International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

An ECPABE Algorithm and RPLS Protocol for Secured Transmission on IOT based Environment

K. Vijayakumar, Vijay Bhanu S

Abstract: ***WSN include Internet Protocol (IP) which extends the Internet of Things (IoT) related to routine life. Security is main thing in emerging technology for IOT application. Therefore, WSN has lot of issues which include: (i) To promote the sensor devices efficiently during the transmission of data for consuming low energy (ii) To resolve the security issues of data faced at the time of transmission through large area of networks. In this paper, to overcome the above issues the novel scheme is proposed. A Secure based smart home automation system in IOT application is built for this study. Furthermore, the data transmission utilizes the energy using Low power consumption protocol using RPLS and to secure the data a data security scheme ECPABE have been proposed here. The performance of proposed protocol shows the limited energy consumes and proposed ECPABE provides better security level to IoT data than the existing schemes. The results show the proposed scheme security analysis is efficient as well as secure.***

Keywords: Internet of Things (IoT), Smart Home Applications, Sensor Nodes, RPLS protocol, Enhanced Ciphertext Policy Attribute based Encryption (ECP-ABE).

I. INTRODUCTION

In IOT environment, routine life entities are related to internet due to its communication capacity and computing purpose. IOT extends the perception by using internet also it is feasible with verity of applications. Home automation system in IOT applications have two device namely actuator as a user and preceptor as a sensor device is placed in the home for manage then handle the computation operations. Then each device in the home is interconnected with local server through wireless channel to collect the data also analysis. The major issue is in what way the collected information is transferred securely from one source node to another destination node. As the result, lot of mechanisms is proposed system in WSN which solve the challenging issue security methods and traditional encryption techniques are built [1].

Manuscript published on 30 September 2019
* Correspondence Author
K. Vijayakumar[1], Department of computer science and Engineering, Annamalai University, Tamil Nadu, India. kmk.vijay@gmail.com
Dr. S. Vijay Bhanu[2], Department of Computer science and Engineering, Annamalai University, Tamil Nadu, India. Vbhanu22@yahoo.in

In network each device has resource limited which include controlled the power supply, data processing capability is limited, communication range as well as memory [2]. The second issue is in what way the energy is utilizes the resources for verity of IOT applications. Consequently the security based algorithm consumes less amount of energy for encryption usage that makes efficiently use the resource availability in their networks. Also smart home based IOT application has more than one device is interacting with internet with wide range of distance. Third issue is significant one that can be how efficiently increasing the coverage area to communicate with the network [3]. Therefore, the Smart home system in IOT application is highly secured which can be provide the equalized the level of security. The key generation mechanism for security algorithm based implementation efficiently using data encryption also network capability which support the various amount of IOT nodes for communication is needed in wide coverage area.

Moreover the IOT device is cheap also wireless device which require the energy efficient also robust. Device communication among the network is very difficult to identify because the device are heterogenous in nature. Heterogenous in distributed system is termed as node computation with differently so far, it is friendly, capability like RAM specification, and CPU frequencies may vary.

So, Heterogenous is more significant one in IOT. In IOT environment each devices are completely different in capabilities. For example, Assume Home security system provides variety of sensor provides various types of data like camera provide video type data, door device provides notification message whenever the door opens or close. Because of this kind of device is not possible to provide the regular fault tolerance techniques for IOT. The general architecture is shown in below figure.

This research paper organization is following as Section 2 discussed about the related works. Section

3 illustrates methodology part as well as the implementation results of proposed system are discussed in Section 4. At last, Section 5 concludes the overall work.

