Encryption and decryption of big data streams using Lightweight asymmetric method in WSN

GARGI N R[1*], BINO THOMAS[2]

[1]M techStudent, [2]Assistant Professor

Computer Science and Engineering

St Joseph's college of Engineering and Technology, Palai, Kottayam, kerala, India

ABSTRACT: Resource constrained devices are used in critical fields such as agriculture, smart health, industries and others. These devices produce an immense amount of data. These data streams are used for the analysis and making proper decision related to the applications. It is having restricted processing and storage capabilities which provide maximum data outcomes using less power consumption. An attacker may tamper or access data these data's and is one of the key challenges faced by these devices. These systems are vulnerable to different security threats. Various lightweight cryptographic methods are there for solving issues like authenticity, confidentiality and data integrity. Most of these methods provide security from the attacks, but was completely secure or take more time for performing the security related encryptions steps. In this paper, a lightweight asymmetric algorithm based on RSA with key extension is proposed to provide security to the data sources generated by WSN. The enhancement is RSA is done by changing the key generation method. The system will satisfy all the key security properties. Here the proposed system is compared with existing methods in the perspective of computation time. The comparison is done for finding the better method.

Keywords: Internet of Things (IoT), Rivest, Shamir, Adleman (RSA), Wireless multimedia sensor (WMSN), Wireless sensor networks (WSN),TEA(Tiny encryption algorithm)

I.INTRODUCTION

At present, Resource-constrained devices are commonly used in the Internet of Things (IoT). It is for information assortment and the format of getting admission to oversee conspiracy that allows a client as a piece of IoT. Wireless sensor networks(WSN) are an administered local area that incorporates a monstrous assortment of sensor hubs. It can aggregate the objective realities through the sensor hubs to get data [1]. These networks are used for basic applications like medical services, savvy urban areas, agriculture areas, mechanical control frameworks, and so on as sown in Fig [1].The work of WSNs has been accounted for help ranchers in different perspectives like the upkeep of wiring in a hazardous climate, water system motorization which helps more ingenious water use and decrease of squanders in agriculture sectors.WSNs can be used for checking the development of different primary ventures like structures and other infrastructural projects like flyovers, spans, streets, banks, burrows, and so on, permitting fabricating/designing practices to screen assets distantly without essentially visiting the locales, and this would lessen costs that would have been caused from actual site appearances in structural development and so forth.

The essential elements of a WSN, sensor hubs or the bits, have special residences that force novel necessities of WSN applications. Most widely is they conveying remotely, have little actual size, own low processing abilities, and capacity for the use of the batteries [2].Wireless sensor networks (WSNs) have rich large information streams: an enormous measure of information is created by different sources. It produces colossal measures of information on a regular schedule and sends them to the worker for investigation as information streams [3].The information delivered from a vast assortment of sources is flooding to the information stream administrator for its handling and taking appropriate choice for the basic applications [4]. Resource Sensor Networks (WSN) consolidates remote sensor hubs set up inside the area for the relentless proclamation of substantial or natural conditions. Data trustworthiness is a high initialization movement in WSN, because of cruel environmental factors producing faulty measurements and unreliable information switch over WSN. The earnest of the insights created from sensor hubs plays a crucial capacity to settle on indispensable choices [5].A sensor local area should not uncover the sensor readings to its encompassing networks. In many applications, hubs can convey gigantically fragile information. That information is encoding the information with a key for beneficiaries; however, key confirmation is extreme in remote sensor networks because of organizations [6]. Information respectability is the assurance that the records got with the guide of utilizing the place for getting away are the equivalent as that created with the guide of utilizing the stockpile and have now not, at this point been coincidentally or malignantly changed course. Trustworthiness attacks manage content material without the data or consent of the proprietor [7]. The biggest challenging tasks for these devices are to ensuring confidentiality and integrity with high information dependability.

In conventional cryptography, a cipher is a change over a variant of plain text by some vital qualities to make text safer. Cryptography is a main procedure related to segments of records security. Cryptography is worried about the encoding and deciphering of messages into puzzle code. These days the privateness of information of individuals or organizations is provided through cryptography, guaranteeing that information despatched is consistent in a way that the legitimate beneficiary can get right of section to the information, technique there's no malicious assault. An essential thought behind the framework is to accomplish information privacy and trustworthiness, to keep away from information from unapproved information access, deficient to comprehend the genuine significance. Here the significant employments of the cryptography to communicate the information through

a dubious Networks and ensure that unaccredited sources don't perceive the data situation. The first information is the plain content is changed over to encode text using scrambled calculation at the sender side.

