Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 10, Issue. 2, February 2021, pg.1 – 8

Novel Technique for Securing IoT Systems by using Multiple ECC and Ceaser Cipher Cryptography

Ramakrishna Hegde[1]; Soumyasri S M[2]
Associate Professor, Dept. of Computer Science & Engineering, Vidyavardhaka College of Engineering Mysuru, Karnataka, India
Assistant Professor, Dept. of Computer Science, Vidyhaashrama College, Mysuru, Karnataka, India
ramhegde111@gmail.com; drsoumyasrism@gmail.com
DOI: 10.47760/ijcsmc.2021.v10i02.001

Abstract: ***The Internet of Things (IoT) is one of the emerging technologies that has grabbed the attention of researchers from academia and industry. In near future IoT is expected to be seamlessly integrated into our environment and human will be wholly solely dependent on this technology for comfort and easy life style. Any security compromise of the system will directly affect human life. Privacy and security in IoT, is proven one of the most challenging areas. As we know that, the IoT devices have constraints like low power and less computational speed and the traditional encryption algorithm seems not feasible for IoT devices. So, we need to develop Lightweight encryption algorithm for IoT devices for secure communication and secure data transmission in IoT environment. Current cryptographic models and security schemes are based on widely adopted encryption algorithms, and privacy standards. Confidentiality is ensured in most of the cases with Advanced Encryption Standard (AES). Alternatively, Diffie-Hellman (DH) and Multi Curve Elliptic Curve Cryptography (ECC) supplement the privacy schemes, basically in asymmetric cryptography. Since the applicability of these cryptographic models and security schemes is a little bit unclear, detailed analysis is needed, in order to be ensured, that they can be implemented in the specified resources of IoT. Especially in the case, of minimized capabilities of hand-held and portable devices another very important and effective cryptographic technique can be used is Novel Caesar cipher method is the public key cryptography technique. This method includes two statics (i.e. encryption and decryption). Encryption on Ceaser cipher changes the word in the text with another word and original text is replaced with another word. Then the cipher text can be generated. In order to achieve better results, there is an ongoing research for more flexible cryptographic suites. Special interest has been attracted by the security schemes of combined mode that supports probably encryption and authentication.***
Keywords: Cryptography, Internet of Things, Multi Curve ECC, Elliptic Curve Cryptography, Ceaser Cipher Cryptography

1. INTRODUCTION

The *Internet of Things* (IoT) is one of the emerging technologies that has grabbed the attention of researchers from academia and industry. The idea of the Internet of Things (IoT) is to connect or give access to everything to the Internet. IoT environment not only provides the facility of Human to Machine connectivity, however, it also creates Machine to Machine connectivity. In future most of the devices are connected through IoT and human beings are going to be depends heavily on electron gadgets. Since IoT market is growing extremely fast during last five five years. IoT is going to be next big technology in future. Since most of the day to day

activities including personal management and business managements are connected with IoT technologies one or the other ways. Many critical transactions will happen by using IoT technologies. Any security compromise of the system will directly affect human life. Privacy and security in IoT, is proven one of the most challenging areas. As we know that, the IoT devices have constraints like low power and less computational speed and the traditional encryption algorithm seems not feasible for IoT devices. So, we need to develop Lightweight encryption algorithm for IoT devices for secure communication and secure data transmission in IoT environment.

2. RELATED WORKS

Current cryptographic models and security schemes are based on widely adopted encryption algorithms, and privacy standards. Confidentiality is ensured in most of the cases with Advanced Encryption Standard (AES)[8]. Alternatively, Diffie-Hellman (DH)[6] and Multi Curve Elliptic Curve Cryptography (ECC) supplement the privacy schemes, basically in asymmetric cryptography. Since the applicability of these cryptographic models and security schemes is a little bit unclear, detailed analysis is needed, in order to be ensured, that they can be implemented in the specified resources of IoT. Especially in the case, of minimized capabilities of hand-held and portable devices. Elliptic Curve Cryptography is a promising asymmetric cryptographic algorithm with an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields [1]. Ramakrishna Hegde [2] have proposed a multi-bend ECC based cryptographic system joined with an optimized modified grid encoding steganography procedure was utilized to encrypt the client's mystery information. An artificial bee colony calculation was utilized in order to embed the cipher-text into H.264 video and executed outcomes of proposed procedure had been compared with LSB steganography and ordinary FMO system.

