ISSN Application No. 21726

Global Journal of Computer and Internet Security

Volume No. 11

Issue No. 3

September - December 2023

ENRICHED PUBLICATIONS PVT. LTD

S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR-5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-47026006

ISSN Application No. 21726

Global Journal of Computer and Internet Security

Aims and Scope

The Journal of Computer and Internet Security presents research and development results of lasting significance in the theory, design, implementation, analysis, and application of secure computer systems. It also provides a forum for ideas about the meaning and implications of security and privacy, particularly those with important consequences for the technical community.

ISSN Application No. 21726

Global Journal of Computer and Internet Security

(Volume No. 11, Issue No. 3, September - December 2023)

Contents

Augmented Cloud Security with Performance using Machine Learning

[1] Majjaru Chandra Babu, [2] Sheba Pari N, [3] Senthilkumar K
[1,2]Reasearch Scholar, VIT University, Vellore, India
[3]Associate Professor, VIT University, Vellore, India
E-mail: [1]chandrasoft504@gmail.com

ABSTRACT

Cloud computing is a rapid technology which increases day by day to store, share and process personal and public data. In this connection, users can access the data through the internet which are processed through the cloud servers. When outsourcing user's data among servers using network usually attacks from the different security issues, where security plays a significant role, therefore security and privacy are the major challenging issue due to extensive consent all over the globe, new risks and vulnerabilities have appeared too. In this paper, we recommended a framework that fragments the data concerning the security constraints. When we compare the performance of existing technologies is drastically improved by adding it with a machine learning technique. Where the basic algorithms of machine learning technique i.e. base and Meta level techniques are reformed, this will improve the prediction and classification accuracy among existing methods.

Keywords - Cloud Computing, Machine Learning, KNN Techniques, Privacy, Security, Classification.

I. INTRODUCTION

Machine learning can support in business and other data storage levels to identify the threats and respond. In this connection for data classification in cloud level we used to implement machine learning technology; here data classification is a process of typical category for primary data classification supporting with build classifier. A training set of familiar datasets makes the classifier. To construct a suitable classifier, a massive volume of trained data sets is required. This expansion negotiations new models where servers present data classification in a cloud to its various clients/users. Explicitly, when the server processes the data automatically on remote servers. However untrusted third party-servers can access the private data.

Furthermore, every vigorous detail or training dataset specifications may not be revealed by the servers even if it delivers the classification services to its customer. Thus, a scheme that ensures the privacy of the server's training set and client dataset is required. Hence, a re-encryption framework is essential prerequisite to forestall the revoked user from accessing the encrypted information as well as to generate reliable keys for valid users. Therefore, in this paper a hybrid re-encryption model based on index classification which wills categories the data from sensitivity.

II.RELATED WORK

Cloud users have significant advantages over the internet to make use the data storage, availability, and privacy. Besides, the data is stored on different servers so that the user can access or make an application the information anywhere and anytime. Customers have access to public information that increases their collaboration. Access to the cloud archive will be cheaper as there is no need to accept expensive hardware. Also, the cloud backup, arguments and files can be quickly restored. Despite these cloud-based benefits, there are considerable limitations. Outside the open cloud, there is information on external servers and cannot be managed by legal users. Data available to unauthorized customers globally and the cloud computing model is not safe.

Problems of cloud computing have been discussed from the customer's perspective [3]. Main security issues to address Information security and privacy. Many methods, such as Aravat, have been proposed to protect data. The technique used is not practical and is based on different methods of modelling.

To provide information system in the cloud, AES method [4] was used to store user data on cloud servers.

Details, Privacy Information and Cloud Quantization Issue, Discussed [5]. This document uses several methods such as KP-ABE, reception methods (proxy and laziness). Cryptography and steganography techniques were used to preserve the author's data and information [6]. This model is a three-stage data protection module designed to protect user data. Dimensions: The use of cryogenic algorithms for RSA, data masking with concise technique and finally the encryption of data access using the RSA algorithm.

The sample [7] analyzed a data classification model that allows for overhead and minimum processing time. In this article, another security mechanism is analyzed with a different key length, which guarantees data privacy. Various encryption algorithms analyzed this model for better resultsregarding reliability and efficiency. The lack of documentation explained that the automatic classification of the data is required. Besides, more secure encryption algorithms like RSA require cryptography of an elliptical curve.

[2] The Privacy-based Data Classification Model for Cloud Computing has been proposed. In this work, the K-NN method (near neighboring K) is used to classify data. Determines what information should be disclosed to what data is saved. K-NN data is used for classification. The data is classified as sensitive and sensitive. Secret data is protected using the RSA algorithm and master data collected on cloud servers. Lack of documentation The RSA algorithm is only used for confidential data. In addition, the automatic classification of the K-NN model (basic, confidential, most confidential) was not implemented.

Previously used techniques were used to encrypt information without regard to their sensitivity level. Encryption of all data to customers is very expensive to reduce costs. Start by dividing the various categories (most confidential, confidential, or standard) data, and then apply coding procedures to sensitive data. It will help save encryption/decryption time, but it will also be economical for consumers.

III. PROPOSED WORK

Data classification will determine the data sets according to their value. These values depend on limits on user data and access control methods [8]. The study will look for different algorithms to classify learning data, such as KNN, Nave Bayes and modified algorithms of Naïve Bayes, and analyze their performance.

3.1 Cloud simulation environment:

The cloudsim shown in Figure 1 is used for the proposed model, which addresses the issue of privacy and data classification. We first emulate and then we create data centers. VMM (Virtual Machine Manager) is used to organize virtual machines and allocate virtual machines to cloud-based blacks or cloudlets. Only authentic users can perform an authentication process to access data.

3.2 Data Classification:

Apply the improved Naïve Bayes algorithm for classification.

Classification procedure stepwise

Step1- Joining Decision table with Naïve Bayes to deploy Meta classifier as the decision tree

Step-2 Here predictions of the base learners are given as input to the meta-learner. Where meta-learner is a scheme that merges the out of the base Lerner models. i.e. Level-0 and Level-1.

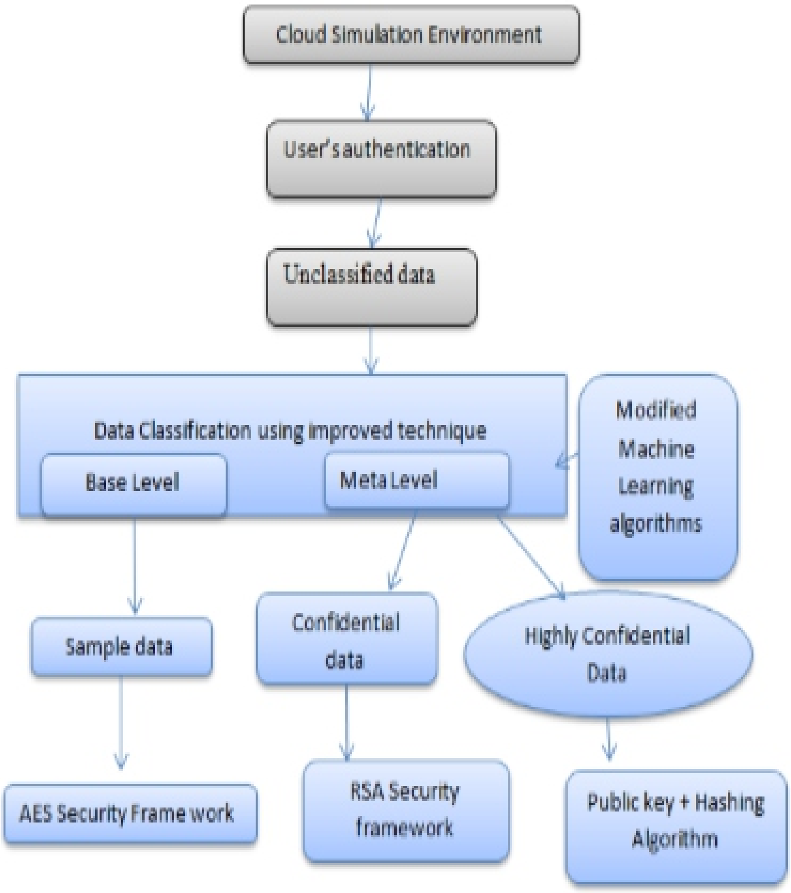


Figure 1: Proposed Model

Here classification KNN is union with updated learning techniques. Finally this leads the predications abilities and correctness of present KNN.

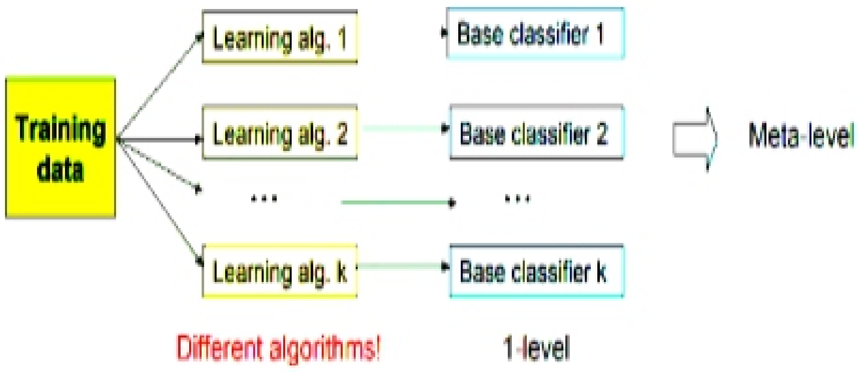
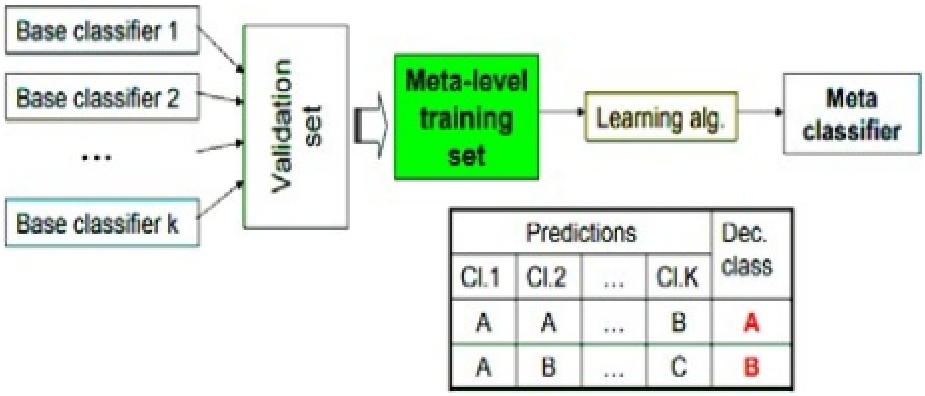