Fig 1: Application areas of WSN

Using unscrambling calculation the Cipher text is changed over into plain content at the collector side [8]. Regular cryptography is used in workers, work areas, tablets. With implanted systems,8-cycle, 16-bit, and 32-bit microcontrollers and which could fighting to manage constant requirements for customary cryptography methods[9]. RFID and sensor gadgets, particularly, have restricted quantities of doors to be had for insurance and are consistently extraordinarily restricted with the force channel at the gadget [9]. Lightweight cryptography is an encryption procedure that works a brief impression and low computational intricacy. It is designed for expanding the projects of cryptography to limited contraptions and its related overall normalization and tips assemblage are as of now in progress. The lightweight execution mostly leads to more modest RAM utilization, and it is ideal for preparing more modest messages too. In planning lightweight cryptography arrangements, the following propensities are seen: Short square and key length will convey inconveniences: brief square can cause inconveniences including CBC disintegrates faster than various parts while the assortment of n-bit blocks encoded procedures 2n/2[10].

II RELATED WORK

A novel plan is considered for the lightweight hash strengths because of the wipe development to limit memory prerequisites. Propelled by the stream figure Grain and by the square code KATAN (among the lightest secure codes), the hash work-family QUARK was proposed, made of three cases: U-QUARK, D-QUARK, and S-QUARK. As a QUARK, made of three cases: U-QUARK, D-QUARK, and S-QUARK. As a wipe development, QUARK can be used for message verification, stream encryption, or then again confirmed encryption [9].

In the work an ultra-lightweight block cipher called PRESENT is discussed as a substitute for AES [10] . Here the size of the squares is nearly little and its ability is to for more modest keys. Everyone contains an 80 bit or a 128 pieces key that is used for the encryption interaction. Present works as shown by the SPN method. Present chips away at the squares that size is 64bits. With the SPN technique, its capacity on the plain content and check a key which uses some rounds of replacement boxes(S-boxes) and change pressing boxes (P-boxes). The SPN strategy is the Substitution stage strategy.

PHOTON is a lightweight cryptography method for hashing and is founded absolutely on an AES type approach [11]. It can make 80-piece, 128-bit, 160-piece, 224-piece, and 256-cycle hash. Here in the system a subjective length enters and delivers a variable-span yield. The PHOTON-n-r-r is to be used as the innovation. Here n is the size of the hash is clarified, r is the passage piece of the hash and r' is the left bit which is considered as yield.

Ronald et al. describe RC5 encryption algorithm as a lightweight square cipher, a fast symmetric block cipher suitable for hardware or software implementations [12]. In the methods uses a variable square length, an alternate arrangement of rounds, and a variable key length (it could be 0 to 2048 bits). It shows splendid capacities for a lightweight cryptography technique. Here a result be used to suit the encryption to the abilities of the apparatus. On the off chance that its far low-controlled apparatus with a compelled memory and a little actual impression, here used a 32-digit block length and an 80-cycle key, with just a few rounds. The apparatus can manage while the instrument using a 128-cycle block size and a 128-bit key, then it very well may be said as protected. It additionally can be adaptable, wherein a solitary expel on the two aspects can upgrade or diminish the necessities [12].

A specific quick, smooth and Feistel-principally based on Tiny Encryption Algorithm (TEA) is one of the quickest and one of most extreme green encryption calculation. Plain Text 'P' is used to destroy into parts Left [0] and Right[0], while 'C' is the code printed content (Left[64], Right[64]). P is used for scrambling the 2d 1/2 of over 64 handling adjusts through 1/2 of the plaintext after which is blended altogether to make the code text based substance section. TEA units a 128-bit key to separate in 4 32-digit significant expressions, with a square length of 64 bit under encoding, wherein 32-bit expressions might be isolated. In its encryption round, TEA involves Feistel duties notwithstanding a chain of increases and spot ways, TEA uses the Feistel strategy, referred to as F [13].

Bogdanov A et al. exploring the design space of lightweight hash functions based on the sponge construction instantiated with present-type permutations. The resulting family of hash functions by considering the sponge construction instantiated with present-type permutations is called spongent. SPONGENT chooses for a lower rate and somewhat lower area requirements. Based on

the parameters, the situation can be turned and can make SPONGENT faster though bigger. SPONGENT system uses the wide PRESENT-type permutation. With a set of finite number of input bits, the system will produce an n-bit hash value. The system is secure against differential cryptanalysis, collision attack, linear attack, etc. Here the method using the limited gadget and its emphasizes through the states with the section information [14].