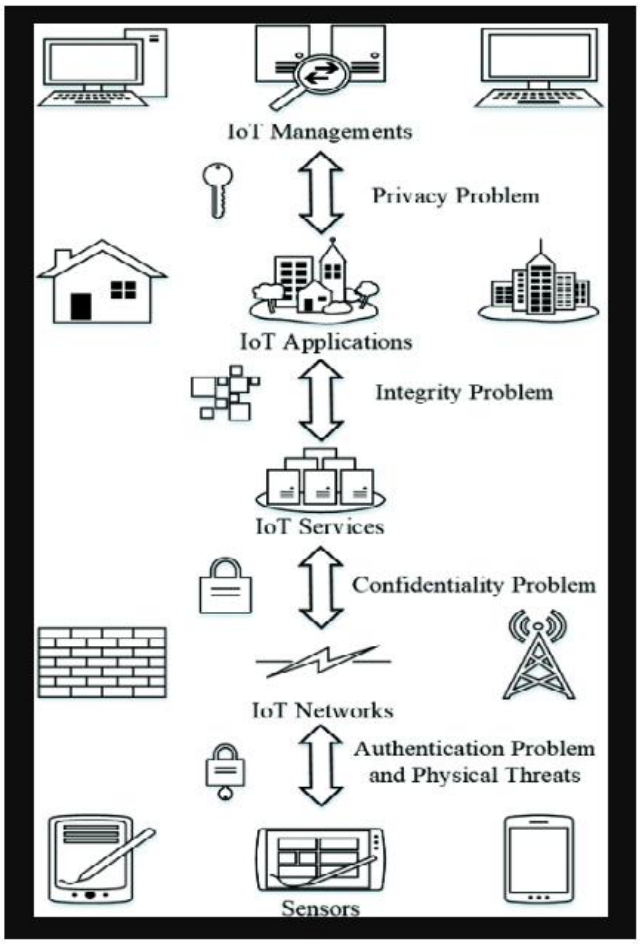

Fig.1. General Architecture of Smart home system

II. RELATED WORK

Currently, different types of protocols have been proposed for wireless networks that security issues are upgrade, network reliability also energy efficiency are needed to improve. The discussion can be carried out into two categories such as protocol based and data security based performance.

A. Energy efficient Protocol

Twayej et al, 2018,[5] an routing protocol efficiently utilize the energy in Wireless Sensor Networks (WSN) is discussed, that offers the platform control as well as M2M networks. If the node cause the energy efficient is insufficient then it is active in all the time to tackle the adaptive sleep mode solution that maintains Network Performance (N.P) in high levels. MLCMS protocol performance to evaluate then it is compared with the multi-hop low-energy adaptive clustering hierarchy (M-LEACH) protocol. The proposed MLCMS protocol achieves 62% when compared to M-LEACH then it achieves 147% energy efficiency effectively. Then, the proposed model 6LoWPAN is constructed also MLCMS performance impacts is evaluated by Network Simulator (NS3) simulation. The system which received the packets 7% gain when compared to MLCMS except the 6LoWPAN also improves the flexibility. Consequently, the sleep mode scheme is adaptive one which is based residual energy on CH's in active period time that can be introduced by MLCMS then it is establish comparative analysis which extends the system lifetime two times. Then it can be evaluated by MLCMS, it does not adaptive sleep mode algorithm. Additionally, the proposed system with the sleep mode algorithm, that can be reducing the delay as well as the delivery, is increased by 10%.

Sun et al, 2012 [6] recommended M2M application model which is using the existing method that interconnects the user and the home network called Time Division-Synchronous Code Division Multiple Access (TD-SCDMA) network. Later, the password-based authentication is designed as well as key establishment protocol is used to recognize the communicating parties and then protect the channel is established for transmissions of data. The proposed protocol result shows the reliability. The limitation of the work is secure architecture is designed for home network which focus on the low energy cost. After that, whole secure system is constructed by combination of two part i.e Energy saving [14] and security.

Harith Yahya et al, 2017 [7] proposed a received signal strength identification (RSSI) readings for controlled reverse-trickle timer to keep up the maximum responsiveness with least amount of overhead. The detection of objective function consultation when the node is moved or inconsistency that make the decision informed one. COOJA tool is used for simulations that can be used for various mobility scenarios of animal tracking and healthcare application which consider the multi hop routing protocol. The proposed dynamic RPL result shows the adaptability of various mobility scenarios as well as the PDR achieve maximum result, end to end delay is very low then the energy consumption[15] is reasonable one when compared to existing methods.

K. Frikken et al., [8] authentication protocol related to Physical Unclonable Function (PCF) which propose the zero-knowledge proof of knowledge (ZKPK) use of discrete logarithm. The protocol cannot make Challenge Response Pair (CRP) reveal any messages without using zero-knowledge proofs. Every time the user requires giving input a password to the device by using this protocol. In IOT system, authentication reduces the effectiveness of the protocol. This protocol is used to perform only authentication between the user as well as server then it cannot used for two devices each other for authentication.

Xiao Ni et al 2007 [9] discussed about new approach which realize the encryption operation commands by computed AES algorithm model with variable key as well as fixed key. In the protocol for AES security which is newly designed, protocol interrogation is engaged by using the key fob then radio device after that the key fob initiates a connection. Here, car dealer or car manufacturer is taken as fixed key then it can be used for handshake message then pseudo random number (PRN) of encryption purpose. The PRN is used for Key fob which can serve variable key. Today's attacker world, this method is effectively defeating the attacks like statistics attack, brute-force key guess attack, masquerade attack, etc.

B. Security oriented methods

Cristian Chilipirea et al 2016, [4] proposed new model which illustrated the device capability also utilize the data which is dynamically change the faulty device but it cannot matched directly. Still, this technique is used to device which is overlapped like that some part is temporarily disable as well as save the energy. Based on this study the home security system in IOT application[17], how the model is applied anywhere it is critical in robustness. For example, this system use heat sensor device, WiFi Scanner then door device instead of replaces the faulty security device camera. Finally it proves the two types of energy efficient model as well as fault tolerance model is offered. The proposed system is home security, which extended the environment like multi-room, multi-user. It is defined by the device capabilities like fuzzy based logic which means the camera device is forget to identify the person in 100% accuracy because it is combined with WiFi scanner so the accuracy is high.