Figure 2. Level-1 Classifier using Base and Meta layers

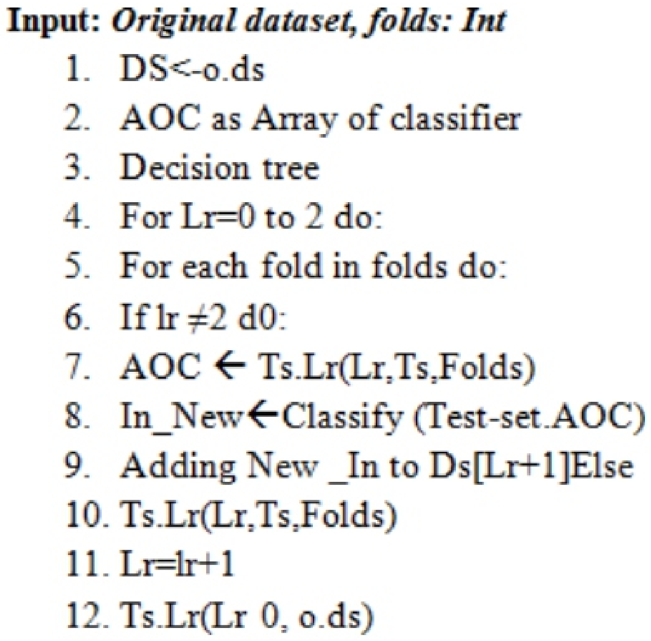
• As per shown figure 2. By applying several learning algorithms we can generate Base classifiers i.e Nearest Neighbor, Naive Bayes, Decision Trees to the similar data.



Predictions				Dec. class
Cl.1	Cl.2	...	Cl.K	
A	A	...	B	A
A	B	...	C	B

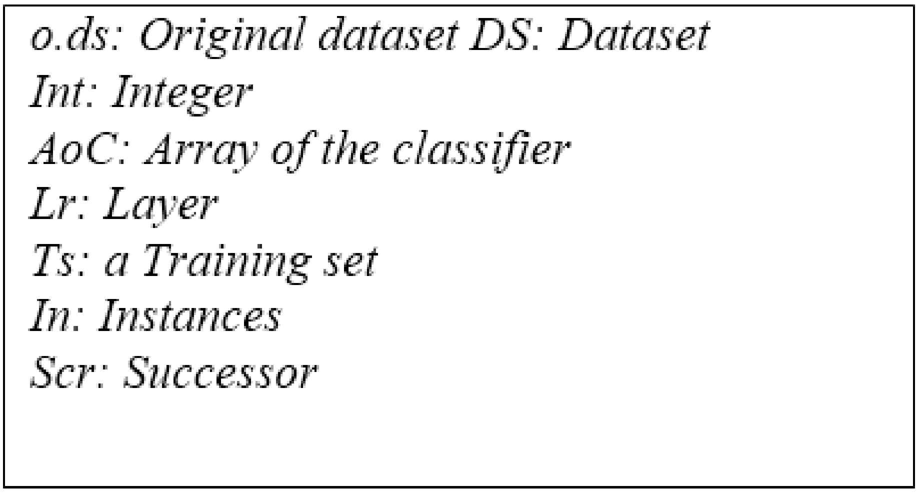
Figure 3. Learning Meta-Classifier

Base classifiers Predictions in the additional certification set with correct class decisions → with a meta-level learning set. The other learning algorithm is used to build meta-classifier. Meta-classification seeks to learn the relationship between the predict and the final decision;



```
Input: Original dataset, folds: Int
DS<-o.ds
AOC as Array of classifier
Decision tree
For Lr=0 to 2 do:
For each fold in folds do:
If lr ≠2 d0:
AOC ← Ts.Lr(Lr,Ts,Folds)
In_New←Classify (Test-set.AOC)
Adding New _In to Ds[Lr+1]Else
Ts.Lr(Lr,Ts,Folds)
Lr=lr+1
Ts.Lr(Lr 0, o.ds)
```

Where:



o.ds: Original dataset DS: Dataset
Int: Integer
AoC: Array of the classifier
Lr: Layer
Ts: a Training set
In: Instances
Scr: Successor

3.3 Data Encryption Architecture

Basic: Every uploaded data must be encrypted for the sake of security using AES algorithm

Confidential: for security reason, every uploaded data will be encrypted using RSA algorithm

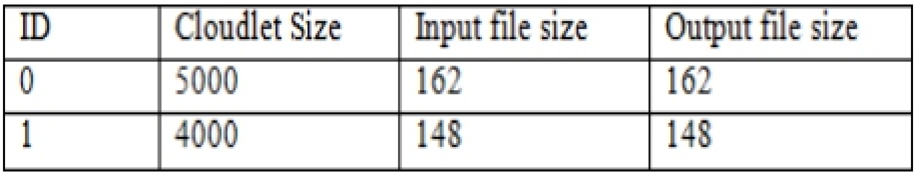
Highly confidential: for high-end sensitive data, to provide the security we use the hybrid model which consist of elgammal and hashing algorithm.

The significant objective of the proposed algorithm is to get useful results than the presented algorithm like KNN it depends on fundamental parameters like classification time, security at cloud integrity and data integrity level.

The valuation constraints taken into account for the assessment of the effectiveness of the proposed system are: (a) the time available for the classification of the data; (b) the accuracy of the classified data; (c) true positive rate; (d) the encryption time; (e) decryption time Features and description of a cloud service model. Before starting the simulation, SaaS (software as a service), PaaS (platform-to-service) and IaaS (infrastructure-to-service) features have to be considered. Fixed. The features are as follows: Table 1: SaaS model features are implemented with virtual machines in a simulation environment. ID = non- specific cloud-based identification. Length = Cloudlet size. I/O file size is measured bytes.

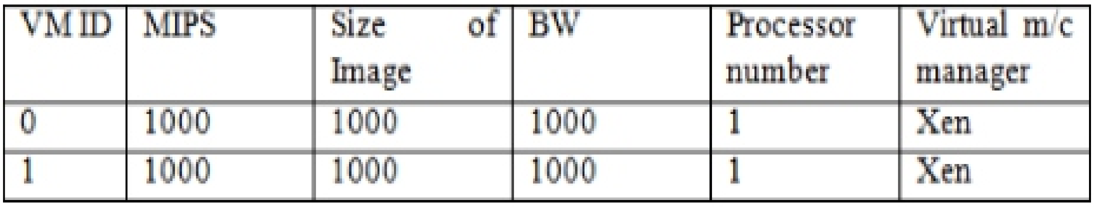
Estimated parameters considering the performance of the proposed system performance:
A) Classification data takes time.
B) The accuracy of classified data.

Table 1: SaaS model attributes



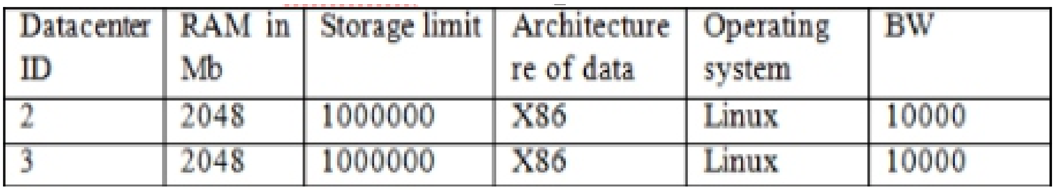
ID	Cloudlet Size	Input file size	Output file size
0	5000	162	162
1	4000	148	148

Table 2: The properties of VM in PaaS Model MIPS: machine instruction per second, BW: bandwidth, Pr. Number: processor numbers used in VM.



VM ID	MIPS	Size of Image	BW	Processor number	Virtual m/c manager
0	1000	1000	1000	1	Xen
1	1000	1000	1000	1	Xen

Table 3: Shows the properties of the IaaS model. Here data centres' are assigned to VM.



Datacenter ID	RAM in Mb	Storage limit	Architecture re of data	Operating system	BW
2	2048	1000000	X86	Linux	10000
3	2048	1000000	X86	Linux	10000

RESULTS AND DISCUSSIONS

The proposed method is implemented using Cloudsim and Net Beans IDE 8.0. Cloudsim is a cloud computing simulation environment that provides basic classes that explain the library and virtual machines, data centers, users and applications. The results of classification and encryption are illustrated in the following figures of Figure 2, Figure 3, Figure 4, Figure 5 and Figure 6. Comparison between KNN and Bayes Naive These cryptographic methods occur on these statistics.