III. DATASET ANALYSIS

In this we are using Chicago Dataset and this dataset is available in data world source used to perform the research work [15]**.** The Chicago Park District keeps up with sensors in the water at sea shores along Chicago's Lake Michigan lakefront. These sensors for the most part catch the demonstrated estimations hourly while the sensors are in activity throughout the late spring. During different seasons and at some different occasions, data from the sensors may not be accessible.

IV.PROPOSED SYSTEM

In this paper, we propose enhanced RSA algorithm with key extension method to provide more security to the WSN. The primary aim of this lightweight asymmetric method is to increase the security properties in resource constrained devices. Assuring the data trustworthiness along with confidentiality and integrity. The proposed system makes Encryption and Decryption much more efficient and avoiding the attacks for tampering the data. WSN generate enormous amount of data by various sources. The system protects these data streams. Here developed a single platform that providing high preference to the privacy of individual or organizations data streams. The system will also compare the runtime of enhanced RSA with TEA algorithm. The Tiny Encryption Algorithm is a lightweight symmetric block cipher, prominent for remarkable for its effortlessness of depiction and execution. This security method's salient features are:

- High security
- Computation time is less than that of TEA algorithm.
- Attacks can be reduced

The proposed system having two phases: Encryption process and decryption process. The input dataset used here is The beach-water-quality-automated-sensors-1. The encryption is done by using the enhanced RSA public key and Decryption by using Enhanced RSA private key.

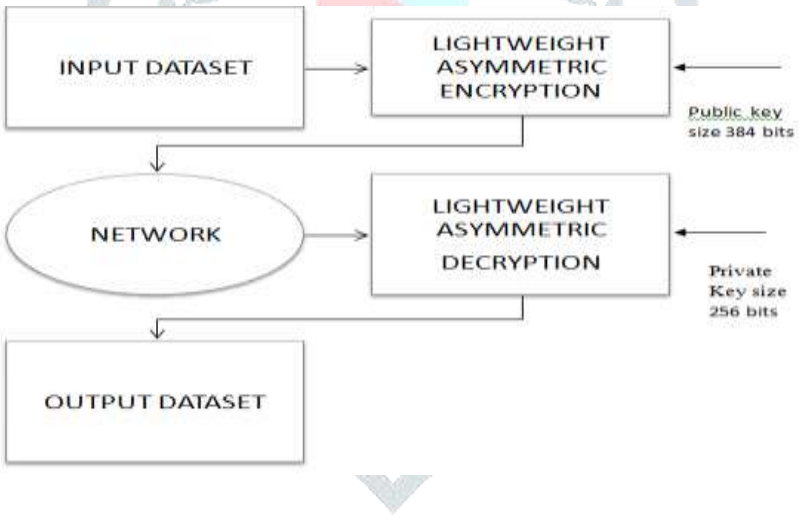

fig 1:proposed architecture

RSA is also called Public key cryptographic algorithm Ron Revest, Ade Semir, Len Alleman in 1977.This algorithm is based on the concept of modular arithmetic and exponentiation. The RSA is block cipher.in which the plaintext and cipher text are integers between 0 and n-1.RSA makes use of an expression with exponential [16].

1).Key generation:

- Select two large numbers P and q,where p≠ q.
- Calculate n,that $n=p*q$. (1)
- Calculate $\Phi(n)=(p-1)*(q-1)$ (2)
- Select an integer e such that it is not a factor of (p-1) and (q-1),GCD(e,Φ(n))=1
- Calculate d=a*bmodn=1
- The public key=(e,n) and private key=(d,n)

2) Encryption algorithm

Cipher text $C=M^e modn$ *(3)*

3) Decryption Algorithm

Plain text $M=C^d modn$ *(4)*

4.1 Extension Key in RSA

1).Key generation:

- Select two large numbers P and q,where p≠ q.
- Calculate n,that $n=|(p-q)*(p+q)|$. *(5)*
- Calculate $\Phi(n)=|((p-1)-(q-1))*((p-1)+(q-1))|$ *(6)*
- Select an integer e such that it is not a factor of (p-1) and (q-1),GCD(e,Φ(n))=1
- Calculate d=a*bmodn=1
- The public key=(e,n) and private key=(d,n)

