ISSN 2347 - 3983

Volume 8. No. 5, May 2020

International Journal of Emerging Trends in Engineering Research

Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter111852020.pdf

https://doi.org/10.30534/ijeter/2020/111852020

Network Security using Notable Cryptographic Algorithm for IoT Data

Muzammil Parvez M[1], R. S. Ernest Ravindran[2], Syed Inthiyaz[3], Ch. Tejkumar[4], K. Veera Ram Sai[5], K. Ashok Shiva Reddy[6]

Assistant Professor[1], Associate Professor[2,3], Student[4,5,6]

[1,2,3,4,5,6] Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur.

ABSTRACT

Internet of Things (IoT) performs an imperative job within the field of Information Technology, Industries as well as Healthcare etc. As information within IoT application would be identified with the physical domain, guaranteeing information safety is an essential requirement for some cases. Since in the IoT setting clients, yet in addition approved articles may get to data. Security speaks to a basic part for empowering the across the board reception of IoT innovations, and applications. In this way this paper proposes a staggered encryption procedure to upgrade the security of the IoT information. In this methodology the information detected from the IoT gadgets are scrambled in the entryway utilizing Merkle-Hellman encryption and Elliptic Curve Cryptography (ECC), to guarantee the security of the information.

Key words: Internet of Things, Data Security, ECC, Merkle-Hellman Cryptosystem

1. INTRODUCTION

Internet of Things (IoT) [6] is a more current innovation in this quickest world. Any physical articles like telephone, PC, fridge, printer, air cooler and so on are considered as keen things. IoT can be characterized as a system of extraordinarily recognizable, available, and reasonable keen things that are equipped for performing correspondence, calculation and extreme choice making. "It is a unified part of Future Internet in addition to could be categorized as a unique worldwide system outline with self-arranging skills reliant on on typical and interoperable communication conventions where corporeal as well as simulated things have characters, credited in physical, utilize astute interfaces, along with are consistently corresponding into the data organize.

IoT [7] expects segments to empower correspondence between gadgets, for example, remote associations like Sensors, Bluetooth, RFID, ZigBee, WSN, WMAN, Wifi or WLAN. Sensor information is a [7] fundamental part of loT framework, moreover it shares data to outsiders to profit useful services as well as applications like, location-based services, keen home administration in addition to old checking etc. IoT information properties produce numerous information the executives' issues [3], for example, versatility of information, interoperability, getting to information, information filing so forth. IoT information stockpiling can be nearby, appropriated as well as brought together. Here, information security is very challenging due to the various information properties. Giving information security to the gushing or detected information is a significant issue, [3], in IoT. To utilize gadget correspondence successfully, we have to improve the security. Cryptography [4] is a compelling method to ensure the delicate data. This paper proposes a staggered encryption for IoT information utilizing Merkle-Hellman Knapsack cryptosystem along with ECC. ECC is appropriate for IoT applications [5], that need long haul security necessities. Additionally, Elliptic bends offers elevated level of security as well as smaller the key length. Subset issue,[3], is made in Merkle Hellman rucksack cryptosystem to encode the information. Henceforth, the calculation is basic productive.

The art and knowledge of hiding the messages to introduce privacy in information security is recognized as cryptography. [6] Cryptography is the skill of safeguarding information, cryptanalysis is the skill of examining and breaking protected communication. Classical cryptanalysis includes an exciting grouping of logical reasoning, mathematical application tools, shape outcome, persistence, willpower, and blessing. Cryptanalysts are also named as attackers. Cryptology holds both cryptography and cryptanalysis[15]. The known parameters in the cryptography is Confidentiality, Data integrity, Authentication, Non-repudiation and is shown in figure-1.