Sandeep et al, 2017[10] developed IoT-based secure smart home automation system. Further the data encryption using energy efficient called Triangle based security algorithm (TBSA) which is related to key generation mechanism. The proposed method is combination of low power Wi-Fi in WSN also develop internet based Novel application that provide secure data transmission in wide range of network which is associate with sensor device node. The proposed model is excellent performance by satisfy the security requirement. The proposed TBSA algorithm results show energy consumption [16] is low when compared to existing model. The limitation of proposed method is implemented in various applications in IOT platform similar to agriculture,emergency response, medical monitoring, energy management, healthcare as well as industrial automation. Furthermore, efficient biometric-based security algorithm is developed which is based on Heart Rate Variability (HRV) is used to secure the present healthcare system in Wireless Body Sensor Networks (WBSNs). The parameters to be consider as Root-Mean Squared of the Successive Differences (RMSSD) as well as Standard Deviation of NN interval (SDNN) with Triangle based security algorithm that is used in WBSNs using entity identifications or key generation.

B. Vaidya et al. 2011 [11] illustrates the authentication scheme which is robust as well as efficient[19]. This scheme is based on strong-password approach that offers the digital home network environment is secured remote access. The lightweight computation scheme is proposed with low-cost smart card technology that contains the one time password with hashing then hash chaining technique. The main aim is to rectify the all security requirements like forward secrecy then stolen smart card attack also functional requirement like no time synchronization then verification table. The existing comparison of representative schemes are validated by the proposed scheme which is more robust in authentication by using enhanced security property. Finally conduct the proposed scheme formal verification.

Aqib Jamil et al 2019,[12] discussed smart home appliances optimization by using optimization techniques. The combination of Cuckoo search algorithm and earthworm optimization can be used for scheduling the smart home appliances. Based on three groups the Home appliances are classified then using real-time pricing scheme. Evaluate the techniques as well as comparison of performance. The hybrid technique proposed result shows the cost of electricity is decreased by 49% as well as compared with unscheduled cost. The trade off can be exists among the user comfort then electricity cost. Because of this the consumption of power is reduced while on-peak hours also. If the consumer need to minimize the waiting time of the electrical devices in home which can compromise the electrical cost. The future enhancement of the proposed system is integrated with pumped storage system for electricity generation while low prices and demand then it can be utilized in demand hours and high price. Additionally, this system can be focused on smart home coordination to sell the extra electricity produced by consumers.

Niksa Skeled zija et al, 2014 [13] discussed about the modern smart monitoring and control system implementation as well as concept of building automatization. To design the systems which enable the energy consumption reduction significantly then carbon footprint build under the control can be increased by energy efficiently [15]. The optimized energy flow of Model Predictive Control (MPC) algorithm to run the control unit. The WSN may collect the data using MPC algorithm to calculate as well as the requirements are estimated from heat corrections related to weather prediction then ventilation. The limitation is proposed system functionality is providing the service and extra modules like remote access system control, smart entry control subsystem, human behaviour patterns learning as well as monitoring, configuring then controlling the system configuration through tablet or smartphone [20] etc.

III. EXISTING METHOD

Identity-based encryption

The scheme identity-based encryption (IBE) which include four probabilistic polynomial-time algorithms:

IBE.Setup(1^{λ}) The setup algorithm takes as input a security parameter 'λ'; it outputs some '*pms'* public parameters and '*msk'* master secret key.

IBE.KeyGen(*id,msk,pms*) The key generation algorithm takes master key *msk* as input, the public parameters *pms* then the identity $\mathrm{id} \in \{0,1\}^*$. The private key sk_{id} as output.

IBE.Encryption(*m,id,pms*) For encryption algorithm, '*pms'* public parameters take as input, a message '*m'* and identity *id*. Ciphertext '*C* 'is output.

IDE.Decryption(*C,id,* sk_{id}*,pms*) For Decryption algorithm, Ciphertext *C* is input, an identity id, 'sk_{id}' Secret key and '*pms'* public parameters. Finally the output is Message '*m'*.

The property of correctness requires that,if the following four protocols are

$$run(msk, pms) \leftarrow IBE.setup(1^{\lambda})$$

sk_{id}←IBE.keyGen(id,msk,pms),

C←IBM.Encrypt(m,id,pms) then

$\tilde{m} \leftarrow IBE.Decrypt(C, id, sk_{id}, pms)$,

then it holds $\tilde{m}$=m.

This scheme utilize integer factorization problem to design the IBE scheme.