2) Encryption algorithm

Cipher text $C=M^e modn$

3) Decryption Algorithm

Plain text $M=C^d modn$

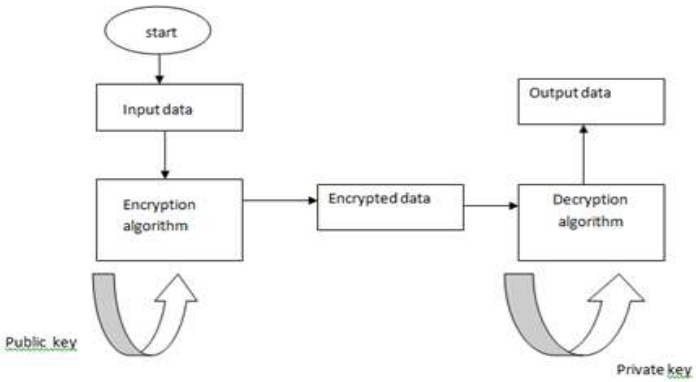

fig 3: proposed system workflow

The RSA is based on the factorizing of two large numbers and finding public key and private key. If one of the prime number is found, then the whole scheme has cracked by the cryptanalytic method. So here the enhancement of RSA is done changing the key generation method. p and q are prime numbers. First find p-q value and the p+q value. Next step is to find the value of n by multiplying (p-q) and (p+q). the value n is taken as in modular form (avoiding the occurrence of negative value for n). Remaining

process are similar to RSA algorithm. The extension of key in RSA will avoid the easy cracking of scheme. Even If one of the prime number is found, whole scheme cannot be cracked by the cryptanalytic method.

V EXPERIMENTAL ANALYSIS& RESULTS

The system implemented the Enhanced RSA with Key Extension with the sensor dataset beach-water-quality-automated-sensors-1.The encryption and decryptions are done by the lightweight asymmetric enhanced RSA encryption and decryption algorithm, respectively. It is a significant secure encryption decryption model for WSN because of the key extension. The change in key generation will make it more difficult for cryptanalytic attacks to find the value of n and the factors of the numbers generated after using this method. The equation for finding the value of n is unknown for attackers, the cryptanalysis is a more hard process and hence its provide security. The system will compare the runtimes of TEA algorithm and RSA algorithm. It will show that the Enhanced RSA is better than TEA algorithm. This system is providing more security because TEA algorithm is lightweight asymmetric algorithm: both keys are same for encryption and decryption. It is faster than TEA because of the tiny encryption process of large data streams.