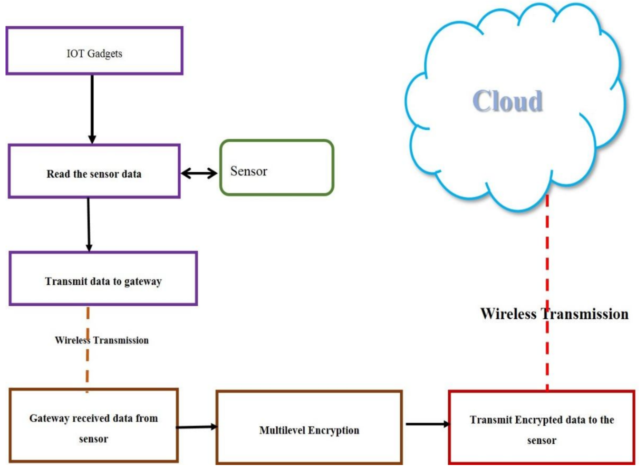


Figure 1: Overall process of Cryptography algorithm

2. METHODOLOGY

2.1 Existing Model

Till now the most popular algorithm is RSA “Rivest, Shamir, Adleman” algorithm, this algorithm is best for its security concerns, but it is very slow on reality [8]. To overcome this problem and to improve the security we tend to design this new model[16].

This new proposed model will increase the security to certain level that is greater than the RSA and this new model will reduce the time take to encrypt the data in compared to the existing model[14]. In this methodology, a multi-level encryption strategy (Merkle- Hellman Knapsack cryptosystem with Elliptic Curve Cryptography),[2], is utilized. The motivation behind the planned method is to verify the information detected from the IoT, [7] gadgets.

The model of the planned approach. Information from the IoT [5], gadgets will be sent to the entryway utilizing conventions, for example, CoAP as well as HTTP over the web. When information is gotten by the entryway, it is set up for transmission to the server. Before the information being transmitted to the server, they are encoded utilizing staggered encryption procedure [9].

2.2 System Model of Proposed Approach:

2.2.1. Elliptic Curve Cryptosystem

Elliptic Curve Cryptography (ECC), [2] is people in general key cryptography [4] approach utilized for information encryption. Neal Koblitz along with Victor Miller planned elliptic bends in 1985 to plan open key cryptographic frameworks [4]. This tackles the significant issue, [3] of open key cryptography by furnishing elevated level security with less key length. An Elliptic Curve,[2] is a plane bend characterized by a condition.

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

A standard type of elliptic bend E over limited field Fp (p is an enormous prime number) is processed by utilizing the accompanying condition.

$$= x^3 + ax + b \ (mod\ p)$$

At that point, the strategy includes picking two non-negative whole numbers a, b which are not as much as p with the end goal that, it fulfills the condition.

$$4a^3 + 27b^2 (mod\ p) \neq 0$$

2.2.2. Merkle Hellman Knapsack Cryptosystem:

Ralph Merkle along with Martin Hellman imagined the super increasing subset issue [3], in the year 1978. It endeavors to mask an effectively tackled occurrence of the subset issue called super increasing subset entirety issue, by measured duplication a stage [13].

The idea of super increasing request is covered up by vector v1usingmodular augmentation and a stage, and afterward the super cumulative vector is spoken to by v[10]. The contorted vector shapes the encoded message. The first super increasing vector shapes the private key which is utilized to decode the message[12].

Key Generation:

Phase 1: Both sender and receiver agree with the base point P.

Phase 2: Private Key = d, pubic key Q = d * P

Encryption

Phase 1: Select an elliptic curve Ep(a, b). E has N points on it

Phase 2: Pure text has to represent on the curve

Phase 3: Randomly select ‘d’ from [1-(n-1)]

Phase 4: Consider message ‘m’ has the point ‘M’ on the curve ‘E’

Phase 5: Two (2) cipher texts will be generated C1 = d *p, C2 = M + d * Q.

2.2.3. Multilevel Encryption Technique:

The planned staggered encryption system performs encryption in two stages.

Firstly, the given plain content is separated by every character as well as afterward converts it into its equal paired qualities. Double esteems are then scrambled utilizing Merkle-Hellman encryption system. Mainly, it is to produce a subset issue [3], which can be illuminated smoothly. Here, by utilizing particular portrayal with change the very expanding nature can be covered up.

The Merkle-Hellman encryption technique is given underneath.

Step 1: Choose super increasing sequence of positive integers. Where each numbers is larger than the totality of all previous numbers s=(s1,s2,s3,…..sn)

Step 2: convert each character of the plain text into binary equivalent represented by b.

Step 3: choose an integer (a) which is larger than the totality of all numbers in the classification s and its co-prime (r)

Step 4: The sequence s and the numbers a and r form the private key of the cryptosystem.

Step 5: All the elements in the sequences are multiplied with number rand the modulus of the multiple is taken by dividing with the number a.

Step 6: pi = si* r mod (a), where all the elements in the sequence pare multiplied with the conforming elements of the binary sequence b and then adding the resulting sum.

