between the cypher text (Ci), the original plain text (Pi), and the key (t). The process of deciphering is accomplished by using the inverse function of encryption, which may be represented by the following formula (2).

$$Pi = Ci - t \quad (2)$$

Once the communication has been encrypted, it will be sent via the networks to ensure optimal security. Ultimately, this communication will be deciphered at the receiving end.

Multi-Curve ECC

Multi-Curve ECC refers to the use of several elliptic curves in elliptic curve cryptography. Elliptic Curve Cryptography (ECC) is a very efficient and safe cryptographic procedure that falls under the category of public key cryptography. This approach relies on the configuration of elliptic curves over finite fields[1]. The primary benefit of ECC is its decreased key size need compared to other cryptographic methods. This is very advantageous for implementing encryption on compact devices with restricted resources in terms of power, CPU, and memory. Additionally, it aids in the management of many sessions for expansive web servers. The robustness of an asymmetric encryption technique, such as ECC, lies on the intricacy of calculating the inverse of the function used to create the key. Generating the key is a straightforward and uncomplicated process. However, it is computationally impossible to determine the inputs that were used to generate the key. In ECC, the challenging problem is referred to as the "Elliptic Curve Discrete Logarithm Problem," which involves the difficulty of calculating the discrete logarithm (type) from the result. In addition, there are other sophisticated cryptographic algorithms that use the ECC cryptosystem as a foundation, making it an optimal choice. The process of transforming the client's confidential information into an encrypted form was carried out using Elliptic Curve Cryptography (ECC).

Modelling of ECC and Optimized Modified Matrix Encoding (OMME)

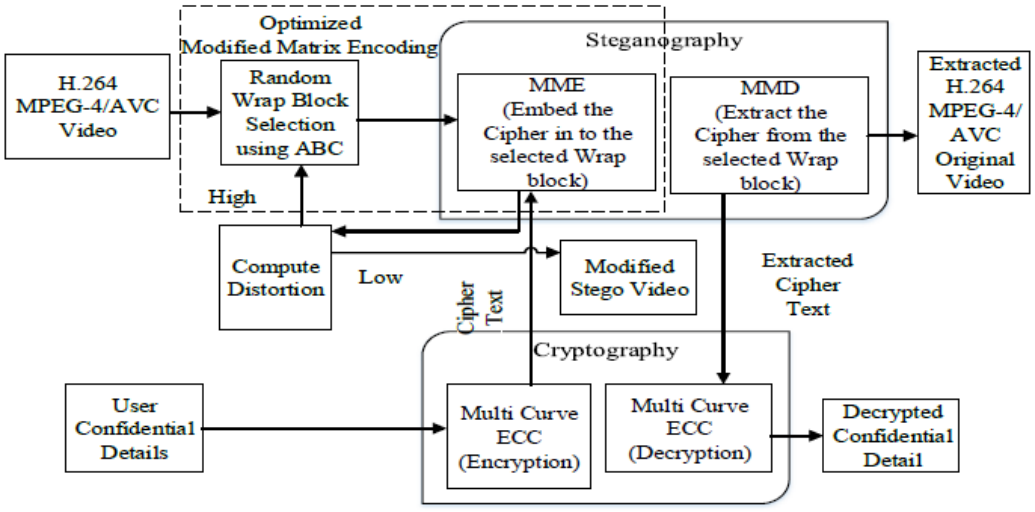

Figure 1: Representation of Proposed work.

Figure 1 presents a diagrammatic representation of the suggested framework. In this context, we use the Optimised Modified Matrix Encoding (OMME) steganographic technique, a well recognised method, to conceal confidential codes inside a video clip. This approach is chosen for its enhanced

International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Available online at: www.jrrset.com
ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395
Volume 9, Issue 1 - January 2020-2021 - Pages 101-108

level of security. We have enhanced the security and resilience of the cryptographic algorithm ECC by using a range of elliptic curves. Using several elliptic curves to generate the code enhances the security of the encrypted client data. In the modified matrix encoding approach, all the pixels of the image are altered using undisclosed information. In this context, a significant amount of distortion occurs in the resulting stego-image, which Steganalysis may easily detect. Therefore, it is necessary to use selected pixels to embed the coded text into the image. The ABC streamlining calculation is used for this selection of pixels.