The entire security of ECC depends on the ability to compute a point multiplication and the inability to compute the multiplicand given the original and product points [3]. The ECC standards are specified in SEC, Standards for Efficient Cryptography [4]. Elliptic curve cryptography was introduced in the mid-1980s independently by Koblitz and Miller [5]. This research work is very promising alternative for cryptographic protocols based on the discrete logarithm problem in the multiplicative group of a finite field (e.g., Diffie-Hellman key exchange [6] or ElGamal encryption/signature [7]

3. SECURITY CHALLENGES FOR IoT

I. Insufficient testing and updating

- The primary source of most IoT security issues is that manufacturers do not spend enough time and resources on security.
- device that was once thought of as secure when the customers first bought it becomes insecure and eventually prone to hackers and other security issues.
- For example, most fitness trackers with Bluetooth remain visible after the first pairing, a smart refrigerator can expose Gmail login credentials, and a smart fingerprint padlock can be accessed with a Bluetooth key that has the same MAC address as the padlock device.
- This is precisely one of the biggest security issues with IoT.
- The following are some security risks in IoT devices from manufacturers:

- Weak, guessable, or hard-coded passwords
- Hardware issues
- Lack of a secure update mechanism
- Old and unpatched embedded operating systems and software
- Insecure data transfer and storage

- **Reason:**
  - IoT manufacturers are more eager to produce and deliver their devices as fast as they can, without giving security too much of a thought.
  - most manufacturers offer firmware updates only for a short period of time, only to stop the moment they start working on the next headline-grabbing gadget. They use unsupported legacy Linux kernels.
  - lack of universal IoT security standards, manufacturers will continue creating devices with poor security
  - Manufacturers that started to add Internet connection to their devices do not always have the "security" concept as the crucial element in their product design process.
- This leaves their trusted customers exposed to potential attacks as a result of outdated hardware and software.
- **Solution:** To protect their customers against such attacks, each device needs proper testing before being launched into the public and companies need to update them regularly.

II. Lack Of User Knowledge & Awareness.

- One of the biggest IoT security risks and challenges is the user's ignorance and lack of awareness of the IoT functionality. As a result, everybody is put at risk.
- Tricking a human is, most of the time, the easiest way to gain access to a network.
- A type of IoT security risk that is often overlooked is **social engineering attacks**. Instead of targeting devices, a hacker targets a human, using the IoT.
- Social engineering was used in the 2010 Stuxnet attack against a nuclear facility in Iran. The attack was directed to industrial programmable logic controllers (PLCs), which also fall into an IoT device category.
- The attack corrupted 1,000 centrifuges and made the plant explode. I
- t is believed that the internal network was isolated from the public network to avoid attacks, but all it took was a worker to plug a USB flash drive into one of the internal computers.

III. Data Integrity Risks Of IoT Security In Healthcare

- With IoT, data is always on the move. It is being transmitted, stored, and processed.
- Most IoT devices extract and collect information from the external environment. It can be a smart thermostat, HVAC, TVs, medical devices.

- Sometimes these devices send the collected data to the cloud without any encryption.
- As a result, a hacker can gain access to a medical IoT device, gaining control over it and being able to alter the data it collects.
- A controlled medical IoT device can be used to send false signals, which in turn can make health practitioners take actions that may damage the health of their patients.
- For example, a hacked medical IoT device can report a fully charged battery to the maintenance station while in reality the battery is about to die. Worse, there are risks of IoT security in healthcare devices like pacemakers or the ones making the insulin shots.
- The vulnerabilities found on St. Jude Medical's implantable cardiac gave access to hackers, enabling them to alter the pacing or shocks, or even worse, deplete the battery.

IV. Home Invasions

- One of the scariest threats that IoT can possess is of the home invasion.
- Nowadays, IoT devices are used in a large number at homes and offices which has given rise to the home automation.
- The security of these IoT devices is a huge matter of concern as it can expose your IP address that can pinpoint to your residential address.
- This vital information can be sold by the hackers to the underground websites which are havens for criminal outfits.
- if you're using IoT devices in your security systems, then there is a possibility that they might compromise as well as leave your house at a huge potential threat.