Step 7: The encrypted Message is M = $\sum pi*bi$

Secondly, these scrambled characters are additionally encoded by elliptic bend cryptography (ECC). ECC is used to

produce the figure content of the outcome gave by Merkle-Hellman encryption[17]
All the steps are shown as flow chart in figure-2.

2.3. Flow Chart

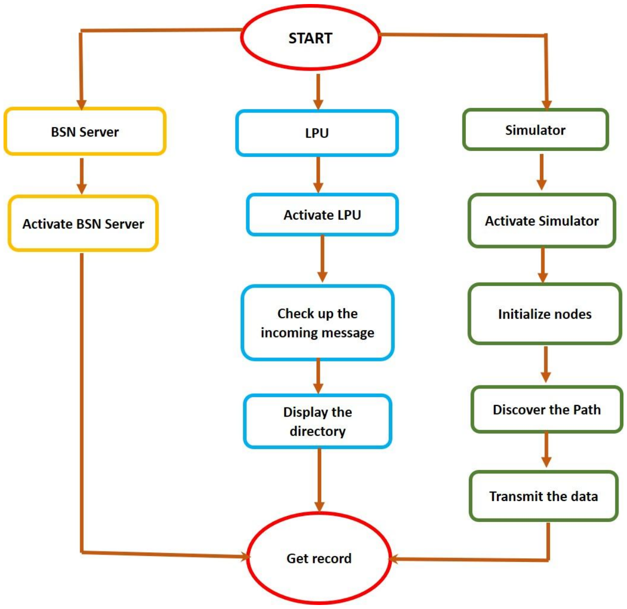
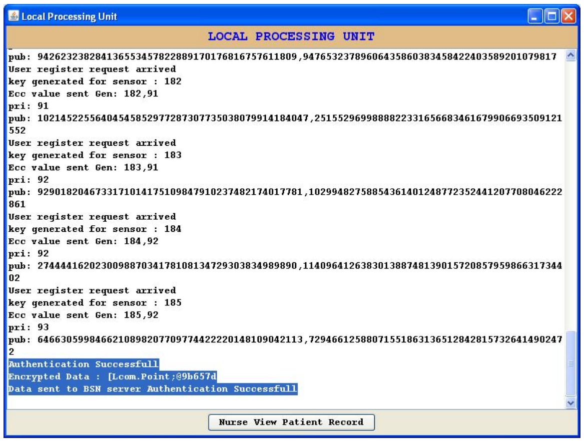


Figure 2: Flow Chart

3. RESULTS AND DISCUSSION

In this planned methodology, the information is verified by applying two distinctive encryption systems, for example, Merkle-Hellman backpack cryptosystem with Elliptic bend Cryptography [1]. With these strategies, the information could be shared safely.

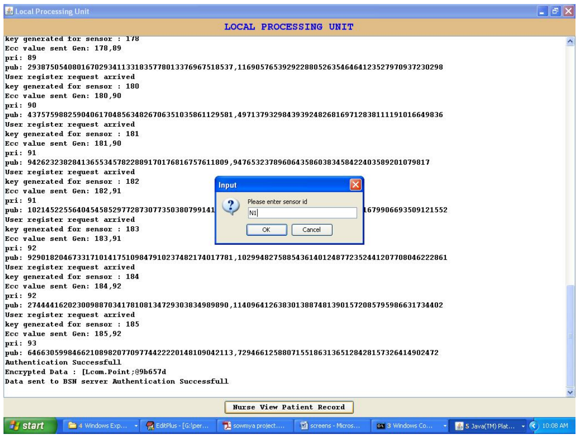
Now we can see encrypted data at LPU screen at bottom of the screen as in figure-3.



```
pub: 94262323828413655345782288917017681675761 1809,947653237896064358603834584224035892010 79817
User register request arrived
key generated for sensor : 182
Ecc value sent Gen: 182,91
pri: 91
pub: 10214522556404545852977287307735038079914184047,251552969988882233165668346167990669350912 1
552
User register request arrived
key generated for sensor : 183
Ecc value sent Gen: 183,91
pri: 92
pub: 92901820467331710141751098479102374821740177 81,102994827588543614012487723524412077080462 22
861
User register request arrived
key generated for sensor : 184
Ecc value sent Gen: 184,92
pri: 92
pub: 27444416202300988703417810813472930383498989 0,114096412638301388748139015720857959866317344
02
User register request arrived
key generated for sensor : 185
Ecc value sent Gen: 185,92
pri: 93
pub: 64663059984662108982077097744222201481090421 13,729466125880715518631365128428157326414902 47
2
Authentication Successfull
Encrypted Data : [Lcom.Point;@9b657d
Data sent to BSN server Authentication Successfull
```

