International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

Internet of Things: IETF protocols, Algorithms and Applications

M. Sunil Kumar, K. Jyothi Prakash

Abstract*-- Gathering and transmitting data can do through internet connected things without interaction of human. Internet of Things are becoming more dominant in our environments by the support of technologies. Now a days the digital information shared from Internet of Things devices via Wireless by using Wireless Sensor Networks (WSN). To this end, a set of protocols and some open standards are developed by the IETF for obtaining applications and their services for wireless networks. In this provide privacy and security while transmitting data for health care IOT based applications, because the security is major problem in today's world. This paper focuses on explaining the concepts of the IETF protocols, password strength evaluation method and Steganography technique by using algorithms.

Index terms: IoT, steganography, AES, RSA, cryptography, encryption, health care services, medical images.

I. INTRODUCTION

From last decade, the Internet of Things has begun to be the new scrutiny for both industry and academia. The concept of IoT can be originate by Kevin Ashton in 1999 and he was viewed RFID as crucial to the Internet of Things. The IoT creates dissimilar sets of technologies for fetching real world information from sensor, RFID, actuators connected devices. These enabling technologies afford development of extensive class applications from territories such as the smart environment, which cover smart cities, offices, homes, industrial environments; and healthcare. The IoT creates non-segregated communication environment from both physical and virtual world catenated devices. The IoT systems having remote based digital healthcare systems, so this development the transmission of medical data is became a regular procedure. The patient's health data are transferred to the medical database, which is accessed and shared by government organizations, researchers, health care contributors, insurance companies, and patients. Therefore, it is obligatory to develop organized model to make probity and security of the patient's data received and transmitted from IoT habitat. In this using password strength evaluation method for providing privacy for patient's health data by using their personal information for strong passwords, and for secure transmission of medical data using system encryption algorithms and steganography techniques to conceal the digital information in an image.

The Cryptography word is other word for data encryption. It is the encoded process for the messages, which cannot read by hackers, but authorized persons can do. It is a technique with collection of mathematical ideas and set of algorithms called rule based computations to convert messages for secure communication. By using these algorithms to initiate the cryptographic key and digital signing and provide authentication in the internet web browsing and protect data privacy on privileged communications. Now, they are using modern cryptography this cryptography having some objectives i.e. listed below.

Confidentiality: The concept of confidentiality defines that only the sender and the intended recipient should be able to access the contents of information.

Integrity: The message cannot be modified in transit between intended receiver and sender without the modification being detected.

Authentication: Authentication process helps to initiate proof of identities. This mechanism protect the message was correctly identified from the origin.

Non-repudiation: Non-repudiation does not permit the sender of a information to confute the claim of not conveying the information.

Cryptography exist two types of keys:

1. Symmetric key cryptography: In that same key using while encryption and decryption, E.g. Data Encryption Standard (DES), AES, Triple DES, and Blow fish algorithm.
2. Asymmetric key cryptography: In that it uses two keys, one for encryption and another one for decryption, E.g. RSA algorithm.

In this work for the data encryption they used two main algorithms i.e. AES and RSA algorithms. AES is a symmetric key cryptography to use same keys on both encryption and decryption. It has a 128 bit fixed block size, and 128,192, or 256 bits of key length. The size is split into 128-bit blocks while sending the lengthy messages. Seemingly, extended keys build the cipher more inconvenient to break, but also implement a lengthy process of encryption and decryption. On the perverse, the RSA is used in private communication districts and business because it is a public key algorithm. RSA have a high variable key size from the range of (2-2048) bits. The most important research for hiding data is steganography technique; it is an art and science of hiding message within an image. The advantage of steganography is that it can be used to convey classified information without the reality of the transmission being detected. The DWT is the theory of forms in the human visual system with the matching of multi resolution characteristics, frequency spread, and spatial localization. In this performs the both DWT steganography techniques i.e. DWT-1L and DWT-2L. It's run on the frequency realm. In this the image can be split into high and low recitation parts.

Manuscript published on 30 September 2019.
*Correspondence Author(s)
Dr. M. Sunil Kumar*, Professor, department of Computer Science and Engineering, Sree Vidyanikethan Engineering college, Tirupati, India. Email: sunilmalchi@vidyanikethan.edu
K. Jyothi Prakash, PG Scholar, department of Computer Science and Engineering, Sree Vidyanikethan Engineering college, Tirupati, India. Email: kambala.prakash4@hotmail.com

Steganography technique contains not only image steganography it include text steganography, video steganography and etc.