V. Untrustworthy Communication

- There are many IoT devices which send messages to the network without any encryption.
- companies must ensure encryption of the highest level among their cloud services and devices.
- The best way to do is to use transport encryption and standards like TLS. Another way is to use different networks that isolate different devices.
- On October 2016, a hacker found vulnerability on a specific model of security cameras. Nearly 300,000 Internet of Things (IoT) video recorders started to attack multiple social network websites and brought down Twitter and other high-profile platforms, for almost two hours.
- This attack is just an example of what can happen to IoT devices with poor security.
- It is not only video cameras, but anything with an internet connection, from a refrigerator, smart locks, thermostats, lightbulbs, vehicles, and even smart toys. Using them always poses IoT security challenges and risks to overcome.

4. Modified Caesar Cipher Cryptography for Encrypting Secret Message

The one of the efficient public key cryptography technique is Modified Caesar Cipher Method and in our work we are using this technique for encrypting the control message sent by the user to the desired IoT devices. This method includes two statics (i.e encryption and decryption). Encryption on Ceaser cipher changes the word in the text with another word. In which n is the original text then this n is replaced with another word. Then the cipher text can be obtained through the following equation (1)

$$C_{I=} P_{I+} t \quad (1)$$

In this above equation C_i is the cipher text, P_i is the original plain text, and key is denoted as t. Deciphering process is held through the inverse function of the encryption and it can be given in the following formula (2)

$$P_{i} = C_{i-} t \quad (2)$$

After encrypting the message, it will be communicated over the networks and this is for the efficient security consideration. Finally this message will be decrypted in the other end.

5. Multi- Curve ECC

One of the very efficient and secure cryptographic algorithm Elliptic Curve Cryptography (ECC) is an public key Cryptography. This algorithm is based on the structure of elliptic curves over fine fields[1]. The main advantage of ECC is that, compare to other cryptographic, ECC requires smaller key size. This is very useful for implementing encryption on small devices with limited resources in terms of power, CPU and memory. Also it helps in application such as handling of many sessions of large web servers. The strength of an asymmetric encryption algorithm such as ECC is found in the complexity of computing the inverse of the function used to generate the key. Creating the key is very simple and straight forward. But identifying the inputs that were used to create the key is computationally infeasible. In ECC, the computationally extraordinary issue is designated "Elliptic Curve Discrete Logarithm Problem", and includes the trouble in processing the discrete logarithm (type) from the outcome. Furthermore, there are numerous advanced cryptographic algorithms which utilizes ECC cryptosystem as a base creation it a perfect decision. Cryptography for encoding client's mystery information changed over into scrambled code was performed utilizing Elliptic Curve Cryptography (ECC).

6. Modelling of ECC and Optimized Modified Matrix Encoding (OMME)

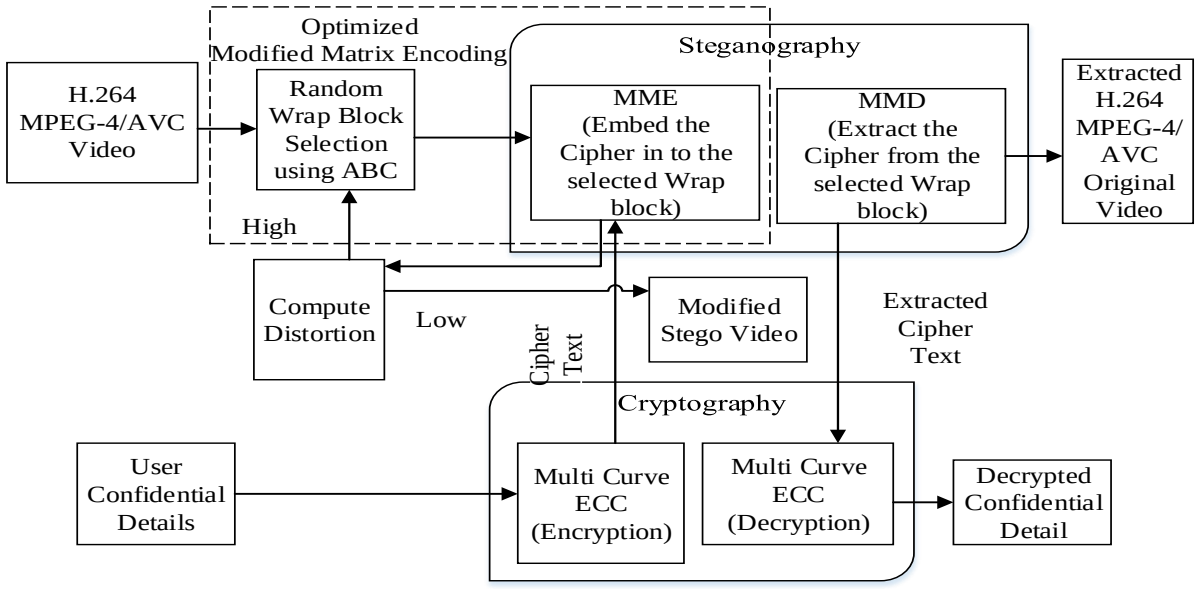

Figure 1: Representation of Proposed work.