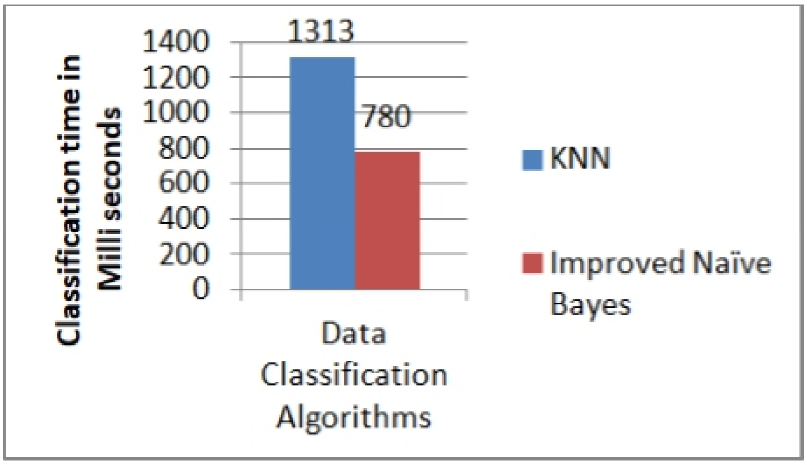


Fig.4.Performance analysis by classification time

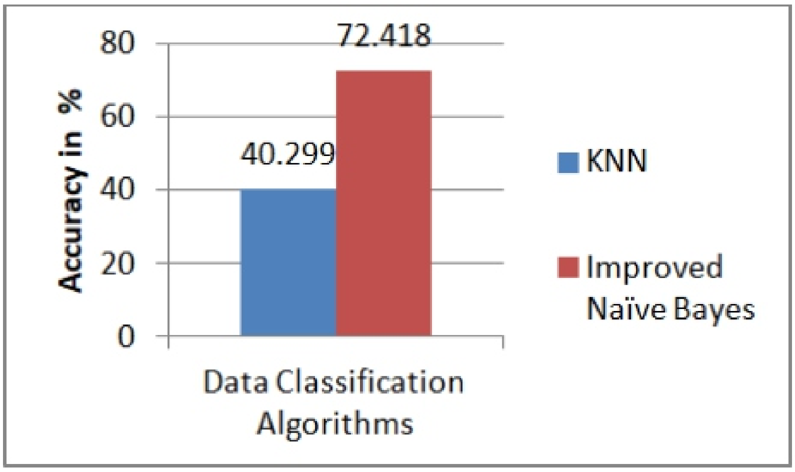


Fig.5.Performance analysis by the accuracy

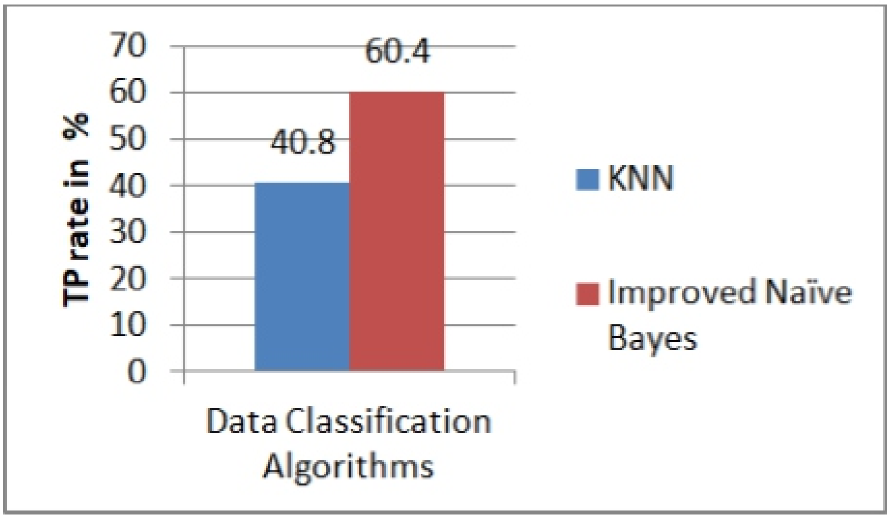


Fig.6.Performance analysis by TP Rate

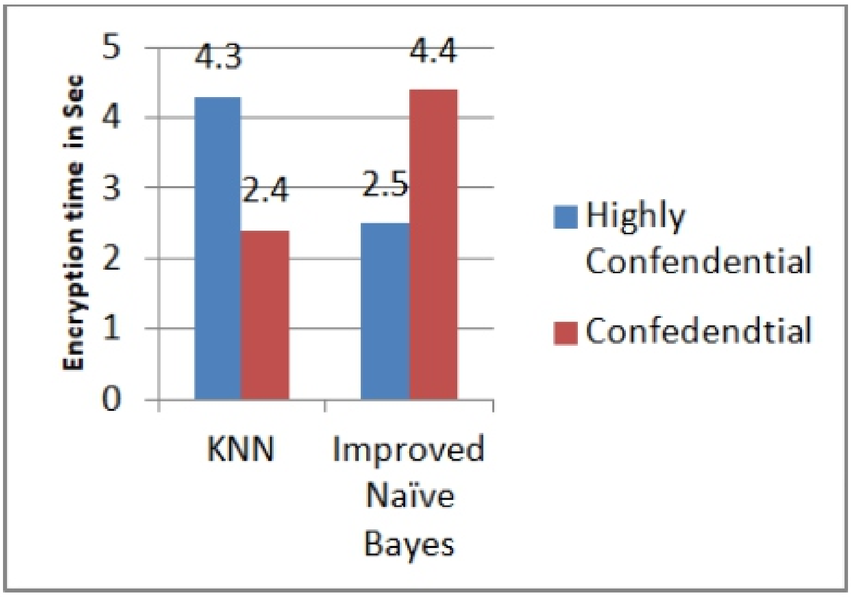


Fig.7.Performance analysis from Encryption Time

From the above results, it concludes that the proposed methodology is better rather than the existing method. Here we are projecting the performance difference among KNN and Improved naïve Bayes algorithm. As per shown in figure 4 it expects the Performance analysis by classification time, similarly figure 5 shows Performance analysis from accuracy, comparison of data classification algorithms KNN and Improved Naïve Bayes Algorithm. KNN algorithm is having accuracy 40.299% and improved naïve Bayes is having 72.418 %, i.e. the proposed algorithm has classified data more correctly similarly Fig.6.Performance analysis from TP Rate, Fig.7.Performance analysis from Encryption Time and Fig 8. Performance Analysis of Decryption time. Consequently, reducing the encryption time in the cloud, using data machine learning algorithms to replace your security needs. The previous analysis provided excellent results for the proposed method of accuracy, data classification time, actual positive speed, coding time and decoding time.

CONCLUSIONS

In this paper, we have proposed a system with data related to security settings. The introduction of existing technologies is greatly enhanced by adding it to a machine learning method. The proposed system simulates the cloud computing environment created using the cloud simulator. The results show that the proposed method is more significant than storing data without specifying data security requirements. Besides, the results suggest that the technique improved naive Bayes works better than the K-NN classification method for accuracy, time classification and TP rate and time coding and decoding. The proposed work has improved security. In the future, the number of safety requirements will be taken into account, taking into account the decision on classification using the machine learning algorithm.

REFERENCES

[1] Munwar ali zardari, Low Tang Jung, Nordin Zakaria," K-NN Classifier for Data Confidentiality in Cloud Computing", IEEE, pp.1-6, 2014.

[2] Almorsy, M., Grundy, J., & Ibrahim, A. S., "Collaboration- Based Cloud Computing Security Management Framework" IEEE conference of cloud computing, Washington (DC), pp. 364-371,2011.

[3] Song, D., E. Shi, I. Fischer and U. Shankar, "Cloud data protection for the masses", IEEE Computer. Soc., Vol. 45,

Issue 1, pp.39-45, 2012

[4] Kashyap S.; Madan N. : "A Review on: Network Security and Cryptographic Algorithm", in International Journal of Advanced Research in Computer Science and Software Engineering, April 2015, Volume 5, Issue 4, pp. 1414-1418.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing.pdf," Ieee Infocom, pp. 1–9, 2010.

[6] V. K. Pant, J. Prakash, and A. Asthana, "Three step data security model for cloud computing based on RSA and steganography," 2015 Int. Conf. Green Comput. Internet Things, pp. 490–494, 2015.

[7] L. Tawalbeh, N. S. Darwazeh, R. S. Al-Qassas, and F. AlDosari, "A secure cloud computing model based on data classification," Procedia Comput. Sci., vol. 52, no. 1, pp. 1153–1158, 2015.

[8] R. Shaikh and M. Sasikumar, "Data classification for achieving security in cloud computing," Procedia Comput. Sci., vol. 45, no. C, pp. 493–498, 2015.

A Collaborative Lightweight Scheme for Secured Key Establishment using Heuristic Algorithm for Internet of Things

[1] Prakash Palanivel, [2] C. Suresh Gnana Dhas

[1]Information Security Analyst, Skill TeQ, Adambakkam, Chennai, Tamilnadu, India – 600088.
[2]Professor and Head, Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Tiruchengode, Namakkal District, Tamilnadu, India – 637205
E-mail: [1]prakash.palanivel@skillteq.com, [2]sureshc.me@gmail.com

ABSTRACT

The Internet of Things (IoT) is a popular field that integrates physical world with internet for increasing the efficiency of data usage by the owners. The physical devices connected through IoT are embedding with software, electronics, sensors and actuators to cloud. There are several protocols available to provide device communication with reduced bandwidth and delay requirements. Such communication between IoT devices should be protected using security mechanisms that should ensure secured key distribution across the network. In this paper, we propose a collaborative key management system with a novel framework that ensures better selection of optimal proxies and that ensures secured cryptographic actions until the completion of encryption action. The framework consists of automated key establishment using bat algorithm and fuzzy neural network, where former optimally selects the proxies using cryptographic actions and latter generates automated key by considering computational burden and memory requirement as its concern. The results shows that the proposed collaborative lightweight scheme obtains improved efficiency than other systems.

Keywords - Optimal Proxy Selection, Key Establishment, Computational Overhead, Fuzzy Neural Network, IoT, Bat Algorithm.

I. INTRODUCTION

The IoT is a collection of various physical devices interconnected with each other to exchange data over the internet. The physical devices in IoT has locatable Internet Protocol address, which is used for processing and communication capabilities that are resource constrained in nature. The network infrastructure is used for accessing and controlling the devices remotely through uninterrupted connections with the computing systems. This reduces the involvement of humans with improved efficiency and accuracy. In various scenarios, the devices connected through gateway node to internet is accessed by several users with authorized access [1].

The main challenge in IoT is the integration of physical devices that leads to reduced end-to-end security between the remote entities. The devices allows to reveal its surrounding state and can communicate with other entities. Hence, this necessities the connection of sensors with other entities through a common gateway to internet. The main issue surrounding the information security is not trivial, since the sensors have constrained power and resource limitations [1]. Further, other challenges related to security includes the communication nature, resource limitation, density of network, poor infrastructure, network topology and physical attacks on unattended sensor nodes. Moreover, the sensor nodes are deployed in order to operate on adversarial situations [2].