The steganography purpose is not only preventing the significant concealed information from others, but also detaching the intuition in having concealed information. The message is becomes difficult to detect because it is privileged document to be camouflaged and transmitted in the carrier. In this paper, it implemented steganography technique to enhance the security while transmitting the medical data to get healthcare system it having high security.

II. RELATED WORK

Zhengguo Sheng *et al*. [1], surveyed on technologies which are support to the IoT for make them smart and better understand our environments and increases the smartness into our things. In this provide IETF protocol suite for accessing services and applications for wireless networks. In that the most important wireless network is WSN to accessing the data fastly because they are IP based network, so in the world IP based networks are connected widely. In this survey provides a brief overview of IETF protocol suite to support the IoT. In that it presents some challenges and opportunities to the each layer in the protocol. The layers are, MAC layer, physical layer, 6lowPAN, CoAP and RPL protocols.

Daojing He *et al*. [2], proposed the method for provide security to the patient's medical data. In recent days they monitor patient's health in real time. In that they have many security problems, so in this it proposed a one method to maintain the data securely. The method is Password Strength Evaluation method, in that it has the patient's personal data to make a password strong, i.e., the patient's personal information to the account. In this it focused on password guessing attacks by the cyber criminals. In that it proposed password strength meter to helps users to select passwords strongly.

Mohamed Elhoseny *et al*. [3], proposed the model to provide security for medical images it consist diagnostic text data. In this it is used steganography technique having hybrid encryption scheme for developing the hybrid security model with integrating discrete wavelet technique. This schema is built from combination of RSA and AES algorithms. This proposed system performs based on PSNR, MSE, BER, SC and SSIM parameters. In this the hybrid security model provides the security and conceal the patient's information into the cover image with high capacity of the output stego image.

Hamid Al-Hamadi *et al*. [4], proposed a protocol of trust based decision making for IoT health care systems. This proposed protocol consider the following three design dimensions as decision making, these are reliability, loss of health probability and classification. In this also developed a protocol for health IoT system, i.e. trust computation protocol. It is to assess the reliability trust of discrete IoT devices. In that also developed a method to derive the probability of health loss and aggregate sensing data, should the patient enter a particular location at particular time. In that also conducted a performance analysis between proposed protocol and two baseline protocols (NMH and NT) with irresistible results.

III. METHODS

A. Password Strength Evaluation:

In order to issue the users feedback regularly from the results of the password strength, most of the information management systems are use some particular password strength meters (PSMs) to help users for the process of improving the password strength at the time of changing the passwords or information services registration. Now, this PSM designs are based on heuristics. These are some conventional web sites of the information management systems. There was some incompatible in password strength measurements, it causes misunderstanding, uncertainty and irritation in users. As per some different design ideas, the following password strength evaluators can split into the following algorithms. These are pattern, rule, and attack-based.

These algorithms are performed at different stages or different attributes. Each algorithm performs different tasks, in that the rule based method is based on the type and length of the characters. In that it is not involving in the user's personal information at the computation level. The pattern based method is mainly for to recognise the construction patterns of every sub part of the password, and then assigning the patterns corresponding scores for their respective patterns. The attack based method uses advanced password attack algorithm to detect the strength of the attacking a current password. This existing evaluators are cannot provide an error free consideration result for this state. The above process is the normal procedure of the password strength evaluation for maintaining the secure patient's data. The below procedure of the password strength evaluation method is providing the security for patient's data using their personal information. This method is to provide the strength of the password by the personal information basis, better than the previous methods. This method can easily and exactly identify the passwords and different forms of invisible variations which contains the personal information classification and context-free grammar of the label processing. This method split into three stages based on personal information. These are: 1. Personal information collection and extraction, 2. Classification and tagging, 3. Password strength calculation stage. The detailed procedure for above stages is provided as follow: In the first stage they are having different personal identification objects of users. In that some are collected of letters, such as hobbies and names; some are collected of numbers, such as date of birth and mobile numbers; and some are collected of permutation of numbers and letters, and exceptional characters, such as usernames. In this the password can construct directly by using some personal information attributes, such as date of birth or name; but some are not used for direct construction of password, such as academic level and gender.