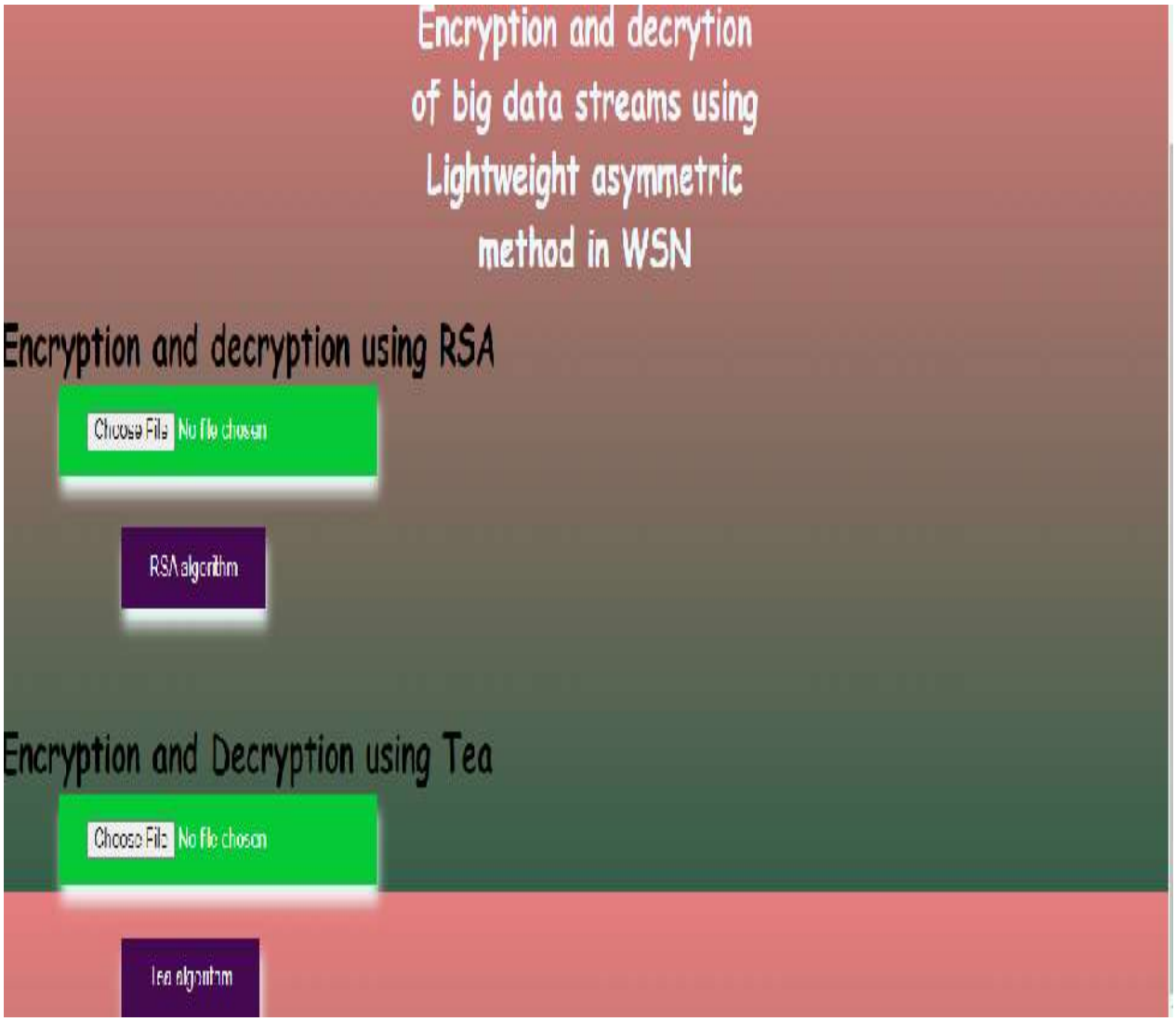

fig 4: proposed system

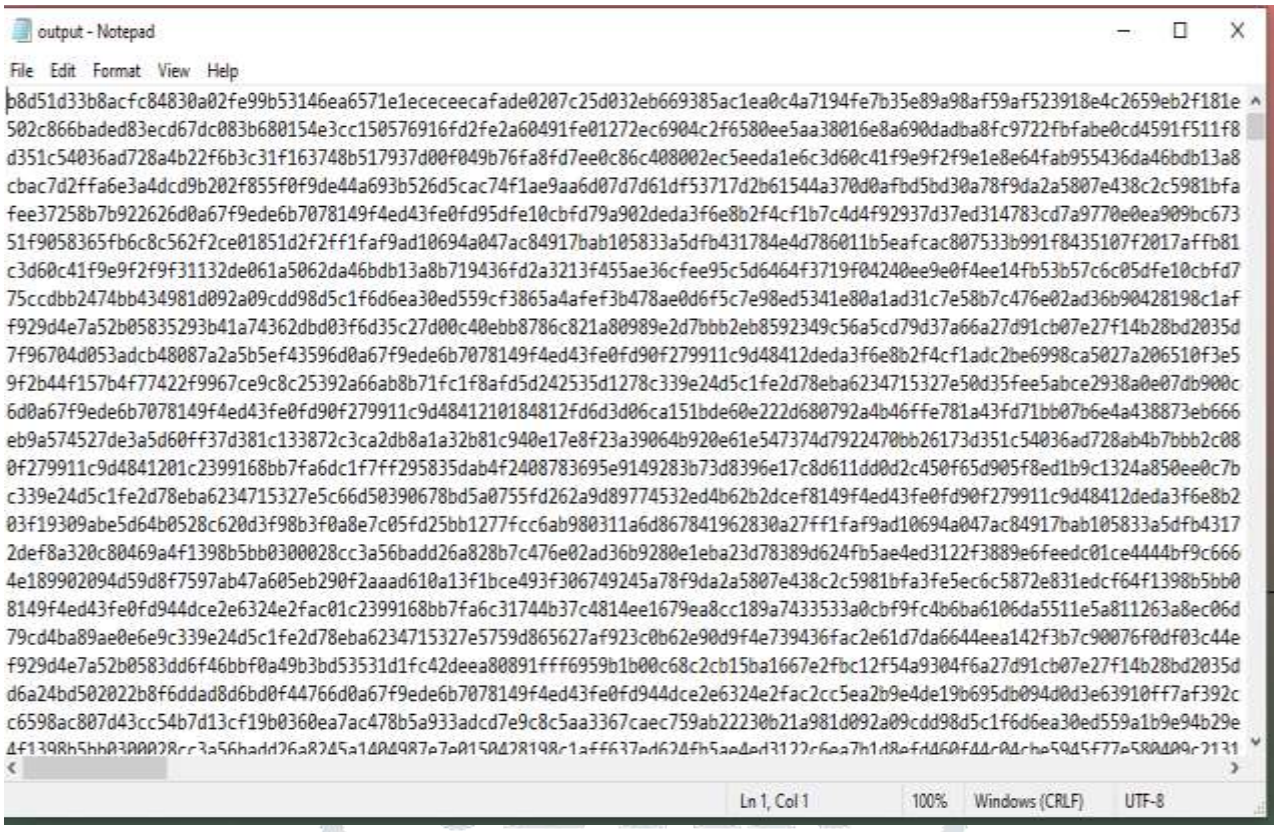

fig 5: encrypted data

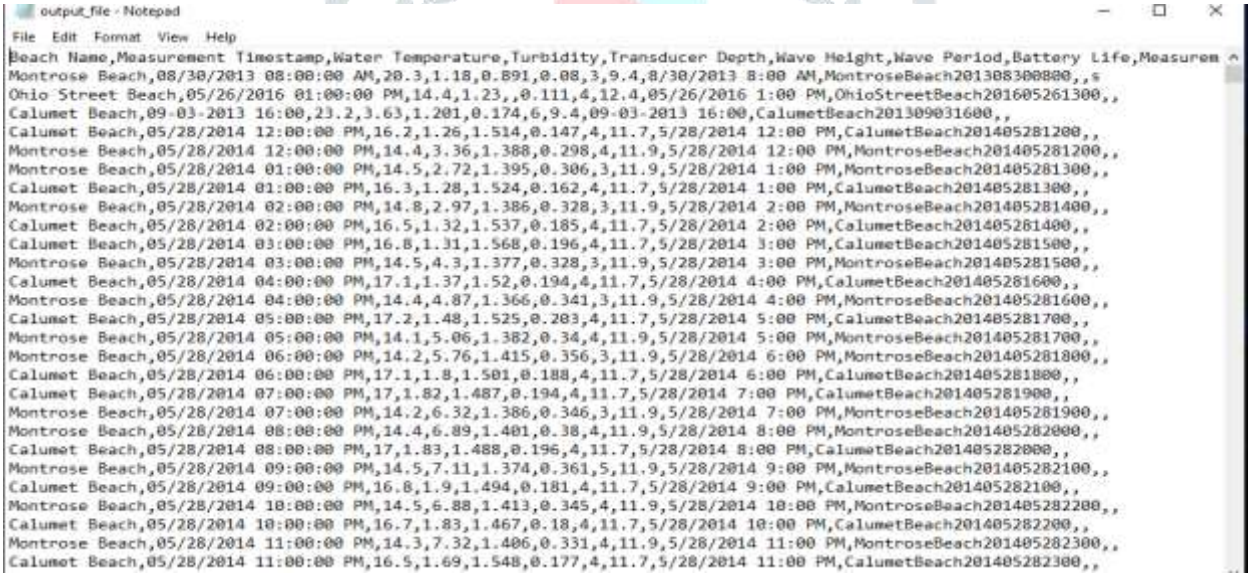

fig 6: decrypted data

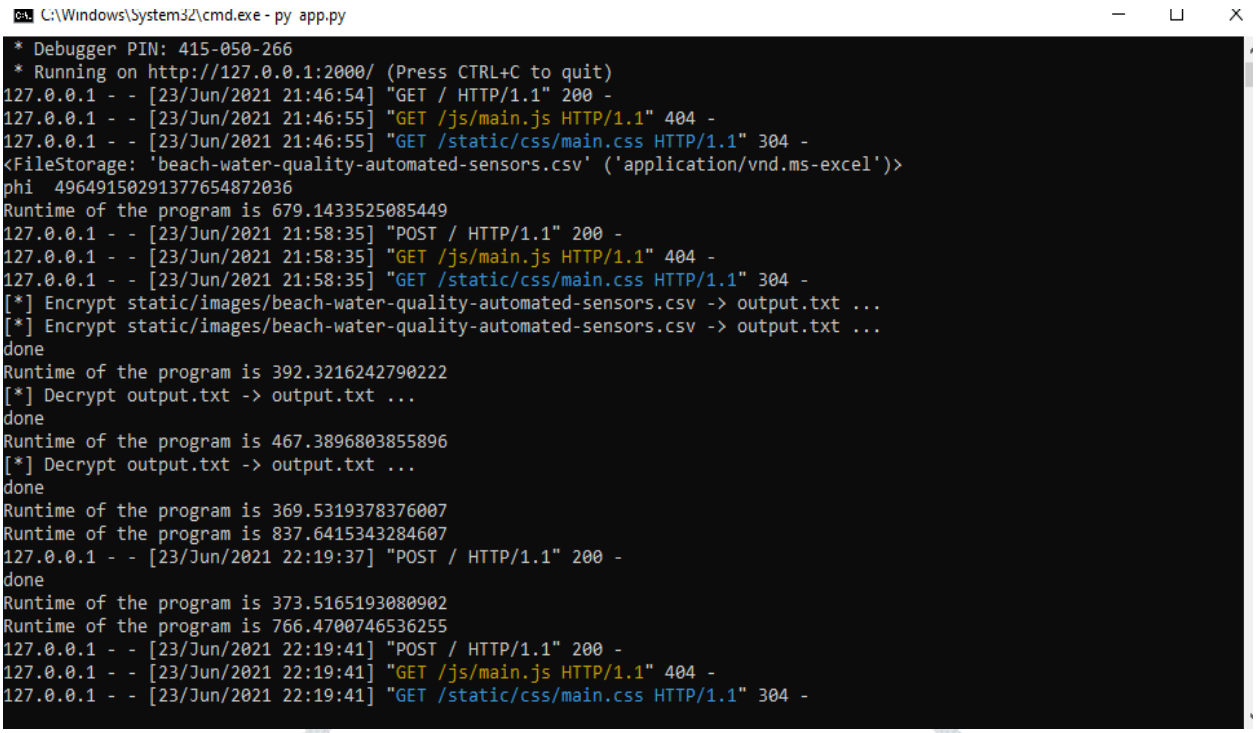

fig 7: runtime of tea algorithm

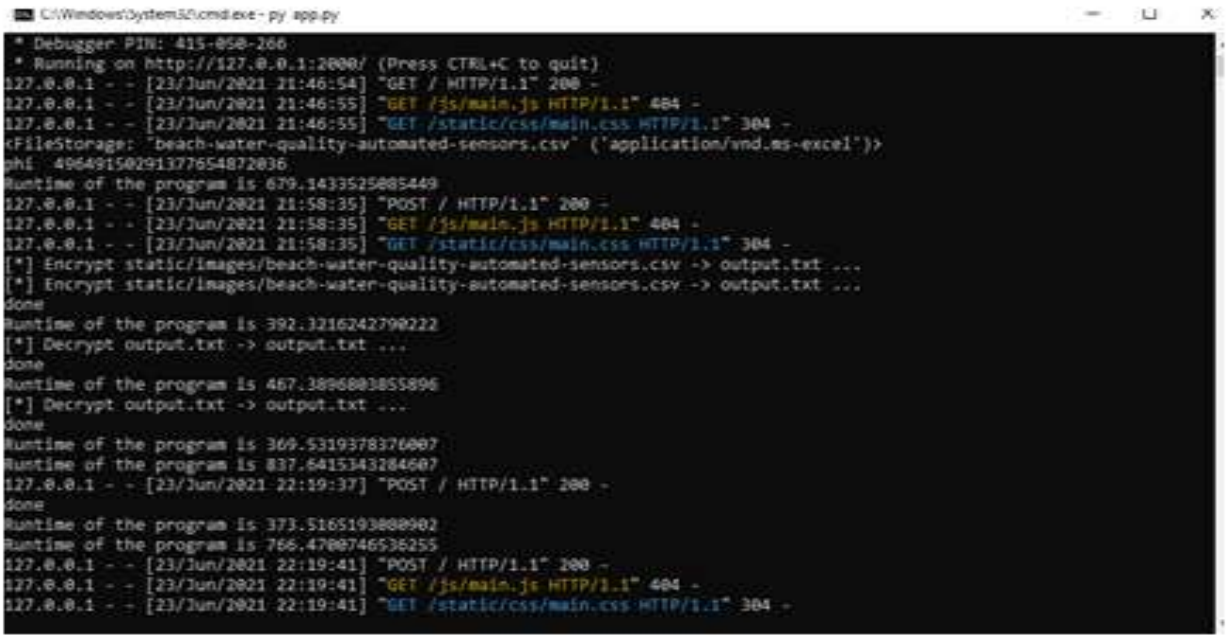

fig 8: runtime of proposed algorithm

VI CONCLUSION & FUTURE WORK

The lightweight cryptography strategies are relevant for resource constrained devices. Hash functions, blocks, streams are the well-known symmetric algorithm. It has advantages and limitations. Lightweight symmetric algorithms are commonly used in WSN. In this paper, a lightweight asymmetric algorithm, an enhanced RSA algorithm with key extension, is considered. The primary goal of this proposed system is to increase the security of the data streams in WSN. It ensures the security of the data by satisfying the confidentiality, integrity with data trustworthiness. The encryption and decryptions are done by the lightweight asymmetric enhanced RSA encryption and decryption algorithm, respectively. It is a high secure Encryption decryption model for WSN. On comparison of the proposed system with TEA algorithm it shows the runtime is less than TEA. It also shows that light asymmetric is secure than symmetric algorithms. The Extension key in RSA may cause the overhead in computation. In future can consider a system using an asymmetric algorithm that provides better security with reduced overhead.

