International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5| ISSN : 2456-3307

Secure Random Bit Size Encryption Algorithm for Wireless Sensor Data Transmission

P. Lokesh Kumar Reddy[1], Dr. B. Rama Bhupal Reddy[2], Dr. S. Rama Krishna[3]
[1]Research Scholar, Department of Computer Science, Rayalaseema University, Kurnool, Andhra Pradesh, India
[2] Professor, Department of Mathematics, K.S.R.M. College of Engineering (Autonomous), Kadapa, Andhra Pradesh, India
[3]Professor, Department of Computer Science, S.V. University, Tirupati, Andhra Pradesh, India

ABSTRACT

Wireless Sensor Networks (WSN) due to its constraints requires a security system, which adopts optimal utilization of the available resources and reduced power consumption. Diffie–Hellman key exchange (D–H) is a method of secure encrypted communication between two parties required that they first exchange keys by some secure physical channel. The security utilization parameters are used for many D–H Internet applications at that time is not strong enough to prevent compromise by very well funded attackers, such as the security services of large governments. In this paper, we proposed secured wireless data transmission using Electronic Code Book Public Key Cryptography Standard (ECB-PKCS) algorithm which uses the public key to encrypt data and the key is known to everyone, therefore it is easy to share the public key Safe and secure data transmission so it results in safe and secure data transmission and It is hard to crack since the bit size is unknown.

Keywords: Wireless Sensor Networks, Diffie–Hellman key exchange, Electronic Code Book Public Key Cryptography Standard, secure data transmission, secure encrypted communication.

I. INTRODUCTION

Wireless Sensor Network is one of the most advanced and emerging technologies of the upcoming world and is being used in GPS Tracking, medical fields, Defence Departments, homeland security etc. [1,2]. The topology of WSN works in a triangular pattern [3]. The sensor nodes collect the information from the environment and send it to the sink node, the sink node further transfer the information to a base station and hence completing the transfer of data [4]. Security of data in transit is very essential and the level of security required depends on the type of application [5, 6]. In all security mechanisms, encryption technology is the foundation. Through the encryption, it can achieve authentication, confidentiality, non-repudiation, integrity and other security requirements [7].

The security of wireless sensor network, in today's world wireless technology very fast developed and mostly used in many sectors [8,9]. Hence, the necessity for security becomes very crucial factor [10]. However, the wireless network technology has some restriction such as limited battery power, processing ability, and capacity of memory storage, etc. For this constraint, many new security mechanism and technologies have been developing to overcome these challenges [11]. There are many technologies are available to provide security against the attackers, one of the best technology is cryptography The distributed nature of wireless

sensor networks leads to the use of cloud databases that need to be protected when handling sensitive content [12,13]. In this context, Secure Random Bit Size Encryption Algorithm (ECB-PKCS) is proposed.

Our contribution:

The contribution of the study is given below:

- ✓ To provide security against the attackers by using cryptography.
- ✓ To protect the cloud databases when handling the sensitive content.
- ✓ To provide safe and secure communication
- ✓ To compare the key generation ratio and the key generation time of existing and proposed techniques.

II. LITERATURE SURVEY

In a public key security model is offered by means of Petri Nets. Computational and memory requirements of Elliptic Curve Cryptography (ECC), a public key encryption scheme, for the equivalent security level are more as related to AES [14-19]. No concern is specified to rekeying option if a node or else system is conceded. Our model has the capability of rekeying. Khan et.al, suggested an encryption model with AES in addition to ECC in Petri Net model and the outcomes for dissimilar modulation schemes were verified for BER and SNR [20]. Toldinaset.al, determined with its research that AES needed additional energy for decryption than encryption and suggested three security profiles based on their research [21].

Kavitha et.al,[22] provided a complete study of the hardware and software design of WSN beside with its protocol stack. This study suggested that security breaches in WSN were mostly of two kinds: first one, where information was released into the network, which was not required as it enabled the third person to overhear it; the second one, where data packets were introduced into the network through an opponent leading to excessive traffic and unclean data being collected from the sensor [22].

Zhang et al, [23] offered a Secure Data Collection scheme based on compressive sensing (SeDC), which improved the data privacy through the asymmetric semi-Homomorphic encryption scheme, and decreased the cost of computation by the sparse compressive matrix. The Homomorphic encryption permitted the in-network aggregation in cipher domain, and therefore improved the security and attained the load balance of network [23].