In the second stage it uses the algorithm called PCFG to classify the gathered personal information into the segment of letters *L*, the segment of digit *D*, and the segment of special character *S*.

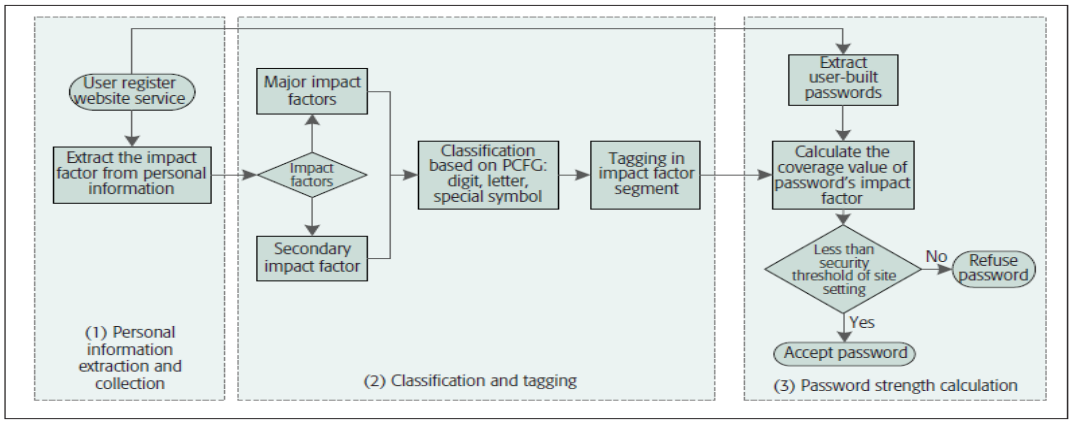

Fig 1: password strength evaluation method

In order to their impact levels, the personal information is split into two influence factors, i.e. major and secondary. For example, the major influence factors are date of birth and the user's name in segment of digit and segment of letter, respectively. By using tagging it can be represented and fully examine dissimilar variations in every field.

In the last stage it considers identify the particular variation of one of the label values of the impact factor in every field class. If detected any label value, it resume considering the coverage length value of impact factor's based on the moving window. The estimation of the password strength can be an integration of the personal information exposure value and other heuristic methods based on the keyboard style, length, regularly used delicate password list, and character structure.

B. Secure Transmission Model:

In this provide security in medical data transmission by using AES and RSA algorithms in IoT environments. This model create four continues procedure.

1. Using AES and RSA algorithms for build hybrid encryption scheme to encrypt the secret patient's data. 2. Using 2D-DWT-1L or 2D-DWT-2L to conceal the encrypted data in a cover image and produces a stego image. 3. Extracting the fixed data. 4. Retrieve the original data from extracted data by using decryption. Following fig.2 shows the process of model for securing the medical data transmission from source to destination.

Algorithm for Encryption of data using AES and RSA:

Step 1: Select the message for encryption.

Step 2: Split the given message into odd message and even message.

Step 3: Create AES key.

Step 4: Assign the odd message for encryption with 128 bits block size.

Step 5: Create RSA key.

Step 6: Assign the even message for encryption using RSA.

Step 7: Perform the both odd and even encryption text into full encryption text.

Step 8: AES and RSA operations are performed on text.

Step 9: The data will be encrypted and acquire the data as cipher text.

Algorithm for Embedding 2D-DWT-2L:

Step 1: Take the secret message and convert into ascii message.

Step 2: Split the message into odd and even.

Step 3: Scan the given cover image and compute by using 2D wavelet technique for the first level and generates level 1 low pass or high pass filters.

Step 4: And compute the second level to generate the level 2 low pass or high pass filters.

Step 5: Perform the loop to assign the odd values to low and high pass and even values to only high pass subbands.

Step 6: Stop the loop operation.

Step 7: The stego image was generated.

Algorithm for Extracting stego image:

Step 1: Take the stego image and scan row by row.

Step 2: Compute the 2D wavelet for the first level and second level by harr filters.

Step 3: Perform the loop operation for extracting the text and assigning the odd and even values.

Step 4: Stop the loop procedure.