The solutions for security in IoT application depends strongly on effective key distribution management system. This is considered infeasible in uncontrolled environments, where millions of sensors tends to change its device configuration. The usage of single key distribution in IoT application is not advisable, since it can be easily obtained by the intruder. Hence, it is very necessary for the sensor nodes in IoT to adapt with its environment and it should provide establishment of secure network using pre-distributed keys, exchange of information with immediate neighboring nodes and with robust nodes. There are several works that customizes elliptical or public key cryptography for such low power wireless sensor nodes and such approach is considered costly due to its high computational or processing requirements. Hence, the key distribution and management is considered as a difficult task in IoT and it requires the use of new approaches [2].

It is very necessary to use a lightweight key management system to reduce the computational burden in IoT networks. In this paper, we propose a collaborative lightweight key management framework to reduce the computational burden in IoT networks. This framework essentially selects optimal proxies using Bat algorithm with secured cryptographic actions until the encryption operation ends. After the selection of proxy servers, Fuzzy Neural Network generates automated key in order to reduce the computational burden and memory requirement.

The outline of paper is as follows: Section 2 provides various methods used by researchers for solving the problem associated with key management. Section 3 provides the proposed design using novel framework.Section 4 evaluates the given work and section 5 concludes the paper with future work.

II.RELATED WORKS

There are few key management systems in IoT application, which are intended to increase the security in IoT applications. Roman et al. [1] proposed a key management principle to negotiate the link layer keys between the sensor nodes in IoT application. This paper analyses the creation of secured channel between any two remote entities using pre-shared key, public key cryptography and link-layer oriented key management systems. Here, public key cryptography is used in server nodes and in client nodes. The pre-shared keys are used for server nodes in real-world application and key management system [3] can provide better solution for client nodes [1].

In distributed IoT applications, lightweight authentication and keying scheme is used to establish secure link between end-users and peer-to-peer sensor nodes. This authentication scheme uses implicit certificates to provide end-to-end security at application level [4].

In hierarchical IoT applications, a lightweight three- factor remote user authentication scheme key management protocol is proposed. The security is analyzed in a random model that applies password, smart card and biometrics as an authentication key. It uses cryptographic hash function along with the symmetric encryption/decryption to make the system efficient. The formal security is proved using ROR model against various possible attacks [2]

In IoT wearable devices, end-to-end authenticated key exchange agreement is proposed to improve the key exchange agreement with wearable devices or smart cards. This method provides dynamic authentication to reduce the possibility of tracking and extraction of personal data. The computational cost of authentication is reduced using elliptic curve cryptography [6].

In IoT cloud application, a security model is proposed with reduced encryption or decryption cost. Then an access control model is used to reduce the cost of key management for owners. Finally, a password authorization update mechanism is used to reduce the cost in dynamic way [7].

In machine-to-machine technology, IoT is implemented with increased security and privacy concerns with password authorization scheme. The mutual authentication method is improved with Elliptic Curve Cryptography based Self-Certified Key Management that relies on self-certified public key management. The less constrained system generates more resource constrained nodes in IoT system and its privacy is generated by the sensor nodes [8].

III. SECURED AND AUTOMATED KEY ESTABLISHMENT MANAGEMENT

The architecture of automated key establishment management is shown in Figure 1. The overall processing flow includes secured transmission of packets using efficient key establishment management. The secured key transmission is optimized through the selection of optimal proxy servers.

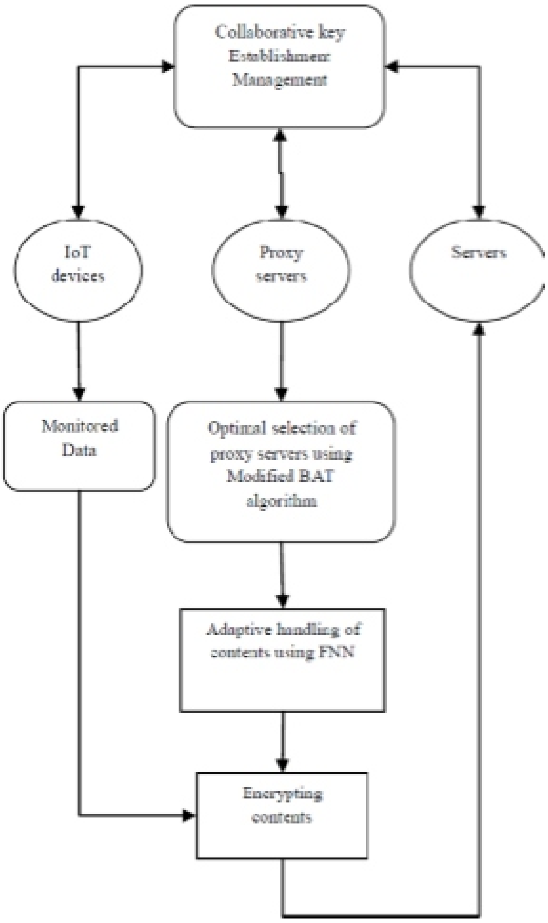

Collaborative key Establishment Management
IoT devices
Proxy servers
Servers
Monitored Data
Optimal selection of proxy servers using Modified BAT algorithm
Adaptive handling of contents using FNN
Encrypting contents

Figure -1. Overall processing flow of the proposed research method

3.1 PROXY SERVER SELECTION USING BAT ALGORITHM

The proxy server needs to be optimally selected in order to fulfill the requirements of data transmission. The use of cryptographic functions with optimal proxy selection can be done without any failure or interruptions. The main constraints associated with it is the optimal consumption of energy and bandwidth. The algorithm for the selection of proxy server selection is given in algorithm 1.

ALGORITHM: Modified Bat Algorithm

```
Step 1. Initialize bat population xi and velocity vi
Step 2. Define frequency fi
Step 3. Initialize pulse emission rate r and loudness A
Step 4. repeat
Step 5. Generate new solutions by adjusting frequency and updating velocity and location
Step 6. if rand>ri then
Step 7. Select a solution among best solutions
Step 8. Generate new local solution around selected best solution
Step 9. end
Step 10. Generate new solution by flying randomly
 Step 11. if rand<Ai and f (xi)<f (x*) then
Step 12. Accept the new solution
Step 13. Decrease Ai, increase ri, by Equations 6 and 7
 Step 14. end
Step 15. Rank the bats and find the current best x*
Step 16. until termination criteria is met;
Step 17. Post process results and visualization
```

3.2 COLLOBORATIVE KEY HANDLING MANAGEMENT

The enhanced distributed approach we propose is based on the use of a (k, n) threshold scheme, wherein the n proxies obtain a polynomial share instead of a partition element, k polynomial shares being enough to reconstruct the source's DH public key through the technique of Lagrange polynomial interpolation. In cryptography, Lagrange polynomials were initially used in Shamir's secret sharing schemes. The proposed threshold scheme satisfies the two properties that the integer partition solution fails to provide:

Given a polynomial function f of degree k - 1 expressed as: $f(x) = q_0 + q_1x + \dots + q^{k-1}x_{k-1}$ with $q_1, q_2, \dots, q_{k-1}$ being random, uniform and independent coefficients and $q_0 = a$. Applying the Lagrange formula, the pol

$$f(x) = \sum_{i=1}^{k} \left(f(i) \times \prod_{j=1,j*}^{k} \frac{x-j}{i-j}\right) \qquad (9)$$

From (9), the secret exponent a can be computed given any subset of k values of f(x):

$$a = f(0) = \sum_{i=1}^{k} \left(f(i) \times \prod_{j=1,j*i}^{k} \frac{-j}{i-j}\right) \qquad (10)$$

In the threshold distributed approach, the distributed shares ai of the private exponent a are obtained as ai = f(i). So, in order to bootstrap the threshold distributed key agreement, the source calculates n values f(1), . . ., f(n) of the polynomial f, with n > k, and sends each f(i) to the correspondent proxy P_i. Each proxy computes then it's part of the source's DH public key g^{ai} mod p = $g^{f(i)}$ mod p and sends it to the server. Upon the reception of a subset P of k values transmitted by the proxies, the server starts by computing the ci coefficients as follows:

$$C_i = \prod_{i \in P, j * i} \frac{-j}{i - j} \qquad (11)$$

Then, B computes the source's DH public key DH_I based on the Lagrange formula:

$$\prod_{i \in P} (g^{f(i)})^{c_i} \bmod p = g^{\sum_{i \in P} f(i) \times \text{€}_i} \bmod p \qquad (12)$$

$$= g^{f(0)} \bmod p$$

$$= g^{a} \bmod p$$

ith coefficient calculated in the previous phase). Pi is unable to compute the coefficient ci since it has no knowledge about the subset P of concrete participating proxies. Having received this value, each proxy Pi uses its share f(i) of the source's private exponent to compute $K_i = B_i^{f(i)} = g^{b.ci.f(i)}$. Each proxy delivers then this computed value to the source A. Upon reception of these k values, the source computes the DH session key KDH as follows:

$$K_{DH} = \prod_{i \in P} g^{bf\,(i)c_i} \bmod p \qquad (13)$$

$$= g^{\,b \sum_{i \in P} f(i) c_i} \bmod p$$

$$= g^{ab} \bmod p$$

By applying the threshold technique to improve the effectiveness of the distributed approach, the source is led to perform more computational operations in the initial phase, in order to calculate the n values of the polynomial that it sends to the n proxies. The cost of the computation can be better estimated if one considers another way of writing f(x), as:

$$f(x) = (\ldots\ldots ((q_{k-1}x + q_{k-2}).x + q_{k-3})x + \cdots).x + q_0 \qquad (14)$$

According to this expression, A performs for each computation of f(i): (k - 1) multiplications between a scalar and a large number and (k - 1) summations of two large numbers. It is worth noting that k and n are small numbers, smaller than the number of secure relationships that the source is able to maintain. On the other hand, the polynomial coefficients are as large as the DH private key of the source.

IV. EXPERIMENTAL RESULTS

This section discusses the performance of proposed system with existing methods. The performance of proposed method is tested in terms of end to end delay, packet delivery ratio, and network lifetime and network throughput against existing system. The results are tested with 1000 sensor nodes in an area of 1000*1000m2. The initial energy of sensor node is set as 0.5J and the location of base station is at the center of the network. The energy of each sensor node is 50nJ/bit with transmission packet size of 4000bits transmitted between the devices.

4.1 END TO END DELAY

The End-to-end delay is defined as total time taken for packet transmission between source and destination IoT nodes due to retransmission and queuing.