The schematic portrayal of the proposed framework is given in Fig 1. Here we make use of one of the well-known Optimised Modified Matrix Encoding (OMME) steganographic algorithm to hide the secret codes in into Video file to achieve better security. We have improved the security and robustness of the cryptographic method ECC by utilizing various elliptic curves.. Utilizing various elliptic curves for producing the code improves the strength of encoded mystery information of client. Generally in modified matrix encoding method, all the pixels of the picture are adjusted with mystery information. Along these lines, a ton of contortion happens in coming about stego-picture, which could be handily distinguished by Steganalysis. Consequently, chose pixels must be utilized to insert the code text into spread picture. For this choice of pixels, ABC streamlining calculation is utilized.

7. Encryption using Multi curve ECC

In ECC, the mathematical functions are represented over an elliptical curve. For encryption, the point on the curve represents the public key and any chosen random number will be private key. In existing systems, single elliptic curve are used but in our proposed system we will consider multiple curves. The main purpose of this research is to finding the rightfulness of using Elliptical Curve Cryptography (ECC) with multiple elliptic curves. The flow of ECC is given in Fig 2. The usage of multiple elliptic curve increases the security of the system without affecting any of its performance parameters. There is no need for any change in the key length because of using multiple elliptic curves for encryption. This encryption at multi-stage makes the system robust.

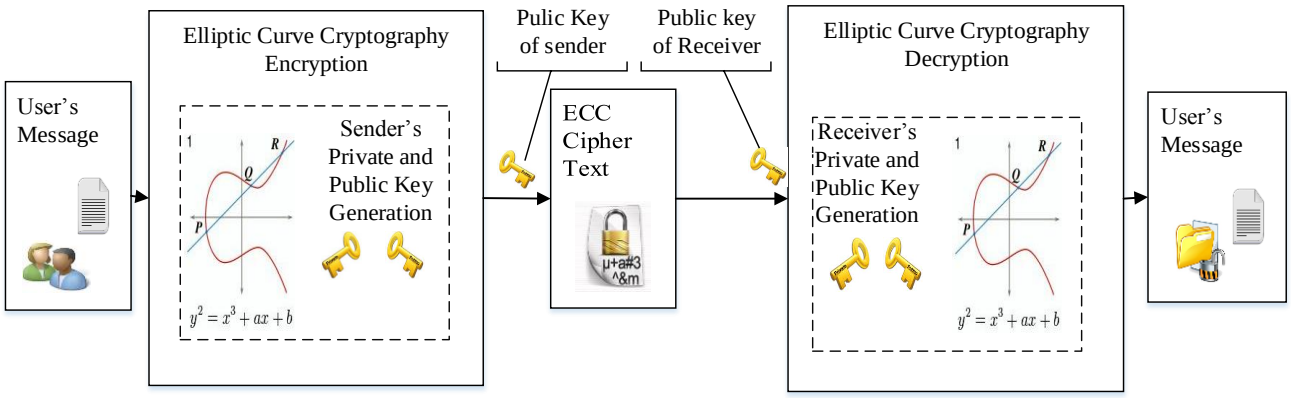

Figure 2: Process flow of ECC

8. Results and Discussions

This area clarifies the recreation consequences of the proposed procedure for security utilizing multi-curve ECC and an improved altered grid encoding method that can be actualized for verification and security. The procedure talked about in this paper has been re-enacted in the working foundation of MATLAB adaptation 8.3 and the recreation aftereffects of this proposed strategy has been contrasted and the exhibition of the past work which has utilized in regular ECC cryptographic calculation to scramble client information and upgraded adjusted network encoding method for implanting figure into computerized photographic picture.