Figure 3: Local Processing unit screen after encryption

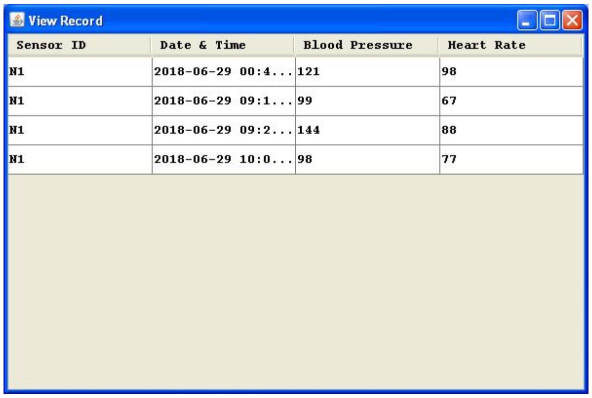
Now nurse al LPU screen can obtain data from BSN server in figure-4 by clicking on 'Nurse View Patient Record' button.



```
key generated for sensor : 178
Ecc value sent Gen: 178,89
pri: 89
pub: 29387505408016702934113318357780133769675185 37,116905765392922880526354646412352797093723 0298
User register request arrived
key generated for sensor : 180
Ecc value sent Gen: 180,90
pri: 90
pub: 43757598825904061704856348267063510358611295 81,497137932984393924826816971283811119101664 9836
User register request arrived
key generated for sensor : 181
Ecc value sent Gen: 181,90
pri: 91
pub: 94262323828413655345782288917017681675761180 9,947653237896064358603834584224035892010798 17
User register request arrived
key generated for sensor : 182
Ecc value sent Gen: 182,91
pri: 91
pub: 102145225564045458529772873077350380799141                            1679906693509121552
User register request arrived
key generated for sensor : 183
Ecc value sent Gen: 183,91
pri: 92
pub: 92901820467331710141751098479102374821740177 81,102994827588543614012487723524412077080462 22861
User register request arrived
key generated for sensor : 184
Ecc value sent Gen: 184,92
pri: 92
pub: 27444416202300988703417810813472930383498989 0,114096412638301388748139015720857959866317 34402
User register request arrived
key generated for sensor : 185
Ecc value sent Gen: 185,92
pri: 93
pub: 64663059984662108982077097744222201481090421 13,729466125880715518631365128428157326414902 472
Authentication Successfull
Encrypted Data : [Lcom.Point;@9b657d
Data sent to BSN server Authentication Successfull
```

Figure 4: Nurse Screen to retrieve the patient data

Here N1, N2, N3….. are the patients or sensors id as shown in figure-5.



Sensor ID	Date & Time	Blood Pressure	Heart Rate
N1	2018-06-29 00:4...	121	98
N1	2018-06-29 09:1...	99	67
N1	2018-06-29 09:2...	144	88
N1	2018-06-29 10:0...	98	77

Figure 5: Given patients reading

4. CONCLUSION

The target of the planned work is to improve the security of the IoT information, that are detected by the IoT gadgets [19]. This is accomplished by the planned staggered encryption. The information is scrambled in the entryway before putting away it in the server cloud. Encryption of information is performed in two (2) phases. In the main stage, Merkle-Hellman rucksack cryptosystem is utilized to encode the information [20]. In the subsequent stage, the scrambled content goes about as a contribution for ECC. At last, they got ciphertext content is sent to the cloud server. This approach guarantees the protection of the information plus develops computation time.