Multi curve ECC for encryption.

Within the context of Elliptic Curve Cryptography (ECC), mathematical functions are expressed using an elliptical curve. In the context of encryption, the public key is represented as a point on the curve, while the private key is a randomly generated integer. Current systems use a single elliptic curve, however our suggested system will include many curves. The primary objective of this study is to determine the validity of using Elliptical Curve Cryptography (ECC) with numerous elliptic curves. Figure 2 illustrates the progression of ECC. Employing numerous elliptic curves enhances the security of the system while maintaining its performance characteristics unaffected. There is no need to alter the key length while using several elliptic curves for encryption. The use of multi-stage encryption enhances the system's resilience.

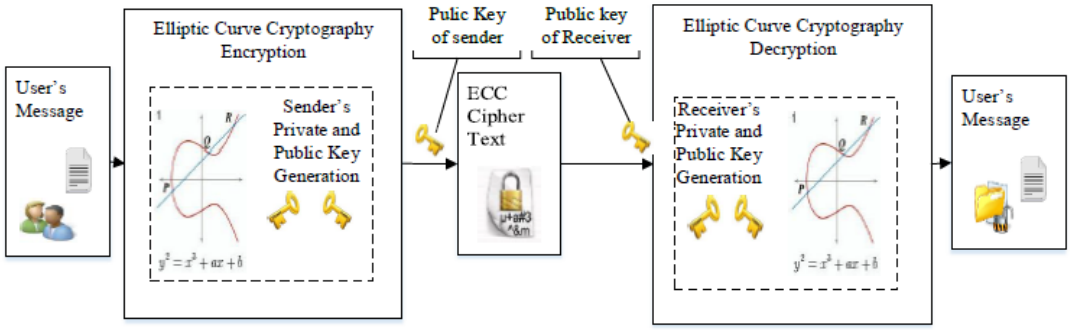

Figure 2: Process flow of ECC

Results and Discussions

This section discusses the recreational outcomes of the suggested security process using multi-curve ECC and an enhanced modified grid encoding technique that may be used for authentication and security purposes. The procedure described in this paper has been implemented in the MATLAB version 8.3 software. The results of the simulation using this proposed method have been compared with the performance of previous work. The previous work involved using conventional ECC cryptographic algorithms to encrypt user data and an improved network encoding technique to embed figures into digital images.

International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Available online at: www.jrrset.com
ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395
Volume 9, Issue 1 - January 2020-2021 - Pages 101-108

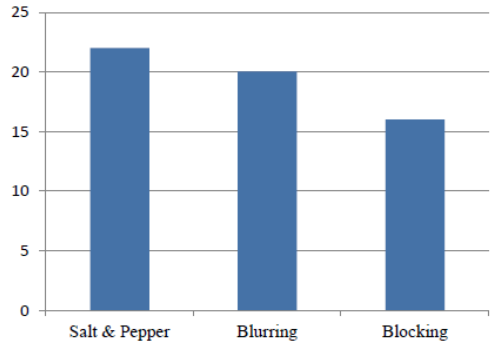

Fig 3: PSNR Attacks.

The comparison chart shown in Figure 3 illustrates the assaults and their accompanying Peak Signal-to-Noise Ratio (PSNR) values obtained using our suggested technique. Figures 4 and 5 show the Mean Squared Error (MSE) value and the Enhanced Structural Similarity Index Measure (ESIM) value for both the current and new systems. There is evidence of enhancement in the suggested system.