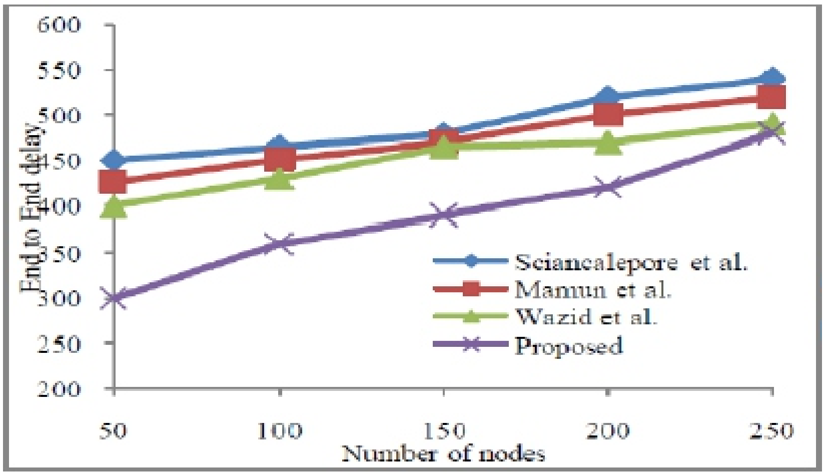


Figure -2. End to End delay comparison

It is seen from Figure 2, the proposed system obtains reduced end to end delay than existing methods like Sciancalepore et al. [3], Mamun et al. [4], Wazid et al. [5]. This shows the efficient transmission of packets without any retransmission or queuing in proposed method than other methods.

4.2 NETWORK LIFETIME

The network lifetime is defined as the total lifetime of all sensor nodes in the network or the time before the network running out of energy or it can be defined as remaining energy of sensor network.

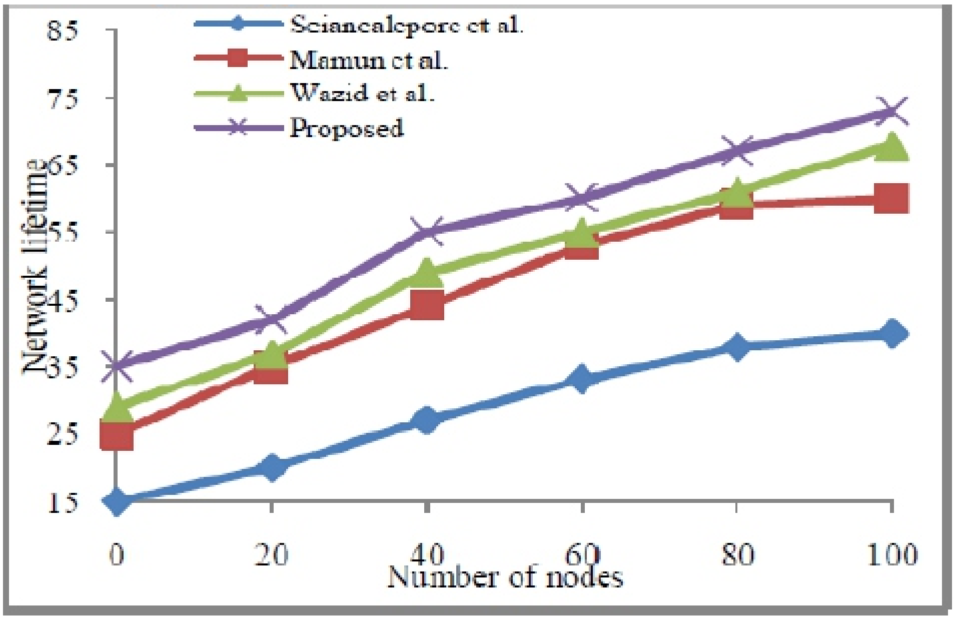


Figure -3. Network Lifetime comparison

It is seen from Figure 3, the proposed system obtains increased network lifetime than existing methods like Sciancalepore et al. [3], Mamun et al. [4], Wazid et al. [5]. This shows the improved transmission of packets for longer time than existing methods.

4.3 THROUGHPUT

Network throughput is defined as the ratio of packet delivery in a communication channel. The throughput is measured as bits per second.

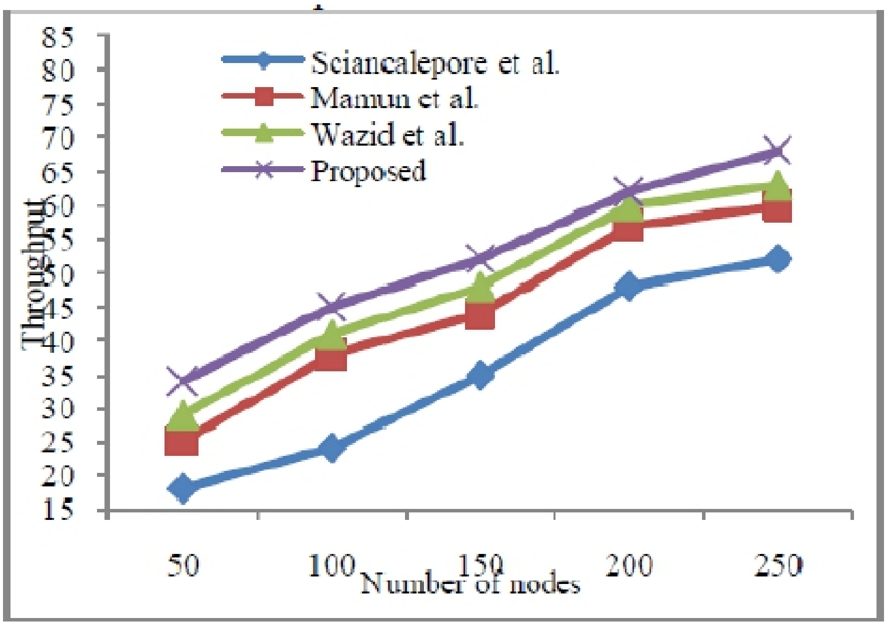


Figure -4. Throughput comparison

It is seen from Figure 4, the proposed system obtains increased network throughput than existing methods like Sciancalepore et al. [3], Mamun et al. [4], Wazid et al. [5]. This shows that transmission of bitrate is increased in proposed system than existing methods.

4.4 PACKET DELIVERY RATIO

The Packet Delivery Ratio is defined as the total number of packets received successfully by the destination node.

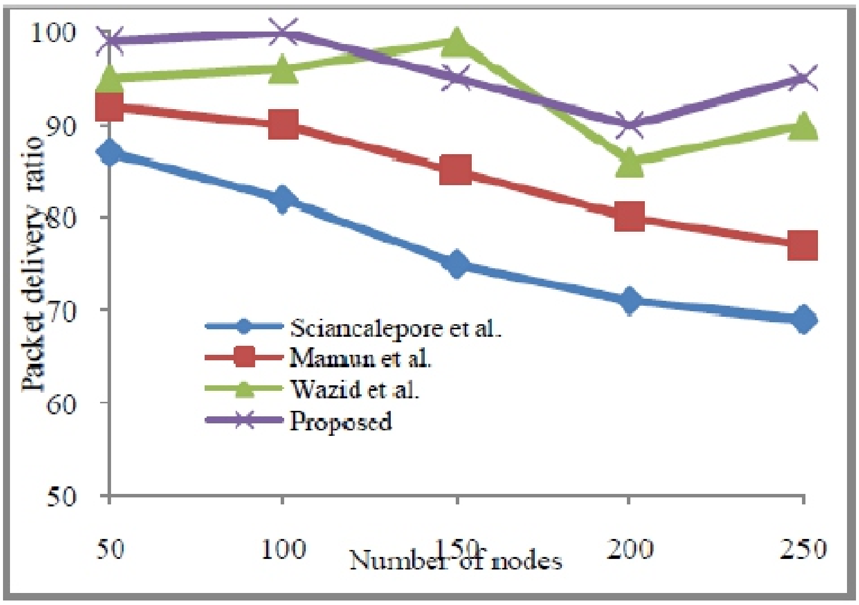


Figure -5. Packet delivery ratio comparison

It is seen from Figure 5, the proposed system obtains increased packet delivery ratio than existing methods like Sciancalepore et al. [3], Mamun et al. [4], Wazid et al. [5]. This shows that packet transmission is improved for longer lifetime in proposed system than existing methods.

4.5 PACKET LOSS RATIO

Packet loss ratio is defined as the percentage of total packets lost during the packet transmission.

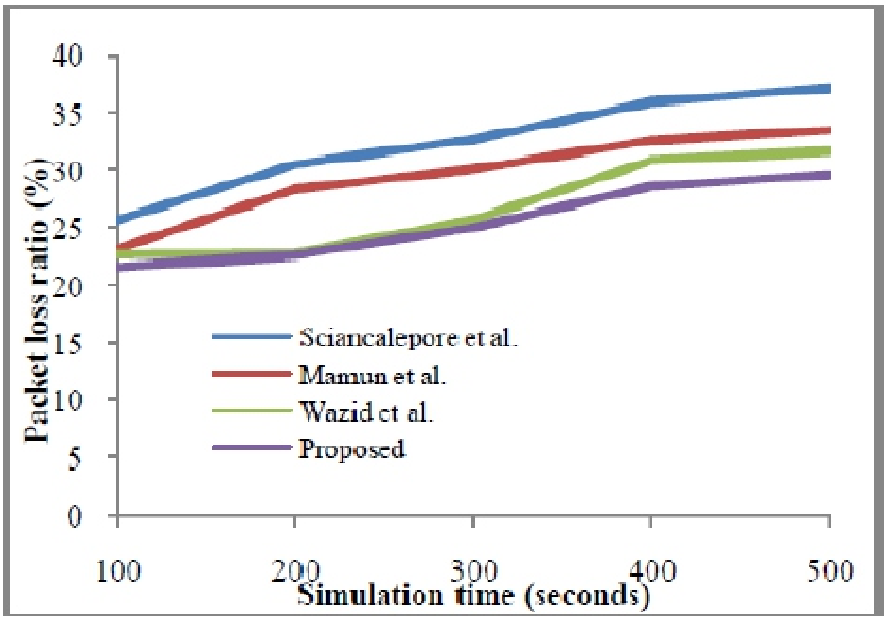


Figure.6. Packet loss ratio comparison

It is seen from Figure 6, the proposed system obtains reduced packet loss ratio than existing methods like Sciancalepore et al. [3], Mamun et al. [4], Wazid et al. [5]. This shows that packet transmission is improved with reduced packet loss for longer lifetime in proposed system than existing methods.