IV. PROPOSED METHODOLOGY

The proposed methodology include two modules: In the first module the data are collected via various sensor nodes in home environment. The home user will collect the data using a novel low energy consumption using RPLS protocol. The second module is transferring the data with enhanced ciphertext Policy attribute based encryption (ECPABE) algorithm.

A. Low-Energy Consumption Protocol using RPLS

The basic Routing Protocol for Low Power and Lossy Networks (RPL) offers the reality of IOT environment. This protocol provides the Spatial diversity, Expressive link, Routing State Propagation also node metrics. RPL performance is evaluated by using metrics to monitor the network behavior performance.

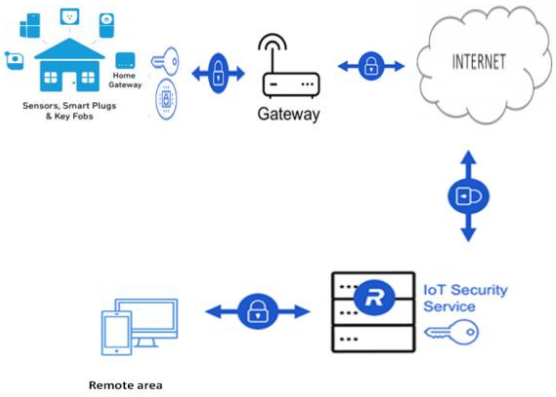

Figure 2: The overall architecture for our proposed system

The Proposed protocol is RPL using Scheduling called RPLS. Based on the scheduled time the data can be collected from the sensor device and move to the user end. The aim of the protocol simulation is identify the node behavior also monitor the RPLS performance with given circumstance based on the performance metrics like latency, packet delivery ratio, power consumption then communication overhead. The RPLS protocol flow can be explained below figure 3. The algorithm of the RPLS protocol can be shown below.

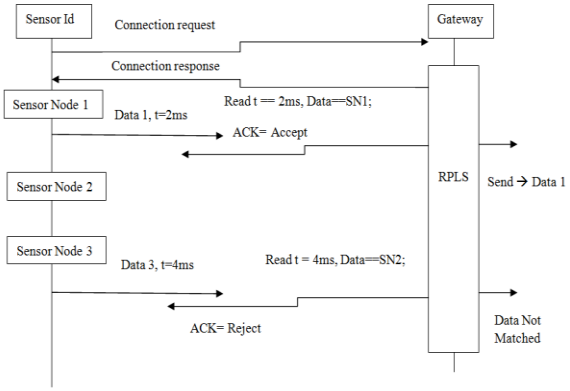

Fig.3.Protocol for RPLS

Algorithm: RPLS Protocol

If(receiving a message for first time)
{
compute $Data_i$ based on Sensor $Node_i$
create list ($Data_i$, time)
}
Send message with new data
}
for(t=2ms;SN=i&&Data= i; t+2)
if (new $data_i$= =SN_i)
{
ACK accept;
Else
ACK reject;
}

B. Proposed Enhanced Ciphertext Policy Attribute Based Encryption (ECPABE) Algorithm

In this environment, the smart home has user's assistance, various types of data is transfer among various smart devices, users and then gateways. The data can be secured from hacker using various security measures are applied also that information is simply-sensed like personal information, images, voice note which is related to the user directly or indirectly. That's why security measures require the following security requirement.

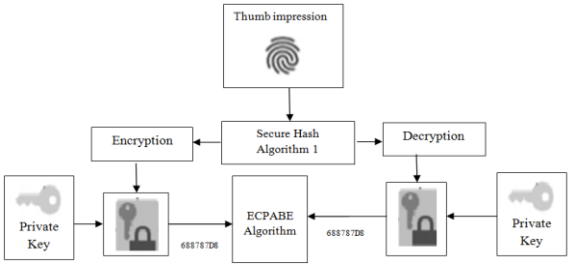

Fig.4.Security Requirement Architecture

Here, the encryption process uses the public key such as the sensor node ID's, user attributes etc and the private key is very unique which may contain the confidential attributes of user such as biometric features of the authorized user. The System setup and security model of ECPABE has given below which includes the model for Encryption, Decryption and Key Generation. Our proposed ECPABE scheme is comprised of four factors. The algorithm is defined as follows:

ECPABE Algorithm

Setup, KeyGen, Encrypt, Decrypt.

- ***Setup(1λ):*** The '*MSK' as* master key *and* '*PK'* public Key is created which is related to security factor '1λ' .
- ***KeyGen(PP, MSK, AL):*** '*SK* ' as Secret key is created for decryption to the users which is related to '*PK*' Public Key and '*MSK' as* master key finally '*AL' as* attribute list .
- ***Encrypt (PP,* M,W*):*** create the ciphertext related to '*PK'* public Key , 'M' as message plaintext and 'W' as predefined access structure .
- ***Decrypt (CT, SK):*** the '*CT' as* ciphertext is Decipher by using '*SK'* as *S*ecret Key *for* decryption.