REFERENCE

[1] M. Luo, Y. Luo, Y. an, and Z. Wang, "Secure and Efficient Access Control Scheme for Wireless Sensor Networks in the Cross-Domain Context of the IoT," *Security and Communication Networks*, vol. 2018.

[2] Carlos Andres Lara-Nino, Arturo Diaz-Perez, and Miguel Morales-Sandoval," Energy and Area Costs of Lightweight Cryptographic Algorithms for Authenticated Encryption in WSN", *Security and Communication Networks* Volume 2018.

[3] Beom-Su Kim 1 , Ki-Il Kim 1 , Babar Shah, Francis Chow and Kyong Hoon Kim,"Wireless Sensor Networks for Big Data Systems*", Sensors* 2019.

[4] V.Prakasham, V. Sowmitha and M.Vimaladevi" A Secured and Authorized SEEN Protocol forMobile Multimedia Data Collection Scheme inWMSNs", *Journal of Xi'an University of Architecture & Technology*, Volume XII, Issue VI, 2020.

[5] Karthik N, Ananthanarayana V S," Data Trustworthiness in Wireless Sensor Networks",*IEEETrustCom/BigDataSE/ISPA,2016.*

[6] B.Veeramallu,S.Sahitya, Ch.LavanyaSusanna "Confidentiality in Wireless SensorNetworks", *International Journal of Soft Computing and Engineering (IJSCE)* ISSN: 2231-2307, Volume-2 Issue-6, January 2013.

[7] Arjan durresi, Vamsi Paruchuri,Rajgopal Kannan, and S.S. Iyengar," Data Integrity Protocol for Sensor Networks", *International Journal of Distributed Sensor Networks*, 1: 205–214, 2005.

[8] Abdalbasit Mohammed, Nurhayat Varol," A Review Paper on Cryptography", 978-1-7281-2827-6/19/$31.00 ©2019 IEEE.

[9] William J. Buchanan, Shancang LiRameezAsif,"Lightweightcryptographymethods"*Journal of Cyber Security Technology*,Mar 2018

[10] Bogdanov A, Knudsen LR, Leander G, et al. PRESENT: "An ultra-lightweight block cipher". LNCS,4727, 2007;450–466.

[11] Guo J, Peyrin T, Poschmann A. "The PHOTON family of lightweight hash functions family",*In advances in Cryptology*–Crypto. 2011;222–239. Springer, 2011.

[12] Ronald L, Rivest,"The RC5 Encryption Algorithm", *MIT Laboratory for Computer Science 545 Technology Square*. Cambridge Mass.

[13] B. Murali Krishna, D. Sai Gopinath, M.Kiran, Sk.Javid,"Reconfigurable Asymmetric Lightweight Cryptosystem" *International Journal of Emerging Trends in Engineering Research*, Volume 8. No. 5, May 2020

[14] Bogdanov A, Knežević M, Leander G, et al. "SPONGENT: the design space of lightweight cryptographic hashing". IACR Cryptology ePrint Archive, 2011:697.

[15] Beach-water-quality-automated-sensors-1 [Online]. Available: https://data.world/cityofchicago/beach-water-quality-automated-sensors, Accessed on: 03.02.2021

[16] Vivek Kapoor, Vivek Sonny Abraham, Ramesh Singh, "Elliptic Curve Cryptography", *ACM Ubiquity*, Volume 9, Issue 20

[17] Biryukov A, Perrin L. "State of the art in lightweight symmetric cryptography". IACR CryptologyePrint Archive, 2017:511,

[18] Hirose S, Ideguchi K, Kuwakado H, et al. "A lightweight 256-bit hash function for hardware andlow-enddevices:Lesamnta-LW".Berlin, Heidelberg: Springer; 2011. p. 151–168.

[19] Jean-Philippe Aumasson, Nagra," QUARK: A Lightweight Hash", *International Association for Cryptologic Research* ,2012

[20] Baraa Tareq Hammad, Norziana Jamil, Mohd Ezanee Rusli and Muhammad Reza Z`aba," A survey of Lightweight Cryptographic Hash Function", *International Journal of Scientific & Engineering Research* Volume 8, Issue 7, July-2017.

[21] George Hatzivasilis · Konstantinos Fysarakis · Ioannis Papaefstathiou · Charalampos Manifavas"A review of lightweight block ciphers", *Journal of Cryptographic Engineering* · June 2018

[22] Qingkuan Dong, Wenxiu Ding and Lili Wei, "Improvement and optimized implementation of cryptoGPS protocol for low-cost radio-frequency identification authentication", *Security and communication networks Security* Comm. Networks (2014)