Wang et al,[24] recommended a privacy Preserving, Energy-Efficient and Scalable Continuous Data Aggregation (PECDA). PECDA considered benefit of secure channels to safeguard the confidentiality of data to counter dramatic energy consumption produced by heavy encryption/decryption processes. Furthermore, PECDA filters data and consequently significantly decreased traffic based on the temporal correlation of sensory data [24]. Shen et al,[25] suggested an effective multilayer authentication protocol and a secure session key generation technique for WBANs. Initially, the authors plan a one-to-many group authentication protocol and a group key establishment procedure amongst Personal Digital Assistance (PDA) and every sensor nodes by means of energy efficiency and less computational cost. Formerly, they offered a novel certificateless verification procedure with no pairings based on certificateless cryptography amongst PDA and Application Provider (AP), with ECC algorithm that delivered less computational cost with high security [25].

III. METHODOLOGY

Cryptography:

The Cryptography is always very vital in data origin validations, entity verification, data integrity, and confidentiality. In modern years, the cryptographic schemes have recommended certain novel and effective techniques to improve secure image encryption. These schemes have a typical structure which achieved the permutation and the diffusion phases alternatively. On the other hand, most of the procedures are confronted with certain difficulties

like the absence of robustness and security. The random number generators are intransitive in cryptography for generation of cryptographic keys, allegorically, secret keys used in symmetric cryptosystems and huge numbers is intransitive in asymmetric cryptosystems for the reason that of random would better be produced randomly. Additionally, random number generators in several cryptographic protocols, such as to create challenges, blinding value is utilized. Likewise, the random number generators are utilized more in the diffusion functions of the image encryption for diffused pixels of the plain image [26, 27, 29].

Currently, there are five primary functions of cryptography:

1. Privacy/confidentiality: Guaranteeing that no one can read the message apart from the intended receiver.
2. Authentication: The method of verifying one's identity.
3. Integrity: Promising the receiver that the received message has not been changed in any way from the original.
4. Non-repudiation: A mechanism to show that the sender actually sent this message.
5. Key exchange: The way by which crypto keys are shared among sender and receiver.

In cryptography, we start with the unencrypted data, referred to as plaintext. Plaintext is encrypted into cipher text, which will in turn (usually) be decrypted back into usable plaintext. The encryption and decryption are based upon the type of cryptography scheme being employed and some form of key. For those who like formulas, this process is sometimes written as:

$$C = Ek(P) \quad (1)$$

$$P = Dk(C) \quad (2)$$

Where **P** = plaintext, **C** = cipher text, **E** = the encryption method, **D** = the decryption method, and **k** = the key.

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are:

- Secret Key Cryptography (SKC): Utilizes a single key for both encryption and decryption; also called symmetric encryption. Mainly utilized for privacy and confidentiality.
- Public Key Cryptography (PKC): Considers one key for encryption and additional for decryption; also known as asymmetric encryption. Mostly utilized for verification, non-repudiation, and exchanging of the key.
- Hash Functions: Considers a mathematical transformation to irreversibly "encrypt" data, provided that a digital fingerprint. Mainly utilized for message integrity.

Electronic Code Book (ECB):

The Electronic Codebook (ECB) mode is a confidentiality mode that features, for an assumed key, the assignment of a fixed cipher text block to every plaintext block, corresponding to the assignment of code words in a codebook. The ECB mode is well-defined as given below:

ECB Encryption:

$C_j = CIPHK(P_j) \quad forj = 1 \ldots n.$ (3)

ECB Decryption:

$P_j = CIPH^{-1}K(C_j) forj = 1 \ldots n.$ (4)

In ECB encryption, the forward cipher function is applied directly and independently to each block of the plaintext. The resulting sequence of output blocks is the cipher text. In ECB decryption, the inverse cipher function is applied directly and independently to each block of the cipher text. The resulting sequence of output blocks is the plaintext.