CONCLUSION

In this paper, we propose an automated secure key establishment framework with Bat algorithm and Fuzzy Neural Network for establishing secured key handling by the better selection of optimal proxy servers with secured data transmission. The selection of optimal proxy servers is carried out by considering bandwidth and energy parameters that are reliable and offers continuous data delivery. The better data delivery and secured key generation is ensured by using Bat algorithm and Fuzzy Neural Network, where the prediction of key is considered difficult. The results of proposed method with other conventional methods show that our proposed method obtains improved security and better delivery of data.

REFERENCES

[1] Roman, R., Alcaraz, C., Lopez, J., &Sklavos, N. (2011). Key management systems for sensor networks in the context of the Internet of Things. Computers & Electrical Engineering, 37(2), 147-159.

[2] Wazid, M., Das, A. K., Odelu, V., Kumar, N., Conti, M., & Jo, M. (2018). Design of secure user authenticated key management protocol for generic IoT networks. IEEE Internet of Things Journal, 5(1), 269-282.

[3] Sciancalepore, S., Piro, G., Boggia, G., & Bianchi, G. (2017). Public key authentication and key agreement in IoT devices with minimal airtime consumption. IEEE Embedded Systems Letters, 9(1), 1-4.

[4] Mamun, Q., &Rana, M. (2017, October). A partial key distribution protocol for WSNs in distributed IoT applications. In Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2017 8th IEEE Annual (pp. 248-254). IEEE.

[5] J. Kennedy, R. Eberhart, Particle swarm optimization, in: Neural Networks, 1995. Proceedings., IEEE International Conference on, Vol. 4, 1995, pp. 1942–1948 vol.4.

[6] Hsu, C. L., Chuang, T. H., Chen, Y. H., Lin, T. W., & Lu, H. C. (2017, September). A dynamic identity end-to-end authentication key exchange protocol for IoT environments. In Digital Information Management (ICDIM), 2017 Twelfth International Conference on (pp. 133-138). IEEE.

[7] Cui, Z., Lv, H., Yin, C., Gao, G., & Zhou, C. (2015, August). Efficient key management for IOT owner in the cloud. In Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on (pp. 56-61). IEEE.

[8] Haripriya, A. P., &Kulothungan, K. (2016, October). ECC based self-certified key management scheme for mutual authentication in Internet of Things. In Emerging Technological Trends (ICETT), International Conference on (pp. 1-6). IEEE.

[9] Y. Shi, R. Eberhart, A modified particle swarm optimizer, in: Evolutionary Computation Proceedings, 1998. IEEE World Congress on Computational Intelligence. The 1998 IEEE International Conference on, 1998, pp. 69–73.

[10] X.-S. Yang, A new metaheuristic bat-inspired algorithm, in: J. Gonzlez, D. Pelta, C. Cruz, G. Terrazas, N. Krasnogor (Eds.), Nature Inspired Cooperative Strategies for Optimization (NICSO 2010), Vol. 284 of Studies in Computational Intelligence, Springer Berlin Heidelberg, 2010, pp. 65–74.

[11] M. Fenton, Bat natural history and echolocation, in: R. Brigham, K. Elisabeth, J. Gareth, P. Stuart, A. Herman (Eds.), Bat Echolocation Research tools, techniques and analysis, Bat Conservation International, 2004, pp. 2–6.

Case Study on Steganography and Malware

Ki- Hyun Jung

[1]Department of Cyber Security, Kyungil University, Republic of Korea

E-mail: khanny.jung@gmail.com

ABSTRACT

Malware is any malicious software to cause damage to computer systems. Steganography is a technique to embed the secret information without any notice. Recently, malware using steganography technique is used to evade detection. In this paper, various cyber attacks are explained and malwares using steganography are described. These attacks are not only difficult to detect but also increased the damage because of various forms and combination with each other.

Keywords- Steganography, Malicious Code, Malware, Information Hiding.

I. INTRODUCTION

Cybersecurity issues are becoming everyday struggle in the world. In the U.S. economy, malicious cyber security activity was estimated between \$57 billion and \$109 billion in 2016 [1-2].

Malware describes any malicious program or code whose purpose is designed to cause harmful damage to a computer. Malware takes many forms of software that may be deployed on desktops, servers, mobile devices, printers and programmable electronic devices. There are many different types of malware such as virus, worms, Trojan, backdoors, rootkits, bots, spyware, ransomware, adware, and scareware [3-4].

Steganography is one kind of information security to communicate with secret by hiding the existence of the secret data itself [5-6]. Digital contents such as image, video, text, audio, network protocol and DNA are used as communication mediums. Steganography can be divided into spatial/frequency domain based techniquesor technical/linguistic based techniques as shown in Fig. 1.

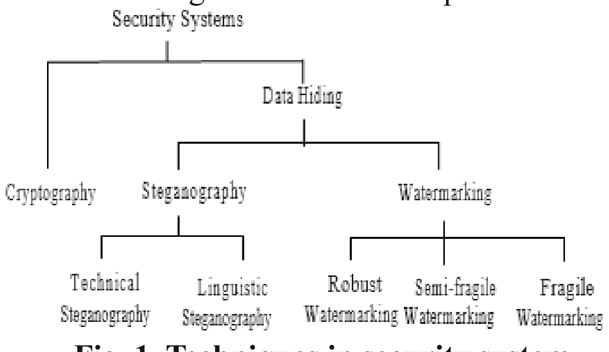


Fig. 1. Techniques in security system.

Recently, malware using steganography techniques was found to hinder detection [7-9]. The malicious code can be carried as hidden messages in image, voice, audio/video and even electrocardiogram data. Hackers use steganography to evade detection by conventional security tools when infiltrate computer systems.

In this article, some malwares using steganography technique are described and damage caused by malware is shown to get interests and research in the field.

II.MALWARE AND STEGANOGRAPHY

2.1. Cyber and Malware Attacks

Common types of cyber attacks are shown inFig. 2. [10-11]. TCP SYN flood attack, teardrop attack, smurf attack, ping of death attack and botnets attacks are common types of DoS/DDoS attack. Session hijacking, IP spoofing and Replay attacks are common types of MITM attack. Drive-by download attack is used generally to spread malware, where hackers plant a malicious script into HTTP or PHP code for insecure websites. For password attack, brute-force and dictionary attacks are often used. The birthday attack try to find two random messages that generate the same message digest by hash algorithms.

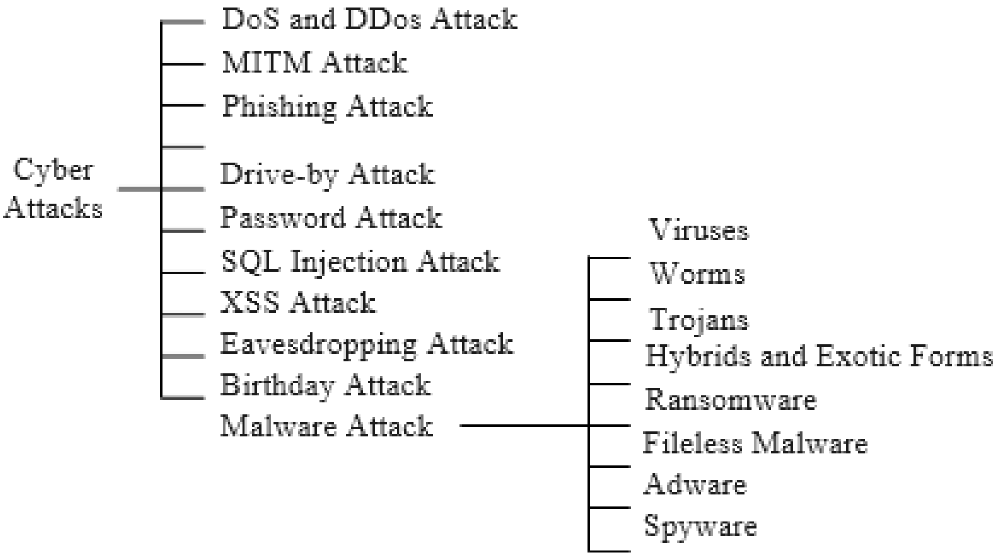


Fig. 2. Types of cyber attacks.

Malware can be described as unwanted software that is installed without consent. Common types ofmalware are viruses, worms, Trojans, hybrids, ransomware, adware, spyware and so on. Viruses are the only type of malware that can infect other files. Worms have ability to replicate itself and to spread without end user action. Trojans hiding in a useful program contain malicious instructions that can establish a back door and exploit by attackers. Recently, most of malware programs are considered rootkits or stealth programs.

2.2. Malware Examples

An attacker uses steganography to embed securely a piece of malicious code. In smartphone apps, steganography malware contains three basic components: stego-text, stego-key, and steganography extracting algorithm [8]

There are some cases of malware using steganography [13-14]. Lurk malware was documented in 2014, which is used to download additional malware on infected computers. Lurk downloads firstly an image which embeds a download URL by least significant bit replacement. The GoziNeverquest malware can inject malicious code into browsers to retrieve URLs, where it could download the configuration file from decrypted a URL from image pixel. Stegoloader is a modular information stealer to check whether it is an analysis computer and then to download an image file from a legitimate website.

2.3. Malware Inspection Scenarios

Malware installation to target systems is complex, but two main steps are required. First, initial decryption and installation of the malware is needed. Second, download of the inspected image and use of the hidden secret information are required to establish covert communication further actions.A possible scenarios malware using steganography is shown in Fig. 3.