Security Model

An ECPABE based security scheme is well secured against selectively preferred the plaintext attack through the security based game among Node A to Node B.

- **Init**: The 'AL' as attribute list of targeted challenge is chosen by the challenger A.
- **Setup**: First given security factor 1λ then execute B using *Setup* algorithm to create the master key 'MSK' and the A delivered the 'PP' public parameter.
- **Challenge**: After obtaining 'M0' and 'M1' from A with identical length , B replies the A based on the 'CT' as ciphertext challenge with successively Encrypt *'(PP, W, M, ζ)'* , where *ζ∈{0,1}*

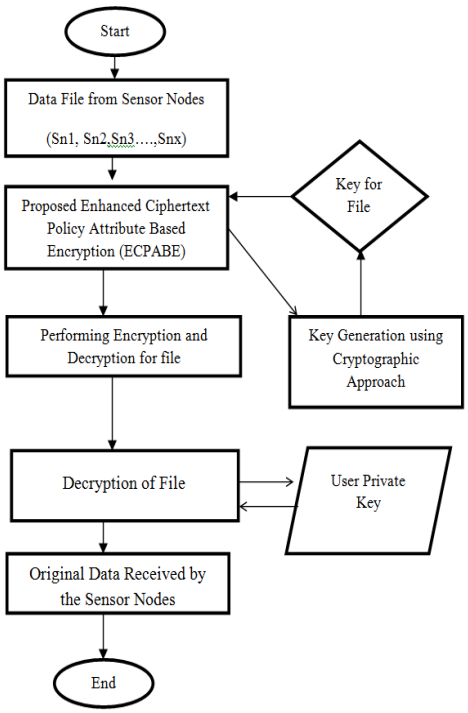

Fig.5.Flow chart of proposed approach

Encryption: "*(PK, S, ck) → CT":* uploading a file M earlier, the algorithm for file encryption process as follows:

- the encryption key 'ck' is selected from key space, then encrypts the original file 'M' symmetrically by encryption key 'ck' to achieve "$E_{ck}(M)$".
- the access structure set $w = v_1, v_2 \ldots . v_n$, which encryptions process of "ck" then resultant encryption key of ciphertext 'ck' by using the following steps.

The algorithm which make the input as 'PK' the public key , 'S' is access policy then the encryption key value is 'ck'. Also choose randomly $s \in Z_p$, which compute "C = ck·Y^{s}" then "C1 = g^{s}", and select the value randomly $s_j \in Z_p$ like $s = \sum_{s=1}^{n} s_j$, computes $C_{j,1} = X_j^{s_j}$ then $C_{j,2} = u_j^{s_j}$.

Choose $z_1, z_2, z \in \mathbb{Z}_p$ and compute

$$C_0 = M \parallel z \oplus \mathcal{H}_1\left(u_1^{z_1} v_1^{z_2}\right), C_1 = M^z . \mathcal{H}_2\left(u_2^{z_1} v_2^{z_2}\right)$$

$$C_2 = g^{\frac{\alpha z_1}{t\omega}}, C_3 = g^{\frac{z_2}{t\omega}}, C_2^{'} = g^{\frac{\alpha^{'} z_1}{t\omega}}, C_3^{'} = g^{z}$$

$$C_4 = \left(W_1 \prod_{i \in X} R_i^{\frac{\prod_{k=0}^{l_1}(i-\omega_k)}{t\omega}} \right)^{z_1+z_2}$$

$$C_5 = \left(W_2 \prod_{i \in Y} R_i^{\frac{\prod_{k=0}^{l_1}(i-\omega_k)}{t\omega}} \right)^{z_1+z_2}$$

Return $CT = C_0, C_1, C_2, C_2', C_3, C_3', C_4, C_4', C_5, J$

Accordingly, the encryption ciphertext key ck as follows:

$$CT = (C, C_1, \{(C_{j,1}, C_{j,2})\}_{j \in [1,n]})$$

At last, the result of algorithm is the ciphertext as "C_{ph} = (Index, E_{ck} (M), CT)".

Decryption: "(SK_2,*CT*)→*ck"*:

The algorithm which make the input data is user's secret key 'SK_2'then encryption ciphertext key "*CT"*.