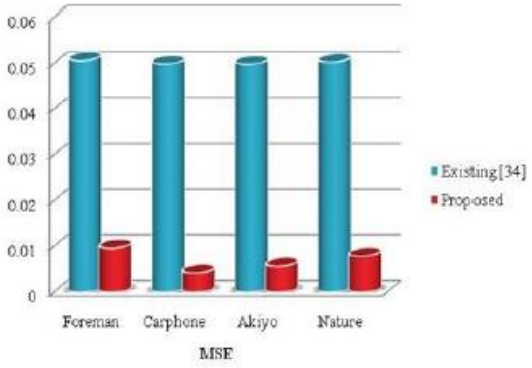

Fig 4: MSE values for Existing and Proposed method

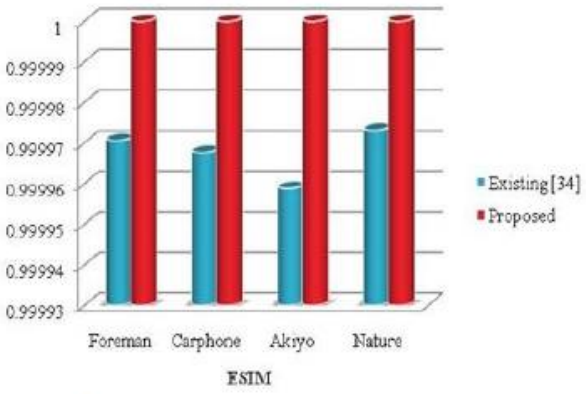

Fig 5: ESIM value for existing and proposed systems

International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Available online at: www.jrrset.com
ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395
Volume 9, Issue 1 - January 2020-2021 - Pages 101-108

Conclusion

This study introduces the notion of compression and encryption as effective solutions to the security dilemma. The LZW data compression technology, known for its lossless properties, was used to improve the capacity of the message being concealed. For enhanced security, the communication is encrypted and decoded using Multiple Elliptic Curve Cryptography (ECC). This paper presents a cryptographic technique that combines a multi-curve elliptic curve cryptography (ECC) with an optimised modified matrix encoding steganography technique. The purpose of this technique is to encrypt users' secret data and embed the cypher into digital photographic images. The implemented results of this proposed technique are compared with the conventional ECC technique for encryption. This effort aimed to enhance the resilience and security of an existing security approach. The findings of the suggested system have shown the efficacy of this multi-curve ECC approach, which may be utilised in smart card technology for future security purposes.

References

[1]. Ju, Song. A lightweight key establishment in wireless sensor network based on elliptic curve cryptography. In Intelligent Control, Automatic Detection and High-End Equipment (ICADE), 2012 IEEE International Conference on, 138-141.IEEE, 2012

[2]. Hegde, R. and Jagadeesha, S. An optimal modified matrix encoding technique for secret writing in MPEG video using ECC. Computer Standards & Interfaces 48 (2016) 173-182

[3]. Raghav P, Dua A. Security and Cryptography in Images and Video Using Elliptic Curve Cryptography (ECC). InCryptographic and Information Security Approaches for Images and Videos 2018 Dec 7 (pp. 141-170). CRC Press.

[4]. Mustafa G, Ashraf R, Mirza MA, Jamil A, Muhammad. A review of data security and cryptographic techniques in IoT based devices. InProceedings of the 2nd International Conference on Future Networks and Distributed Systems 2018 Jun 26 (pp. 1-9).

[5]. Khan MA, Quasim MT, Alghamdi NS, Khan MY. A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data. IEEE Access. 2020 Mar 13;8:52018-27.

[6]. Mohamed NN, Yussoff YM, Saleh MA, Hashim H. Hybrid cryptographic approach for internet ofhybrid cryptographic approach for internet ofthings applications: A review. Journal of Information and Communication Technology. 2020 Jun 11;19(3):279-319.

[7]. Hegde R, Soumyasri SM. Novel technique for securing iot systems by using multiple ECG and ceaser cipher cryptography. Int. J. Comput. Sci. Mob. Comput.(IJCSMC). 2021;10(2):1-8.