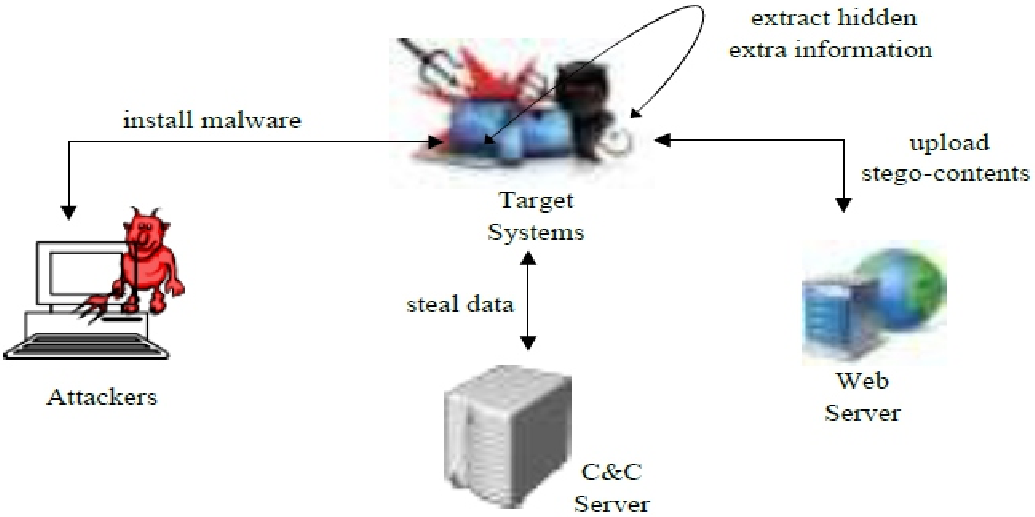


Fig. 3. Attack scenarios.

III. FUTURES AND DISCUSSION

3.1. Malware Statistics

According to AV-TEST statistics, over 350,000 new malware and potentially unwanted applications are registered [15].

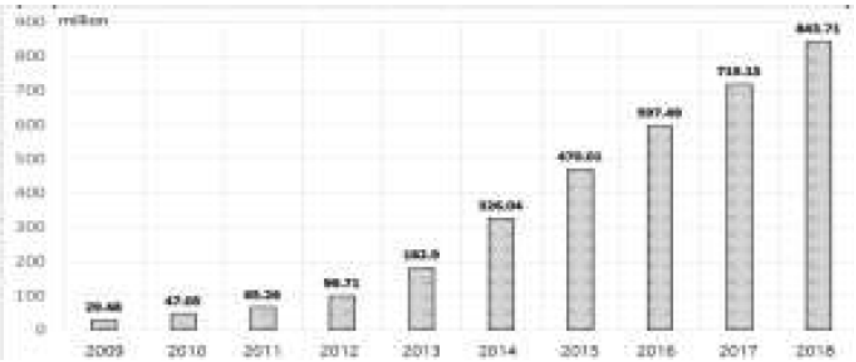


Fig. 4. Malware statistics.

3.2. Steganography in Malware

Malware using steganography can be extremely difficult to detect and scanning performance for every files on small and non-impacting anomalies are huge. Nowadays, more intrusion cases are being found as criminals.

CONCLUSIONS

Steganography has been used for evading detection in malware. Malware attacks are very difficult to detect because of various forms and combination. As results, the damage from malware attacks will increasing. Interests of security and research in the field are mandatory in the future.

ACKNOWLEDGMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2018R1D1A1A09081842) ,Ministry of Culture, Sports and Tourism(MCST) and from Korea Copyright Commission in 2018(2018-f_drm- 9500), and Brain Pool program funded by the Ministry of Science and ICT through the National Research Foundation of Korea(No. 2018H1D3A2065993).

REFERENCES

[1] A.P. Namanya, A. Cullen, and J.P. Disso, "The world of malware: an overview", IEEE 6th International Conference on Future Internet of Things and Cloud, pp. 420-427, 2018.

[2] The Council of Economic Advisers, "The cost of malicious cyber activity to the U.S. economy", February 2018.

[3] Malware, https://en.wikipedia.org/wiki/Malware.

[4] A. Makandar, A. Patrot, "Overview of malware analysis and detection", International Journal of Computer Applications, pp. 35-40, 2015.

[5] M.S. Subhedar, V.H. Makar, "Current status and key issues in image steganography: a survey", Computer Science Review, pp. 95-113, 214.

[6] M. Hussain, A.W.A. Wahab, Y.I.B. Idris, T.S. Ho, and K.H. Jung, "Image steganography in spatial domain: a survey", Signal Processing: Image Communication, pp. 46-66, 2018.

[7] L.J. Young, "The dark side of steganography", https://spectrum.ieee.org, 2015.

[8] S.T. Guillermo, E.T. Juan, and P.L. Pedro, "Stegomalware: playing hide and seek with malicious components in smartphone apps", International Conference on Information Security and Cryptology, pp. 496-515, 2014.

[9] L. Mosuela, "How it works: steganography hides malware in image files", https://www.virusbulletin.com, 2016.

[10] J. Melnick, "Top 10 most common types of cyber attacks", http://blog.netwrix.com, 2018.

[11] R.A. Grimes, "8 types of malware and how to recognize them", httpd://www.csoonline.com, 2018.

[12] P.M. Bureau, C. Dietrich, "Hiding in plain sight", Black Hat, 2015.

[13] F. Wu, H. Narang, and D. Clarke, "An overview of mobile malware and solutions", Journal of Computer and Communications, pp. 8-17, 2014.

[14] K. Cabaj, L. Caviglione, W. Mazurczyk, S. Wendzel, A. Woodward, and S. Zander, "The new threats of information hiding: the road ahead", IT Professional, pp. 31-39, 2018.

[15] Total Malware, https://www.av-test.org/en/statistics/malware/.

Wi- Fi Controlled Keyboard and Mouse with Voice Control and Image Recognition using Smartphone

Savanth Gattu
Indian Institute of Information Technology, Guwahati, Assam, India
E-mail: savanthgattu123@gmail.com

ABSTRACT

This paper describes about controlling the computer and laptops keyboard and mouse with voice control and image recognition from smartphone using Wi-Fi. Now-a-days home appliances are controlled using smart phones, in the same way we can also control the computer keyboard and mouse for typing letters, numbers and playing games etc by sending virtual keystrokes and mouse clicks from phone.

Keywords - HTTP Protocol, Nodemcu, PyAutoGUI, MIT App Inventor, Voice Recognition, Image Recognition

I. INTRODUCTION

Home automation is a part of 'the internet of things' also known asIoT. The way devices and appliances can get networked together to provide us seamless control over all aspects of home and more. From network and communication perspective IoT can be viewed as an aggregation of different networks including mobile networks, WLAN, WSN, mobile ad hoc networks(MANET). The connectivity is key requirement for IoT. The network and communication, speed reliability and connection durability will impact the overall IoT experience. From the smartphones we can also control the computer keyboard and mouse Wirelessly with voice recognition and image recognition using nodemcu with HTTP (Hypertext transfer protocol) protocol from an android app. The android app is created by using the MIT app inventor.

II.SYSTEM DESIGN AND IMPLEMENTATION

In the block diagram shown in Fig 1 shows the total structure of the controlling system. Firstly we will make an android app using MIT app inventor and we will install apk file in our smart phone and we have to take a wifi module called nodemcu (esp8266) and then we will establish wifi connection between two hosts the smartphone and the nodemcu and then a IP address is generated for nodemcu. Secondly with this IP address the information is sent fromclient(smart phone) to the server(nodemcu) and then the server outputs the information on the computer. In this way the communication is done between the smartphone and nodemcu (esp8266). After connection between smartphone and nodemcu, we will connect nodemcu with computer via USB cable(com ports) to output information on Arduino serial monitor .Next Arduino serial monitor and python algorithm are interconnected with some special modules in python.

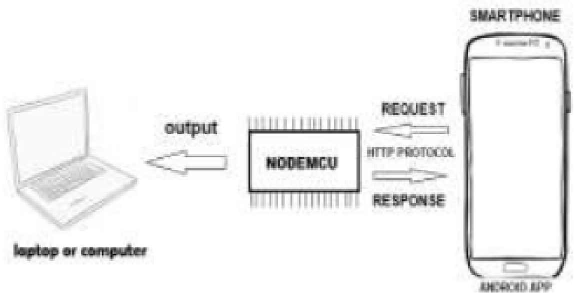
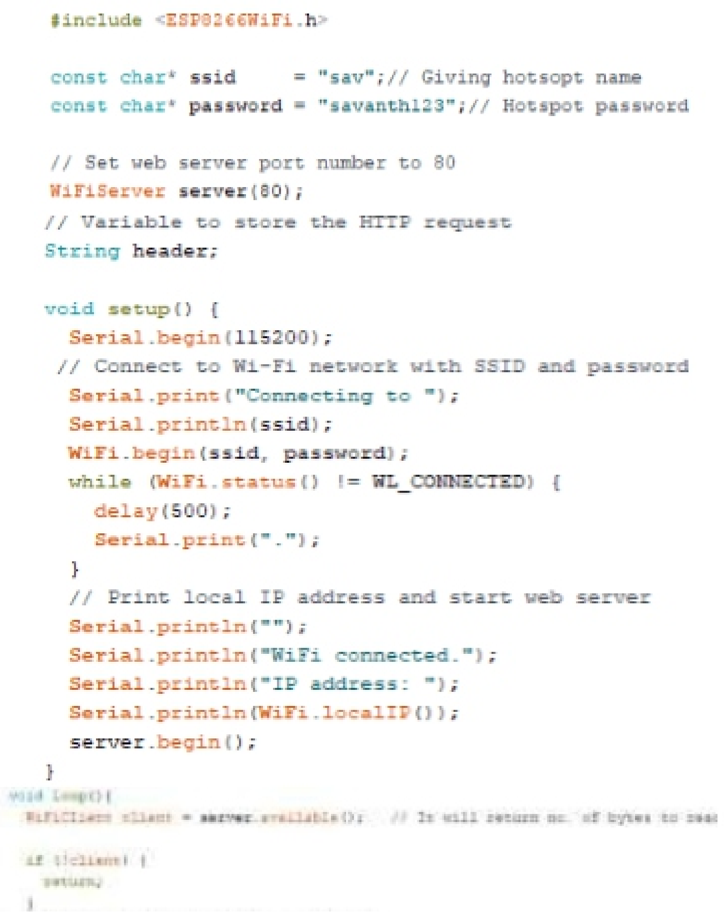


Fig 1. System block diagram

1. NODEMCU AND ANDROID APP

Nodemcu (esp8266) Wi-Fi module is generally used to establish the wireless communication between devices and it can be used as access point mode(AP) and station mode(STA). so firstly we will generate station mode(STA) or Wi-Fi in nodemcu by writing the code from Arduino IDE and we will dump the code in to the board .secondly we will on hotspot in our smartphone, then both the devices are connected with particular username and password as written in the arduino code. After connecting , the Nodemcuboard will generate an IP address in arduino serial monitor. With the generated IP address we will start communicating between these devices using HTTP protocol with GET method. When we pass information from client(smart phone) to server(nodemcu) as URL then it is called as GET method.client will always initiate communication to the server and server will respond back. First the request is sent as URL from client(smart phone) to server(nodemcu) and the nodemcu will send response to the smartphone. And the speech recognition done using the microphone located in the phone.