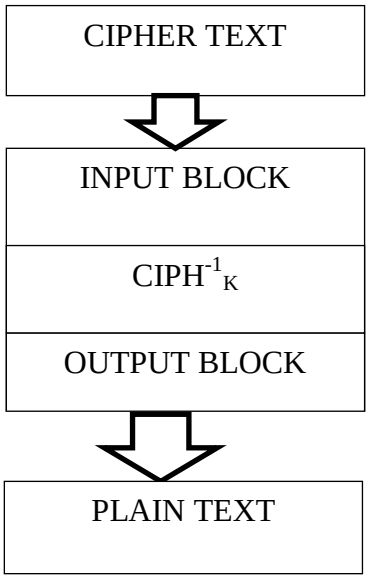

Figure 1: Encryption process in the ECB mode

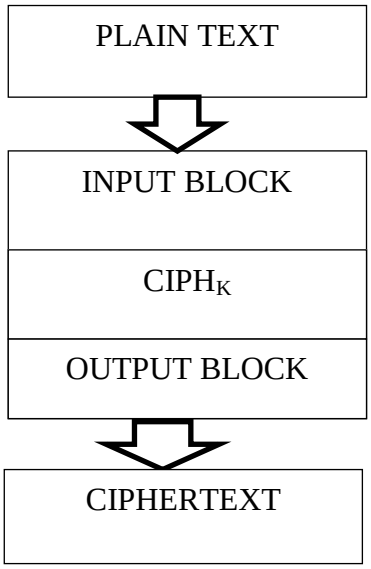

Figure 2: Decryption process in the ECB mode

In ECB encryption and ECB decryption, multiple forward cipher functions and inverse cipher functions can be computed in parallel. In the ECB mode, under a given key, any given plaintext block always gets encrypted to the same cipher text block. If this property is undesirable in a particular application, the ECB mode should not be used. The ECB mode is illustrated in Figure 1 and 2.

Public Key Cryptography Standards (PKCS):

A set of interoperable standards and guidelines for public key cryptography, designed by RSA Data Security Inc.

- PKCS #1: RSA Cryptography Standard (Also RFC 8017)
- PKCS #2: Incorporated into PKCS #1.
- PKCS#3: Diffie-Hellman Key-Agreement Standard
- PKCS #4: Incorporated into PKCS #1.
- PKCS#5:Password-Based Cryptography Standard (PKCS #5 V2.1 is also RFC 8018)
- PKCS #6: Extended-Certificate Syntax Standard (being phased out in favour of X.509v3)
- PKCS #7: Cryptographic Message Syntax Standard (Also RFC 2315)
- PKCS #8: Private-Key Information Syntax Standard (Also RFC 5208)
- PKCS #9: Selected Attribute Types (Also RFC 2985)
- PKCS #10: Certification Request Syntax Standard (Also RFC 2986)
- PKCS #11: Cryptographic Token Interface Standard
- PKCS #12: Personal Information Exchange Syntax Standard (Also RFC 7292)
- PKCS #13: Elliptic Curve Cryptography Standard
- PKCS #14: Pseudorandom Number Generation Standard is no longer available
- PKCS #15: Cryptographic Token Information Format Standard

Electronic Code Book Public Key Cryptography Standard (ECB-PKCS):

In this study, we used a hybrid technique known as ECB_PKCS which will combine the features of both ECB and PKCS and used for security purpose.

- ECB-PKCS is safe since encryption of data done on a random bit.
- It will be difficult to decrypt the data without knowing the private key since the bit size also unknown.
- ECB-PKCS uses the public key to encrypt data and the key is known to everyone, therefore it is easy to share the public key.

Flowchart:

The flowchart of the proposed algorithm is as shown in the below-given figure. The process is explained in the discussion section.

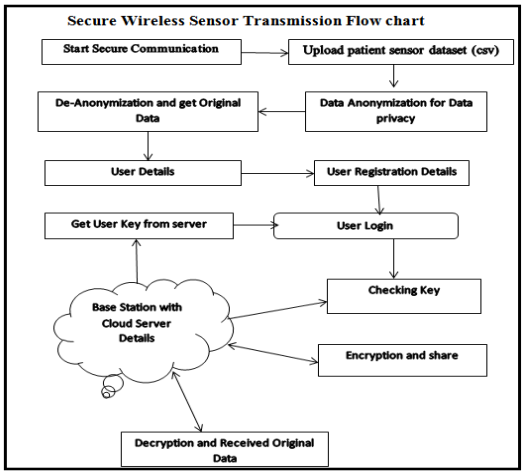

Figure 3

IV. RESULTS AND DISCUSSION

The proposed algorithm is implemented successfully and the results are obtained and discussed in this section.

Home

The below-given figure 4 shows the home page which was obtained for secure wireless sensor data transmission by means of the proposed algorithm ECB_PKCS

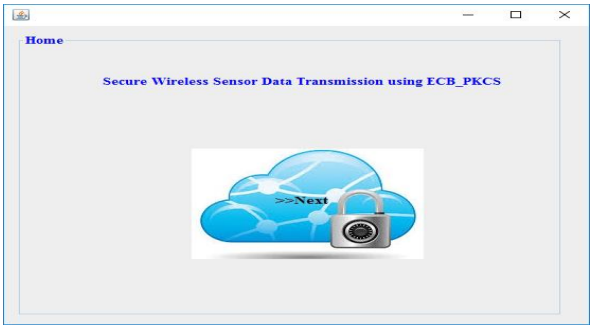

Figure 4. Homepage

The input data set will be given in the form of comma separate vector file (.csv file) is shown in below-given figure 5 which will display the overall information about the patient. The information which is given as an input data set can be seen in the below figure. Here we considered some list of patients and their attributes such as ID, name, age, address, gender, state, email ID, phone number, currency and date of birth. These particulars of patient need to give as an input dataset.