Step 5: Append the odd and even values and assign to the message.

Step 6: Using idwt2 to generate original image.

Step 7: The message was retrieved from cover image and secret message.

Algorithm for decryption using AES and RSA:

Step 1: Take the cipher text and divide into hashed text and hashed key.

Step 2: Decompress the hashed text and assign to the full encrypt message.

Step 3: Decompress the hashed key and assign to the encryption key.

Step 4: Decrypt using AES 128 bit block size.

Step 5: Split the odd and encryption message to odd and even message also.

Step 6: Using AES for decrypting the odd message and RSA for even message.

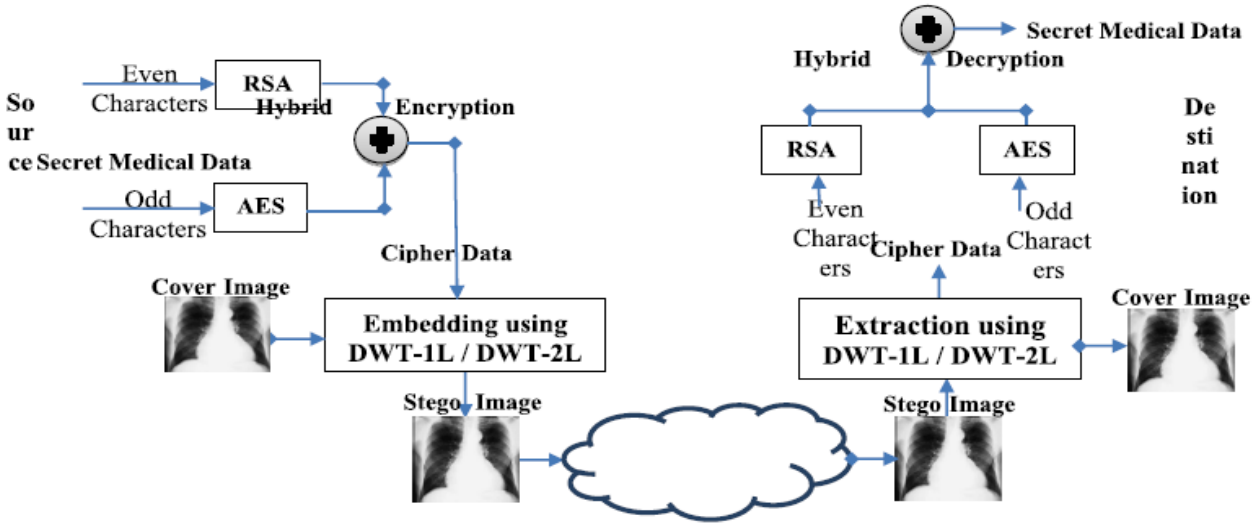

Fig 2: framework for securing the medical data transmision

Step 7: Perform loop operation to insert the odd characters into odd and even characters into even indices.
Step 8: End loop
Step 9: Acquire the plain message.

IV. EVALUATION PARAMETERS

Based on the following parameters the secure results are evaluated; the Peak Signal To Noise Ratio (PSNR), Bit Error Rate (BER), Mean Square Error (MSR), Structural Content (SC), Structural Similarity (SSIM).

A. Peak Signal to Noise Ratio:

It is an error metric to compare the image compression quality and measure the peak error. The higher is the value; it reveals stego image higher quality or hidden message imperceptibility. The following equation is used to calculate the PSNR.

$$\mathrm{PSNR} = 10\log_{10}\left[\frac{\mathrm{I}^2}{\mathrm{MSE}}\right]$$

Where, I is the no. of possible values of the pixel in the image and MSE is the mean square error.

B. Bit Error Rate:

The BER is calculate the no.of bit errors per unit time. It is no.of bits from the error divided by the total no.of transferred bits. The below equation is used to calculate the BER.

$$\mathrm{BER} = \mathrm{Errors}/\mathrm{Total\ no.\ of\ bits}$$

C. Structural Content:

It is based on correlation measure, in this also measures the two images similarity, and it is calculated by using below equation.

$$\mathrm{SC} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(y(i,\ j)\right)^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(x(i,j)\right)^2}$$

Where, y(i, j) is the twisted image and x(i, j) is the actual image.