If user's data attribute list '*Attr'* satisfy the '*S' as* access policy fixed in the ciphertext, then the algorithm which decrypts "*CT"* to achieve the encryption key '*ck'* is following as:

$$ck = \frac{C \prod_{j=1}^{n} e(C_{j,1}, D_{j,2})}{e(C_1, D_1) \prod_{j=1}^{n} e(C_{j,2}, D_{j,1})}$$

At last, the symmetric decryption algorithm for decrypt "$E_{ck}(M)$" is used through the encryption key '*ck* ' to retain original file '*M'*.

$$v_1 = \frac{e\left(\prod_{j=1}^{l1} sk_{3,j}^{awj}, C_2\right) e\left(\prod_{j=1}^{l1} sk_{3,j}^{'} a_{wj}, C_3\right)}{e(sk_1, C_4)^{t_{x'}}}$$

$$X \frac{e\left(\prod_{j=1}^{l1} sk_{4,j}^{awj}, C_2\right) e\left(\prod_{j=1}^{l1} sk_{4,j}^{''} a_{wj}, C_3\right)}{e\left(sk_{2}^{'}, C_5\right)^{t_{y'}}}$$

$$v_2 = \frac{e\left(\prod_{j=1}^{l1} sk_{3,j}^{awj}, C_2\right) e\left(\prod_{j=1}^{l1} sk_{3,j}^{'} a_{wj}, C_3\right)}{e\left(sk_{1}^{'}, C_4\right)^{t_{x'}}}$$

$$X \frac{e\left(\prod_{j=1}^{l1} sk_{4,j}^{awj}, C_2\right) e\left(\prod_{j=1}^{l1} sk_{4,j}^{''} a_{wj}, C_3\right)}{e\left(sk_{2}^{'}, C_5\right)^{t_{y'}}}$$

$$M||Z = C_0 \oplus H_1(V_1)$$

Key Generation

The key generation is process of creating the private key for the individual user which is based on the public key. The thumb impression is converted as the digital 42 bit sequence using SHA 1 algorithm. The Flow chart of Key generation process is shown below.

SHA1 (Secure Hash Algorithm)

A hash function which maps the data of an arbitrarily large size into fixed size. This is fundament one because each user have unique fingerprint data. A cryptographic Hash Code function which to generate a hash code by using a cryptographic function. Assume, SHA-1 Hash is used by Git repositories for ensure a fingerprint remote repository which is in connected with a master repository.

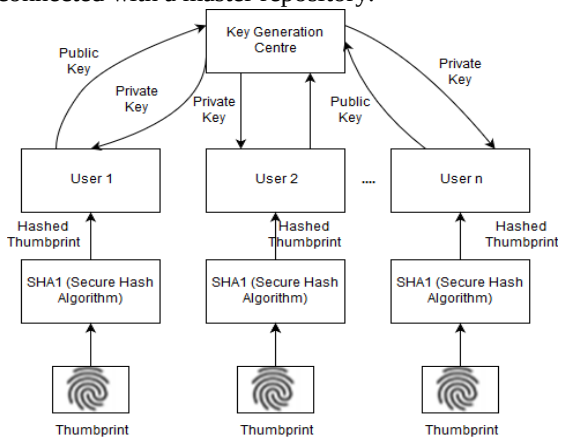

Fig.6.Key Generation Process

The property of cryptographic hash function that hash based message deduction is impossible. For security purpose it is important one, the hash code data might be transferred; however the actual data cannot bother about it.

V. EXPERIMENTAL RESULTS

The performance analysis is done for both energy efficient protocol and security scheme. The proposed Enhanced Ciphertext Policy Attribute based Encryption (ECPABE) Algorithm is compared with Identity based Encryption (IBE) based on encryption-decryption time and computational cost. On the other side a novel RPLS is compared with scheduling based energy efficient protocol (SBEP) in terms of energy consumption, throughput, and time.

Table 1: Performance Measurement Table using Proposed ECPABE Security Scheme

Sensor Device ID	Data File	Encrypted File	Time (ms)	Decrypted File	Time (ms)
Sn1	1333263600,116.5,1.1,60.0,1.0,0.98,132,0,9,0,135,0	2 @L³%¬Ûð'|é,} • ´Š\4OÐ c #Sc–É?"|Ï&+¾ • áöÃ/	40.25	1333263600,116.5,1.1,60.0,1.0,0.98,132,0,9,0,135,0	33.8
Sn3	16-12-2006,17:24:00,4.216,0.418, 234.84,18.4,0,1,17	2 @³¡gÀbs‹ŽC¥ÝÛøw6ªèS • — ú-¦Ák¯ó•z,'	47.73	16-12-2006,17:24:00,4.216,0.418 ,234.84,18.4,0,1,17	36.18

Sn2	0,-0.999750,12.862100,10.368300,10.438300,11.669900,13.493100,13.342300,8.041690,8.739010,26.225700,59.052800	m €ƒ_'¼‹µ m^ÚÖª@~mQãjùêÆq÷–öéÎ© ¶¶!¬œ†ÆÖDFýÓ;eoÝO()	65.34	0,-0.999750,12.862100,10.368300,10.438300,11.669900,13.493100,13.342300,8.041690,8.739010,26.225700,59.052800	49.49