REFERENCES

1. Koblitz.N, “Elliptic Curve Cryptosystems”, “Mathematics of Computation”,MathSciNet review:866109, 1987, Vol. 48, Iss. 177, pp. 203-209.
2. Miller.V, “Use of Elliptic Curves in Cryptography”, CRYPTO’85, Springer-Verlag, 1986, pp.417-426. https://doi.org/10.1007/3-540-39799-X_31
3. Parks R, Pennsylvania T. RFID privacy issues in healthcare: Exploring the Roles of Technologies and Regulations.”Journal of information and privacy” volume-6, 2010; 6(3):1–24.
4. Alfred J.Menezes, Paul C.van Oorschot and Scott A. Vanstone, “Handbook of Applied Cryptography”, Massachusetts Institute of Technology,3rd Edition 1996.
5. Isha and Ashish Kr. Luhach, “Analysis of Lightweight Cryptographic Solutions for Internet of Things”, Indian Journal of Science and Technology, 2016, ISSN: 0974-6846, Vol. 9(28), pp. 1-7. https://doi.org/10.17485/ijst/2016/v9i28/98382
6. Bojanova I, Hurlburt G, Voas J. Imagineering an Internet of Anything. Computer (Long Beach Calif). SERE-2014; 47(6):72–7
7. Behrens R,Ahmed A., Internet of Things: An End-to-End Security Layer. 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), IEEE, 2017, pp. 146-149. https://doi.org/10.1109/ICIN.2017.7899405
8. Sfar AR, Natalizio E, Challal Y, Chtourou Z., A Roadmap for Security Challenges in Internet of Things. “Digital Communications and Networks”, 2017 pp. 1-31.
9. Singh S, Sharma PK, Moon SY, Park JH., Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. “Journal of Ambient Intelligence and Humanized Computing, Springer, 2017, pp. 1-8. https://doi.org/10.1007/s12652-017-0494-4
10. Hossain MM, Fotouhi M, Hasan R., Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In Services (SERVICES), 2015 IEEE World Congress on 2015 June, 2015, pp. 21-28.
11. A. Safi, 2017," Improving the Security of Internet of Things Using Encryption Algorithms", International Scholarly and Scientific Research & Innovation [5]2017 S Koteshwar,2016 "Comparative study of Authenticated Encryption" targeting lightweight IoT applications, 2168-2356 (c) 2016 IEEE.
12. Dr. S. S. Manikandasaran, 2016,"Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage" (IJCSITS)ISSN: 2249-9555.
13. Vijayalakshmi, A., Ghali, V.S., Chandrasekhar Yadav, G.V.P., Gopitilak, V., Muzammil Parvez, M Machine learning based automatic defect detection in non stationary thermal wave imaging 2020 ARPN Journal of Engineering and Applied Sciences
14. Syed Shameem, G. R. K. Prasad, Muzamilparvez. M, U. Reshmi, G. Harshitha, K. Haritha Design and FEM model analysis of MEMS cantilever structure for detection of colon cancer using mass sensing 2019 Research Journal of Pharmacy and Technology. https://doi.org/10.5958/0974-360X.2019.00730.3
15. Vijaya Lakshmi, A., Ghali, V.S., Muzammil Parvez, M., Chandra Sekhar Yadav, G.V.P., Gopi Tilak, V. Fuzzy C-means clustering based anomalies detection in quadratic frequency modulated thermal wave imaging 2019 International Journal of Recent Technology and Engineering
16. Muzammil Parvez, M., Shanmugam, J., Mohan Rao, K.R.R., Lakshmana, C., Shameem, S. Alive node and network lifetime analysis of DEEC protocol and EDDEEC protocol 2018 Journal of Advanced Research in Dynamical and Control Systems.
17. Muzammil Parvez, M. Medical radiograph compression using neural networks and haar wavelet 2016 International Journal of Pharmacy and Technology.
18. Prasad, M.V.D., Inthiyaz, S., Teja Kiran Kumar, M., Sharma, K.H.S., Manohar, M.G., Kumari, R., Ahammad, S.H.” Human activity recognition using deep learning”, International Journal of Emerging Trends in Engineering Research 7(11), pp. 536-541. https://doi.org/10.30534/ijeter/2019/227112019
19. Inthiyaz, S., Madhav, B.T.P., Kishore, P.V.V.” Flower image segmentation with PCA fused colored covariance and gabor texture features based level sets”, Ain Shams Engineering Journal 9(4), pp. 3277-3291.
20. Inthiyaz, S., Madhav, B.T.P., Kishore Kumar, P.V.V.” Flower image segmentation: A comparison between watershed, marker controlled watershed, and watershed edge wavelet fusion”, ARPN Journal of Engineering and Applied Sciences 11(15), pp. 9382-9387.