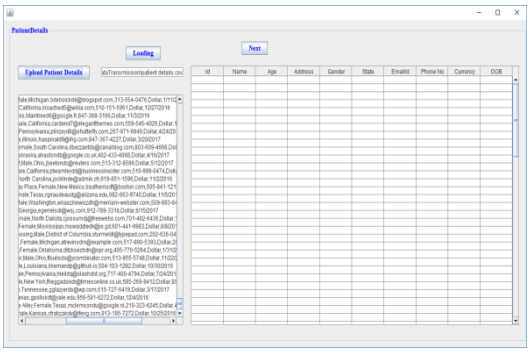

Figure 5. Uploading patient details

The below-given figure 5 shows the details entered by patients with their corresponding attributes. And figure 6 shows the process of data uploading.

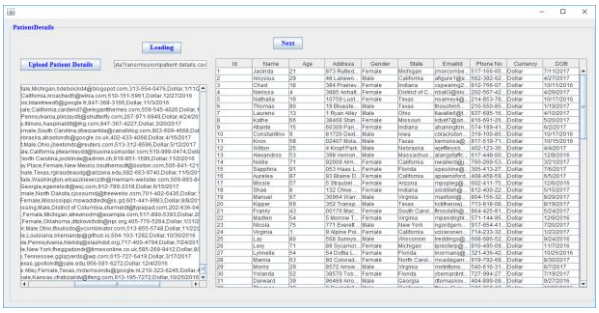

Figure 6. The process of data transmission

Figure 7. Data uploading

The below-given figure 8 shows the procedure of data Anonymization. Data anonymization is the procedure of de-identifying sensitive data while preserving its format and data type. The masked data can be realistic or a random sequence of data or the output of anonymization can be deterministic, i.e., the equal value every time. All these are reliant on the method utilized for anonymization. Theoretically, data masking mentions to a method that swaps the data through a special character while data anonymization or data obfuscation establishes hiding of information and this would suggest replacement of the original data value with a value preserving the format and type. Data anonymization is used to offer

security against any third party entry into the database. For security purpose, we will use this data anonymization technique and the data will be stored in the cloud.

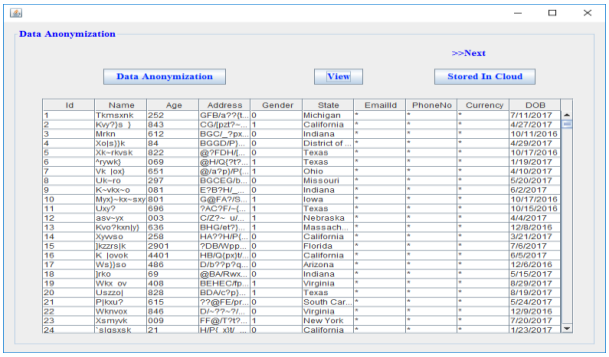

Figure 8. Data Anonymization

Figure 9, 10 and 11 shows the patient login, information and details pages. In figure 10 the process of de-anonymization is shown as below. De-anonymization is a strategy in data mining in which anonymous data is cross-referenced with other sources of data to re-identify the anonymous data source. More and more data are becoming publicly available over the Internet. These data are released after applying some anonymization techniques like removing personally identifiable information (PII) such as names, addresses, and social security numbers to ensure the sources' privacy. This assurance of privacy allows the government to legally share limited data sets with third parties without requiring written permission. Such data has proved to be very valuable for researchers, particularly in health care. However, as the Netflix contest dramatically revealed so much of data is available, even after anonymization, that a specific individual's identity could be re-discovered. The de-anonymization process is used to get the legitimate data i.e., original data.

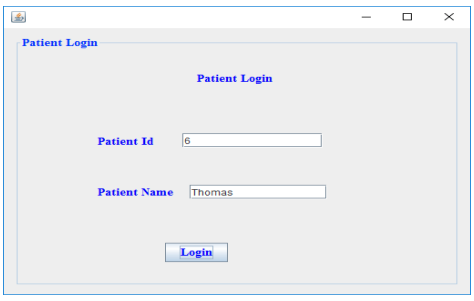

Figure 9. Patient login page

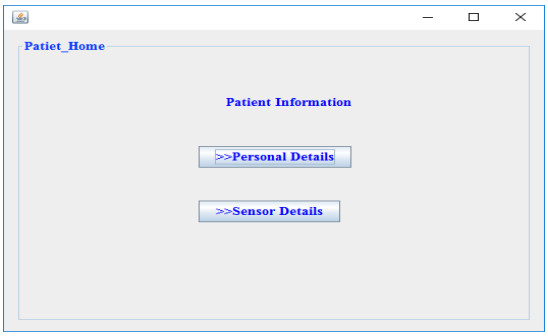

Figure 10. Patient information page

Figure 11. Patient details view page

Figure 12 shows the authentication process which consists of username, password and authentication code for the proper verification process.