Table 2: Comparison of Proposed Security Scheme with Existing Security Algorithm

Sensor Node Data File	Proposed ECPABE Algorithm Security Scheme			Existing Identity Based Attribute (IBE) Security Scheme		
	Encrypt_Time (ms)	*Decrypt_ Time (ms)*	*Data Privacy*	*Encrypt_Time (ms)*	*Decrypt_Time (ms)*	*Data Privacy*
1333263600,116.5,1.1,60.0,1.0,0.98,132,0,9,0,135,0	40.25	33.8	Strong	63.8	59.72	Partially Strong
16-12-2006,17:24:00,4.216,0.418,234.84,18.4,0,1,17	47.73	36.18		72.5	67.43	
0,0.999750,12.862100,10.368300,10.438300,11.669900,13.493100,13.342300,8.041690,8.739010,26.225700,59.052800	65.34	49.49		97.31	83.67	

The above table 2 shows the overall performance of proposed system which is strongly in data privacy when compared to existing system.

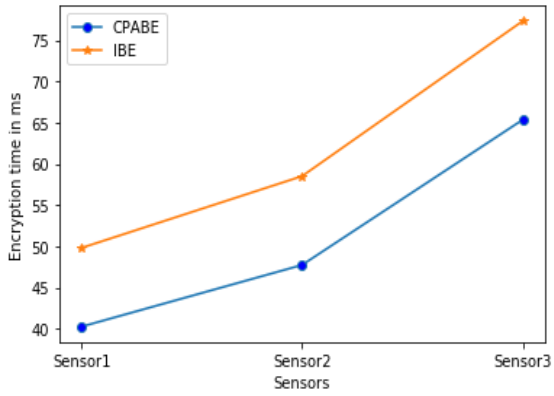

Fig.7. Encryption time

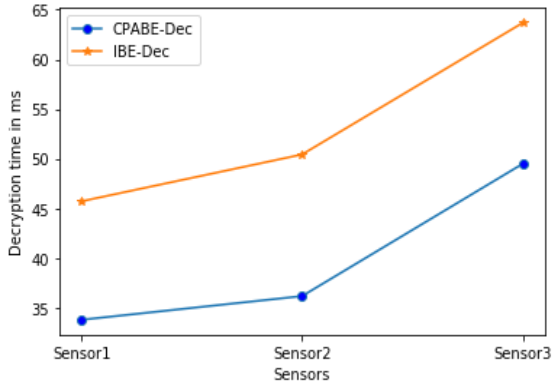

Fig.8. Decryption time

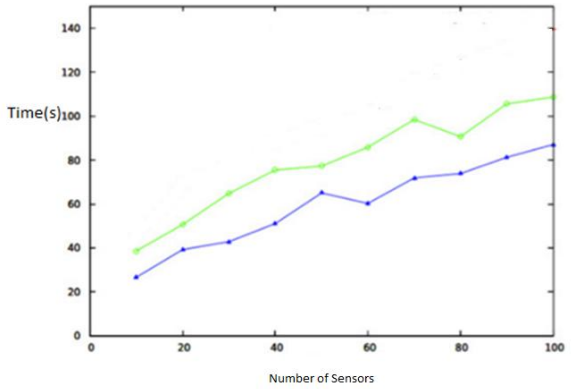

Fig.9.Data privacy for proposed and existing method

The above figure 9 shows the data privacy graph comparison of proposed and existing methods. The green and blue color line indicates Proposed ECPABE algorithm and Existing IBE based Algorithm respectively. The proposed method is compared to existing method which achieves better results.

VI. CONCLUSION

In this paper present a modified RPL with the approach of Scheduling, the data transmission utilizes the energy using Low power consumption protocol and to secure the data a data security scheme ECPABE have been proposed. The RPLS protocol is important for the improved results in a wide range of sensor IOT based applications. Further energy-efficient data encryption, a method namely Proposed Enhanced Ciphertext Policy Attribute based Encryption (ECPABE) Algorithm based on well-organized data security mechanism was proposed. The developed IoT based system has performance is outstanding to satisfy the security requirements.

The result shows the proposed ECPABE algorithm which consumes smaller amount energy with existing method comparison. The experimental results that reveal RPL is suitable protocol for smart home automation system. In future scope, the encryption based algorithm contains various computational rounds which utilize the memory usage which is unsuitable for IOT.

The major concern for IOT device is memory utilization in resource constrains. To analyse the memory usage as well as time taken for computation in algorithm utilization.