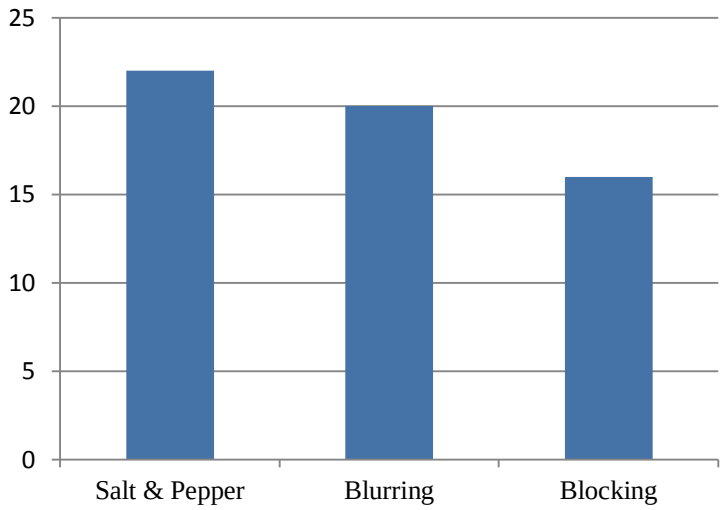

Fig 3: PSNR Attacks.

The comparison chart shown in Fig 3 demonstrate the attacks and their corresponding PSNR of our proposed method. Fig. 4 and Fig 5 shows the MSE value and ESIM value for existing and proposed systems. It shows that there is an improvement in proposed system.

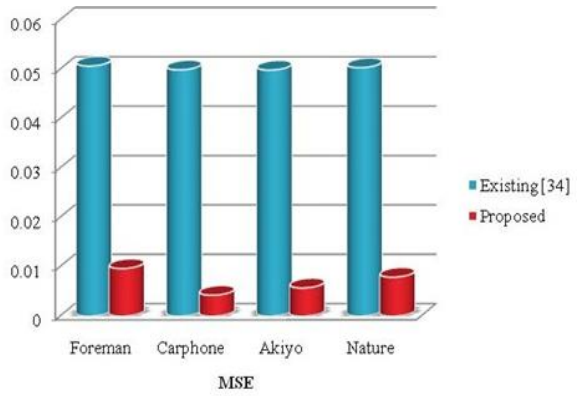

Fig 4: MSE values for Existing and Proposed method

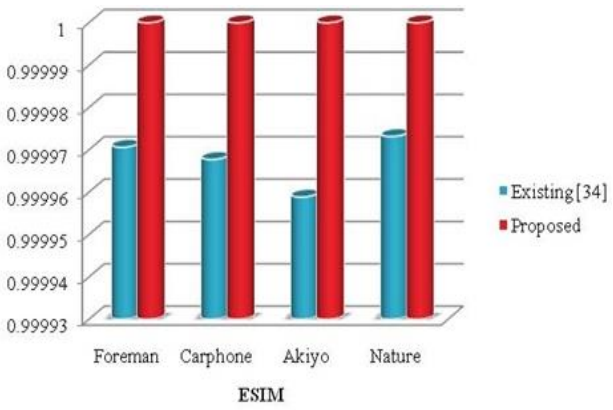

Fig 5: ESIM value for existing and proposed systems

9. Conclusion

This research brings to light the concept of adequately, compression and cryptography which is the scientific remedy to the security problem. A lossless compression algorithm prevalently called LZW data compression was utilized on the message to be covered up to increase the capacity. Thus for the higher security, the message is encrypted and decrypted using Multiple ECC. In this paper, a multi-curve ECC based cryptographic technique combined with an optimized modified matrix encoding steganography technique to encrypt users secret data and then to embed the cipher into digital photographic image was explained and the implemented results of the proposed technique has been compared with conventional ECC technique for encryption. This work was driven towards additional robustness and security to existing security technique. The results of the proposed system have proved the effectiveness of this multi-curve ECC technique which can be implemented in smart card technique for security purpose in future.

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]. http://en.wikipedia.org/wiki/Elliptic_curve_cryptography.

[4]. Certicom, Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, Version 1.0, September 2000

[5]. Victor S. Miller. Use of elliptic curves in cryptography. In H.C. Williams, editor, Advances in Cryptology CRYPTO'85, vol. 218 of Lecture Notes in Computer Science, pp. 417-426. Springer-Verlag, 1986.

[6]. Whitfield Diffie and Martin E. Hellman. New directions in cryptography, IEEE Transactions on Information Theory, 22(6):644-654, 1976.

[7]. Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(4):469- 472, 1985.

[8]. Abdullah, Ako. (2017). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data.