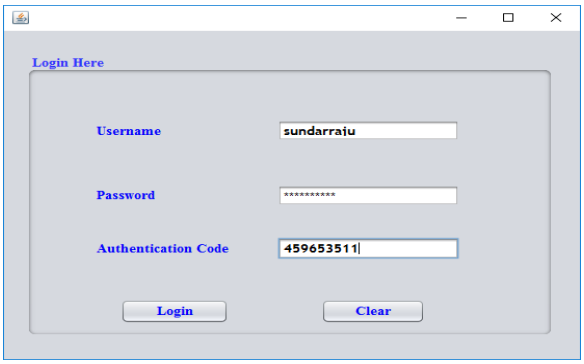

Figure 12. Authentication process

Figure 13 shows the domain authority login process and figure 13 shows its verification process. In this stage, the process of registration was performed if the user is new. After this view user request process will take place then finally the domain authority login details need to enter in order to proceed to the next stage.

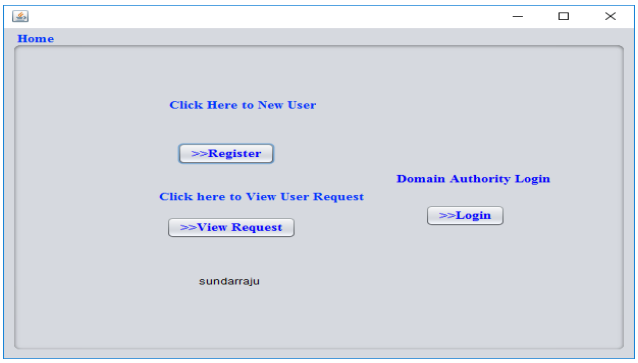

Figure 13. Domain authority login

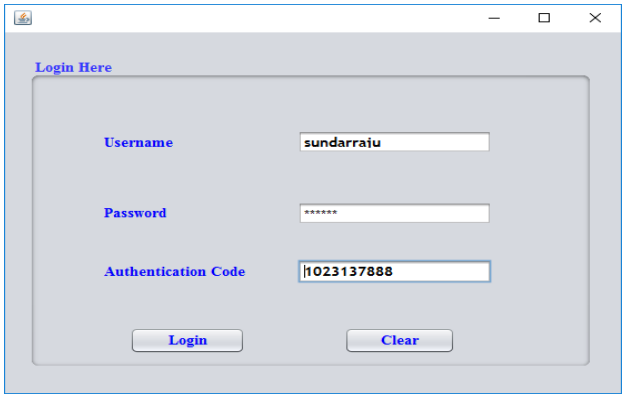

Figure 14. Authentication process

Figure 15 shows the process of secure communication along with cloud details and patient data communication and figure 15 shows the secure communication and user communication with base station details. Figure 16 shows the status of base station communication as given below.

Figure 15. Secure communication along with cloud details and patient data communication