D. Mean Square Error:

It is an error metric to calculate the average error between the stego image and actual image. The below equation is used to compute the MSE.

$$\mathrm{MSE} = \frac{1}{[\mathrm{R}\ \times\ \mathrm{C}]^2}\sum_{i=0}^{n}\sum_{j=1}^{m}\left(X_{ij} - Y_{ij}\right)^2$$

Where, R and C are the no.of columns and rows in the cover image, X_{ij} is the cover image pixel, Y_{ij} is the stego image pixel.

E. Structural Similarity:

It is measures the quality of the two digital images and it's recognize change in information. It has value range between -1 to 1. The SSIM value is 1 when the two images are nearly similar. The below equation is used to compute the SSIM.

$$\mathrm{SSIM} = \frac{\left(2\mu_x\mu_y\ +\ \mathrm{C1}\right)\left(2\sigma_{xy}\ +\ \mathrm{C2}\right)}{\left(\mu_x^2 + \mu_y^2\ +\ \mathrm{C1}\right)\left(\sigma_x^2 + \sigma_y^2\ +\ \mathrm{C2}\right)}$$

Here, average of x is denoted as μ_x, as well as y is μ_y, variance of x is denoted as σ_x^2, as well as y is σ_y^2, and covariance of x and y is denoted as σ_{xy}.

V. CONCLUSION

In the smart health care the IoT devices are irresistible targets for cyber malefactors. The smart IoT based devices provide low security counts in the actual world. In this it mainly concentrated on password guessing attacks. In this the password strength meter takes the patient's personal information to make the passwords strong. And also provide secure transmission model for patient's diagnostic data transmission. In that it uses the AES and RSA algorithms for encryption and decryption of the patient's data by using the wavelet transform technique 2D-1 level or 2D -2 level. The performance is evaluated from the following parameters (BER, PSNR, MSE, SC, and SSIM). In this the patient's diagnostic data can be hided in the cover image from the stego image having the capacity and high imperceptibility by using the transmission model.

Retrieval Number: K24100981119/19©BEIESP
DOI: 10.35940/ijitee.K2410.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

REFERENCES

1. Sheng, Zhengguo, et al. "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities." IEEE Wireless Communications 20.6 (2013): 91-98.
2. He, Daojing, et al. "Privacy in the internet of things for smart healthcare." IEEE Communications Magazine 56.4 (2018): 38-44.
3. Elhoseny, Mohamed, et al. "Secure medical data transmission model for IoT-based healthcare systems." IEEE Access 6 (2018): 20596-20608.
4. Al-Hamadi, Hamid, and Ray Chen. "Trust-based decision making for health IoT systems." IEEE Internet of Things Journal 4.5 (2017): 1408-1419.
5. Soria-Lorente, Anier, and Stefan Berres. "A secure steganographic algorithm based on frequency domain for the transmission of hidden information." *Security and Communication Networks* 2017 (2017).
6. Kamal, Preet, and Gagandeep Jindal. "Review of Different Steganographic techniques on Medical images regarding their efficiency." (2005).
7. Bala, B. Kiran, and A. Bala Kumar. "The Combination of Steganography and Cryptography for Medical Image Applications." *Biomedical and Pharmacology Journal* 10.4 (2017): 1793-1797.
8. Lavania, Shubham, Palash Sushil Matey, and V. Thanikaiselvan. "Real-time implementation of steganography in medical images using integer wavelet transform." *2014 IEEE International Conference on Computational Intelligence and Computing Research*. IEEE, 2014.

AUTHORS PROFILE

Dr. M Sunil Kumar has completed Ph.D in Computer Science and Engineering, S.V.University, TIRUPATI. M.Tech in Computer Science from JNT University. B.Tech in Computer Science & Information Technology from JNT University. He is currently working as Professor in the Department of CSE, Sree Vidyanikethan Engineering College, A. Rangampet, Tirupati, A.P. His main research interest includes Software Engineering, Software Architecture, Information Retrieval and Database Management Systems.

Mr. K. Jyothi Prakash pursuing PG in Computer Science in Department of Computer Science and Engineering from Sree Vidyanikethan Engineering College, Tirupati. B.Tech in Computer science and Engineering from JNT University Ananthapuram. Main research interest includes Computer Networks, Database Management Systems and Software Engineering.