REFERENCES

1. Mondal, B.; Priyadarshi, A.; Hariharan, D. An improved cryptography scheme for secure image communication. Int. J. Comput. Appl. 2013, 67, 23–27.
2. Castagnetti, A.; Pegatoquet, A.; Le, T.N.; Auguin, M. A joint duty-cycle and transmission power management for energy harvesting WSN. IEEE Trans. Ind. Inform. 2014, 10, 928–936.
3. Ahmed, N.; Rahman, H.; Hussain, M.I. A comparison of 802.11 AH and 802.15. 4 for IoT. ICT Express 2016, 2, 100–102
4. Chilipirea, Cristian & Ursache, Andrei & Octavian Popa, Dan & Pop, Florin. (2016). Energy efficiency and robustness for IoT: Building a smart home security system. 43-48. 10.1109/ICCP.2016.7737120.
5. Twayej, Wasan & Al-raweshidy, Hamed. (2018). M2M Routing Protocol for Energy Efficient and Delay Constrained in IoT Based on an Adaptive Sleep Mode. 10.1007/978-3-319-69266-1_15.
6. Xuebin Sun, Shuang Men, Chenglin Zhao and Zheng Zhou, "A security authentication scheme in machine-tomachine home network service", Journal of security and communication networks, pp.1-9, 2012.
7. Kharrufa, Harith & Al-Kashoash, Hayder & Kemp, Andrew. (2019). RPL-based routing protocols in IoT applications: A Review. IEEE Sensors Journal. PP. 1558-1748. 10.1109/JSEN.2019.2910881.
8. K. Frikkenet. al., "Robust Authentication Using Physically Unclonable Functions", In: P. Samarati et al. (eds.): ISC 2009, LNCS 5735, pp. 262-277, Springer, Heidelberg 2009.
9. Ni, Xiao, Shi, Weiren, Fook, Victor Foo Siang, "AES Security Protocol Implementation for Automobile Remote Keyless System", IEEE 65th Vehicular Technology Conference, 2007.
10. Sandeep Pirbhulal, Heye Zhang, Md Eshrat E Alahi, Hemant Ghayvat, Subhas Chandra Mukhopadhyay, Yuan-Ting Zhang and Wanqing Wu, "A Novel Secure IoT-Based Smart Home Automation System Using a Wireless Sensor Network", Journal of Sensors, vol. 17, iss. 69, pp. 1-19, 2017
11. Binod Vaidya, Jong Hyuk Park, Sang-Soo Yeo, Joel J.P.C. Rodrigues, "Robust one-time password authentication scheme using smart card for home network environment", Journal of Computer Communications 34 (2011) pp. 326–336.
12. Jamil A., Javaid N., Khalid M.U., Iqbal M.N., Rashid S., Anwar N. (2019) An Energy Efficient Scheduling of a Smart Home Based on Optimization Techniques. In: Barolli L., Xhafa F., Javaid N., Enokido T. (eds) Innovative Mobile and Internet Services in Ubiquitous Computing. IMIS 2018. Advances in Intelligent Systems and Computing, vol 773. Springer, Cham
13. Niksa Skeled ˇ zija, Josip ˇ Cesi ´ c, Edin Ko ´ co, Vladimir Bachler, Hrvoje Nikola Vu ˇ cemilo, Hrvoje D ˇ zapo, "Smart Home Automation System for Energy Efficient Housing", IEEE 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) , 26-30, 2014.
14. P. U. B. Albuquerque,· D. K. de A. Ohi · N. S. Pereira · B. de A. Prata · G. C. Barroso, "Proposed Architecture for Energy Efficiency and Comfort Optimization in Smart Homes", Journal of Control, Automation and Electrical Systems, Springer, Brazilian Society for Automatics–SBA, 2018.
15. Zeeshan ALI KHAN, Ubaid ABBASI, " An Energy Efficient Architecture for IoT Based Automated Smart Micro-Grid" , Technical Gazette 25,vol. 5,pp. 1472-1477, 2018.
16. Brennan D. Less , Spencer M. Dutton, Iain S. Walker, Max H. Sherman, Jordan D. Clark, Energy savings with outdoor temperature-based smart ventilation control strategies in advanced California homes, Energy & Buildings (2019).
17. Yajing Pang and Sujuan Jia, " Wireless Smart Home System Based On Zigbee", International Journal of Smart Home Vol. 10, No. 4 (2016), pp. 209-220.
18. Jianfei Yang, Han Zou, Hao Jiang, and Lihua Xie," Device-free Occupant Activity Sensing using WiFi-enabled IoT Devices for Smart Homes", IEEE Internet of Things journal, pp. 2327-4662, 2018.
19. George Stamatakis, and Elias Z. Tragos and Apostolos Traganitis, "Energy Efficient Policies for Data Transmission in Disruption Tolerant Heterogeneous IoT Networks", Sensors, Vol. 18,pp. 2891-2906 , 2018.
20. Omkar Bhat, Sagar Bhat, Pradyumna Gokhale, "Implementation of IoT in Smart Homes", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 12, December 2017.