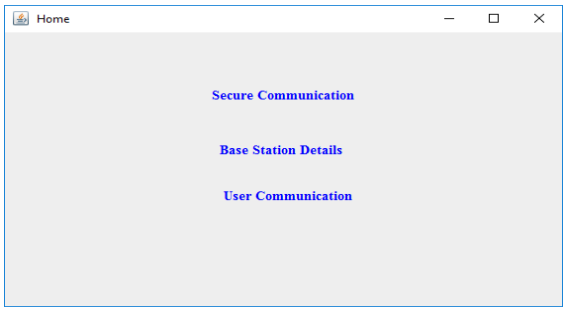

Figure 16. Secure communication and user communication with base station details

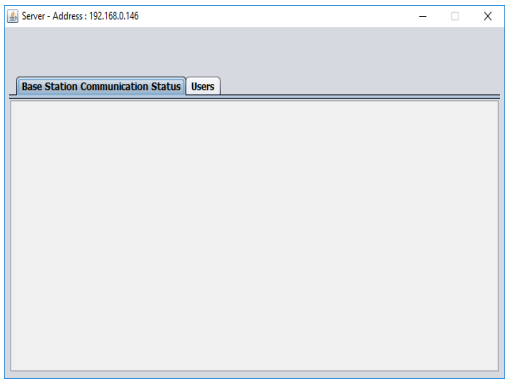

Figure 17. Status of base station communication

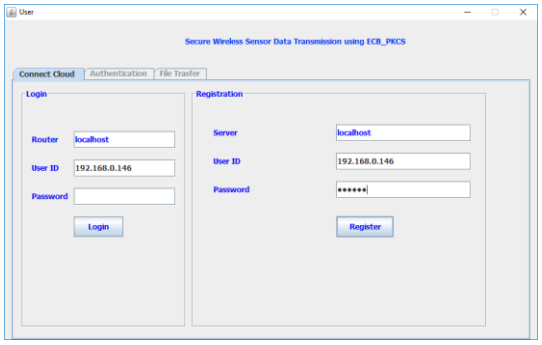

Figure 18. Registration using Server and user id

The process of registration using Server and user id is shown in figure 19 in which login details such as a router and user id and password details in case if the user is an existing user. If the user is a new user then need to register by entering the details of the server, user id, and password as shown in above figure.

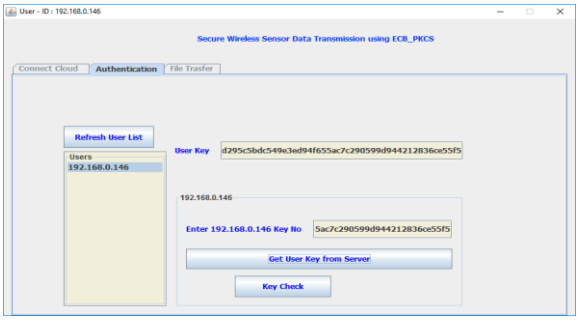

Figure 19. obtaining the user key from the server

After the registration and login process, the process of obtaining the user key from the server will be the next stage as shown in the above figure 20.

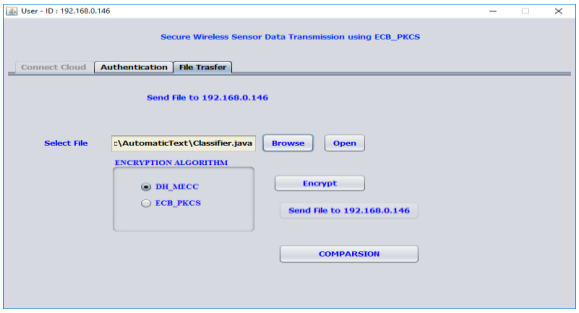

Figure 20. Existing algorithm encryption and decryption

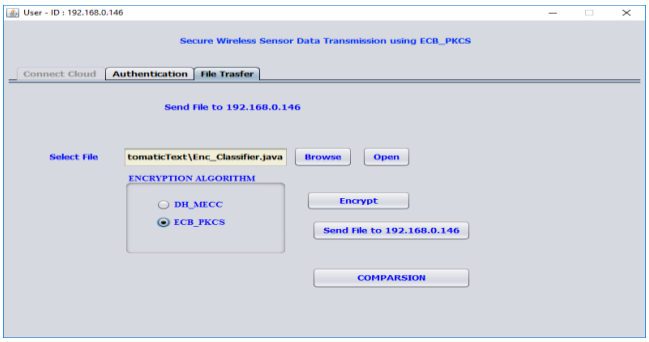

Figure 21. Proposed algorithm encryption and decryption

The above figure 20 and 21 shows the authentication process of the existing and proposed algorithm in order to obtain the comparison between them. In the authentication process, we need to select the algorithm used for encryption and then after encryption, decryption process will take place. Figure 22 and 23 shows the base station communication status and user Id and key status that shows the status of registration, login, issuing of the key, key number authentication etc. for a particular user.

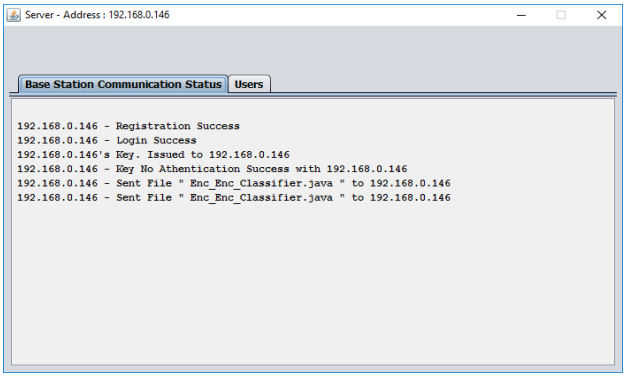

Figure 22. Base station communication status

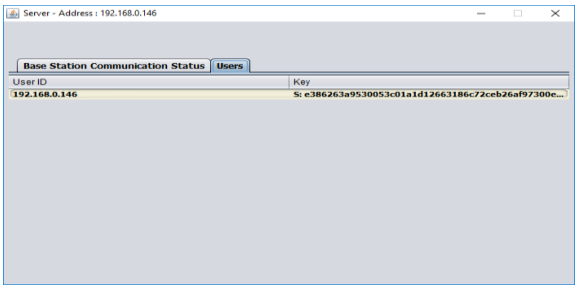

Figure 23. User Id and key status Validation:

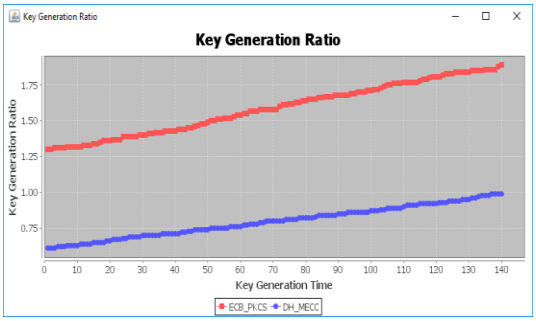

Figure 24. key generation ratio vs. time comparison for existing and proposed algorithm

The above figure 23 shows the comparison graph of key generation ratio and key generation time for existing algorithm i.e., DH_MECC and proposed algorithm i.e., ECB_PKCS algorithm. From the above characteristics, it is proved that the proposed ECB_PKCS algorithm shows better performance compared to the existing DH_MECC algorithm.

V. CONCLUSIONS

we proposed secured wireless data transmission using Electronic Code Book Public Key Cryptography Standard algorithm which utilizes the public key to encrypt data and the key was known to everyone, hence it is easy to share the public key Safe and secure data transmission, therefore, it outcomes in safe and secure data transmission and it is tough to crack as the bit size is unknown. The proposed algorithm is used for safe and secure communication between server and user as given in the discussion part. Data Anonymization and de-Anonymization processes are used for proper security purposes. Finally obtained the comparison graph for key generation ratio and key generation time for existing and proposed algorithms in which proposed shown

the better performance compared with an existing technique.

VI. REFERENCES

[1]. Arampatzis, T., Lygeros, J., & Manesis, S. (2005, June). A survey of applications of wireless sensors and wireless sensor networks. In Intelligent Control, 2005. Proceedings of the 2005 IEEE International Symposium on, Mediterranean Conference on Control and Automation (pp. 719-724). IEEE.

[2]. Sohraby, K., Minoli, D., & Znati, T. (2007). Wireless sensor networks: technology, protocols, and applications. John Wiley &Sons.

[3]. Jin, M., Gu, X., He, Y., & Wang, Y. (2018). Wireless sensor networks. In Conformal Geometry (pp. 253-296). Springer, Cham.

[4]. Gravina, R., Alinia, P., Ghasemzadeh, H., & Fortino, G. (2017). Multi-sensor fusion in body sensor networks: State-of-the-art and research challenges. Information Fusion, 35, 68-80.

[5]. Fadlullah, Z. M., Wei, C., Shi, Z., & Kato, N. (2017). GT-QoSec: A Game-Theoretic Joint Optimization of QoS and Security for Differentiated Services in Next Generation Heterogeneous Networks. IEEE Transactions on Wireless Communications, 16(2), 1037-1050.

Sridhar, T., Vivek, V., & Shekhar, R. (2017, May). Seclogmon: Security in cloud computing using activity log for consumer data protection. In Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on (pp. 1458-1462). IEEE.

[6]. Chauhan, B., Borikar, S., Aote, S., & Katankar, V. (2018). A Survey on Image Cryptography Using Lightweight Encryption Algorithm.

[7]. Tomic, I., & McCann, J. A. (2017). A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols. IEEE Internet of Things Journal, 4(6), 1910-1923.

[8]. Radhappa, H., Pan, L., Xi Zheng, J., & Wen, S. (2017). A practical overview of security issues in wireless sensor network applications. International Journal of Computers and Applications, 1-12.

[9]. Liu, C. H., & Chung, Y. F. (2017). Secure user authentication scheme for wireless healthcare sensor networks. Computers & Electrical Engineering, 59, 250-261.

[10]. Aponte-Luis, J., Gómez-Galan, J. A., Gómez-Bravo, F., Sanchez-Raya, M., Alcina-Espigado, J., & Teixido-Rovira, P. M. (2018). An Efficient Wireless Sensor Network for Industrial Monitoring and Control. Sensors, 18(1), 182.

[11]. Battistelli, C., McKeever, P., Gross, S., Ponci, F., & Monti, A. (2018). Implementing Energy Service Automation Using Cloud Technologies and Public Communications Networks. In Sustainable Cloud and Energy Services (pp. 49-84). Springer, Cham.

[12]. Mehmood, A., Khanan, A., Umar, M. M., Abdullah, S., Ariffin, K. A. Z., & Song, H. (2018). Secure Knowledge and Cluster-Based Intrusion Detection Mechanism for Smart Wireless Sensor Networks. IEEE Access, 6, 5688-5694.

[13]. Liu, Z., Seo, H., Castiglione, A., Choo, K. K. R., & Kim, H. (2018). Memory-Efficient Implementation of Elliptic Curve Cryptography for the Internet-of-Things. IEEE Transactions on Dependable and Secure Computing.

[14]. Qiu, S., Xu, G., Ahmad, H., & Wang, L. (2018). A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems. IEEE Access, 6, 7452-7463.

[15]. Kumar, M., & Gupta, P. (2018). A Novel and Secure Multiparty Key Exchange Scheme Using Trilinear Pairing Map Based on Elliptic Curve Cryptography. In Soft Computing: Theories and Applications (pp. 37-50). Springer, Singapore.

[16]. Thangarasu, N., & Selvakumar, A. A. L. (2018). Improved elliptical curve cryptography and Abelian group theory to resolve linear system problem in sensor-cloud cluster computing. Cluster computing, 1-1

[17]. Qi, M., & Chen, J. (2018). New robust biometrics-based mutual authentication scheme with key agreement using elliptic curve cryptography. Multimedia Tools and Applications, 1-17. 0.

[18]. Martínez, V. G., Gonzalez-Manzano, L., & Munoz, A. M. (2018). Secure Elliptic Curves in Cryptography. In Computer and Network Security Essentials (pp. 283-298). Springer, Cham.

[19]. Khan, A., Shah, S. W., Ali, A., & Ullah, R. (2017, January). Secret key encryption model for Wireless Sensor Networks. In Applied Sciences and Technology (IBCAST), 2017 14th International Bhurban Conference on (pp. 809-815). IEEE.

[20]. Toldinas, J., Damasevicius, R., Venckauskas, A., Blazauskas, T., & Ceponis, J. (2014). Energy consumption of cryptographic algorithms in mobile devices. Elektronika ir Elektrotechnika, 20(5), 158-161.

[21]. Kavitha, T., &Sridharan, D. (2010). Security vulnerabilities in wireless sensor networks: A survey. Journal of Information Assurance and Security, 5(1), 31-44.

[22]. Zhang, P., Wang, S., Guo, K., & Wang, J. (2018). A secure data collection scheme based on compressive sensing in wireless sensor networks. Ad Hoc Networks, 70, 73-84.

[23]. Wang, T., Qin, X., Ding, Y., Liu, L., & Luo, Y. (2018). Privacy-Preserving and Energy-Efficient Continuous Data Aggregation Algorithm in Wireless Sensor Networks. Wireless Personal Communications, 98(1), 665-684.

[24]. Shen, J., Chang, S., Shen, J., Liu, Q., & Sun, X. (2018). A lightweight multi-layer authentication protocol for wireless body area networks. Future Generation Computer Systems, 78, 956-963.

[25]. Qiu, H. (2018). An Efficient Data Protection Architecture Based on Fragmentation and Encryption. arXiv preprint arXiv:1803.04880.

[26]. Javashi, H., & Sabbaghi-Nadooshan, R. (2011). A Novel Elliptic curve cryptography Processor using NoC design. arXiv preprint arXiv:1110.1046.

[27]. Jerry, M., Ni, K., Parihar, A., Raychowdhury, A., & Datta, S. (2018). Stochastic Insulator-to-Metal Phase Transition-Based True Random Number Generator. IEEE Electron Device Letters, 39(1), 139-142.

P.Lokesh Kumar Reddy received the BCA and MCA. M.Tech (JNTUA) degrees from S.V. University, Tirupati in 2004 and 2007. He is working as Assistant Professor in S.V.College of Engineering, Tirupati. His research interest includes wireless networks and sensor networks.

Dr. B. Rama Bhupal Reddy received the M.Sc., M.Phil. and Ph.D Degrees from S.V. University, Tirupati. He is working as Professor in department of Mathematics, K.S.R.M. College of Engineering, (Autonomous) Kadapa. His research interest includes Computational Fluid Dynamics and Mathematical Modeling and computer networks and Cryptography. He published 80 Papers and 9 Text Books. He has supervised 15 M.Phil. Students and one Ph.D student guided. He is also member of Editorial Board of five journals in Research India Publications.

Dr. S. Rama Krishna received the M.Sc., M.Phil., and Ph.D Degrees from S.V. University, Tirupati. He worked in different positions in the department of Mathematics S.V. University, Tirupati. Recently he is working as Vice-Principal, and Professor, Department of Computer Science, S.V. University, Tirupati. His research interest includes Computational Fluid Dynamics and Computer Networks and Cryptography. He has supervised a number of M.Phil students. 12 Ph.D students guided and have completed supervised one Research Project.