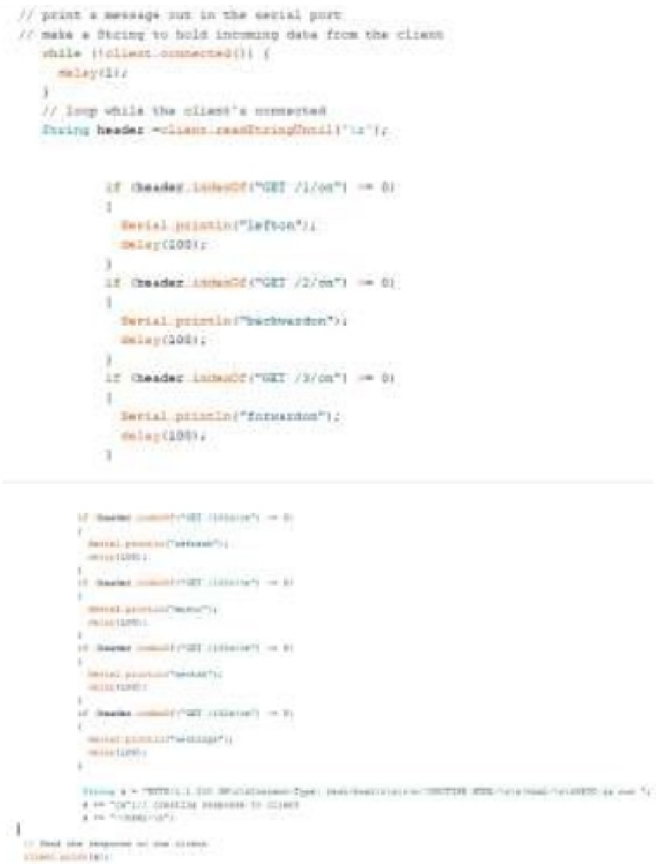
```
 #include <ESP8266WiFi.h>

 const char* ssid     = "sav";// Giving hotsopt name
 const char* password = "savanth123";// Hotspot password

 // Set web server port number to 80
 WiFiServer server(80);
// Variable to store the HTTP request
String header;

void setup() {
  Serial.begin(115200);
 // Connect to Wi-Fi network with SSID and password
  Serial.print("Connecting to ");
  Serial.println(ssid);
  WiFi.begin(ssid, password);
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
  // Print local IP address and start web server
  Serial.println("");
  Serial.println("WiFi connected.");
  Serial.println("IP address: ");
  Serial.println(WiFi.localIP());
  server.begin();
}
void loop(){
  WiFiClient client = server.available();   // It will return no. of bytes to rea

  if (!client) {
    return;
  }
```



```
// print a message out in the serial port
// make a String to hold incoming data from the client
  while (!client.connected()) {
    delay(1);
  }
  // loop while the client's connected
  String header =client.readStringUntil('\r');


        if (header.indexOf("GET /1/on") >= 0)
        {
          Serial.println("lefton");
          delay(100);
        }
        if (header.indexOf("GET /2/on") >= 0)
        {
          Serial.println("backwardon");
          delay(100);
        }
        if (header.indexOf("GET /3/on") >= 0)
        {
          Serial.println("forwardon");
          delay(100);
        }

      if (header.indexOf("GET /[illegible]/on") >= 0)
      {
        Serial.println("[illegible]");
        delay(100);
      }
      if (header.indexOf("GET /[illegible]/on") >= 0)
      {
        Serial.println("menu");
        delay(100);
      }
      if (header.indexOf("GET /[illegible]/on") >= 0)
      {
        Serial.println("[illegible]");
        delay(100);
      }
      if (header.indexOf("GET /[illegible]/on") >= 0)
      {
        Serial.println("[illegible]");
        delay(100);
      }

      String s = "HTTP/1.1 200 OK\r\nContent-Type: text/html\r\n\r\n<!DOCTYPE HTML>\r\n<html>\r\n[illegible]";
      s += "\r\n"; // creating response to client
      s += "</html>\n";
  }
  // Send the response to the client
  client.print(s);
```

Fig 2. Arduino code

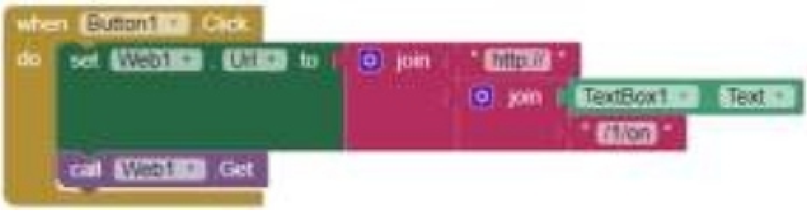


Fig 2. sending request to server(nodemcu)

2. PYTHON ALGORITHM AND SERIAL MONITER

We will mainly import three python libraries in our python script.

A. PyAutoGUI
B. Serial
C. Time

The information from server(nodemcu) and the python code is connected using a python module called serial. This serial library in python used to connect the Arduino serial monitor and python script. As the output information is printed on the serial monitor the information is read by the imported serial module in python code and it controls the keyboard and mouse functionalities with the library called PyAutoGUI . PyAutoGUI is a python module for programmatically controlling the keyboard and mouse. this module can also be used for image recognition. We use time module to put time delays.

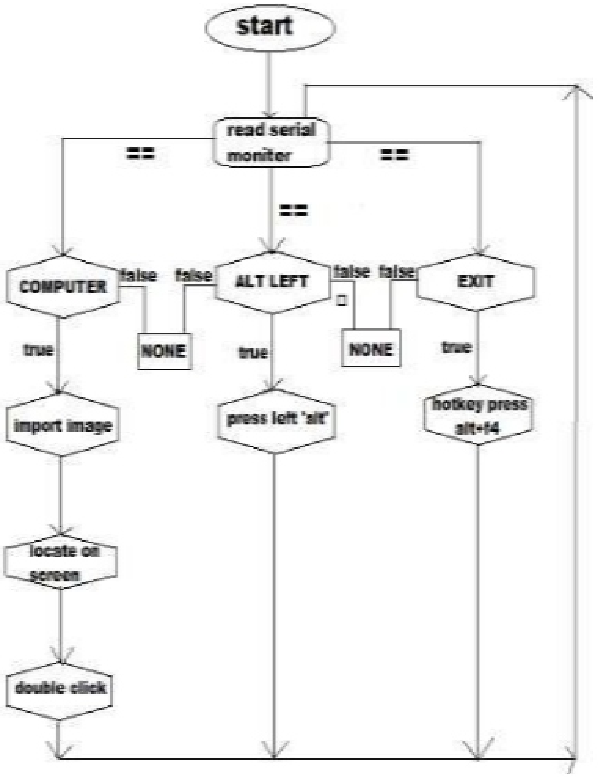
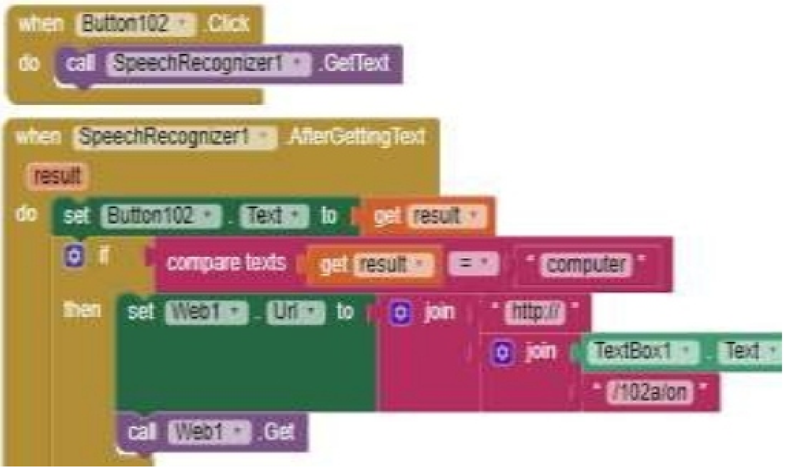


Fig 3. Flow chart of python algorithm

The printed information on arduino serial moniter is recognized by python script in bytes, so we have to decode byte objects to strings using 'decode( )' function by using ASCII mapping. After decoding the particular information we will compare the results.After comparing, if the condition is satisfied then we will call pyautogui functions such as 'pyautogui.press( )' to press the letter on the keyboard keys and 'pyautogui.hotkey( )' function is used to press two or more keyboard keys at the same time and 'pyautogui.typewrite( )' function is used to type the words. For controlling the mouse we use some another functions such as 'pyautogui.position()' function is used to locate the co-ordinates of the cursor on the screen and 'pyautogui.moveRel( )' function is used to move the mouse cursor from present location. And 'pyautogui.click( )' function is used to click the mouse right click or left click according to the arguments mentioned in the function.

3. VOICE CONTROLAND IMAGE RECOGNITION

Firstly we have to create a database of all images or icons present on the screen of computer and we have to set particular path for this database with python code in python IDLE and when ever we will get request from smartphone by speech recognizer from android app ,then for a particular keyword orcommand we will import the particular image from the created folder by using pyautogui functionsand for particular functionthe mouse cursor will locate the particular image on the screen. After locating, we will click the detected icons by using pyautogui functions. In this way the pyautogui image recognition works. suppose for example if we call ' open my computer ' in android app the speech recognizer sends the information to the nodemcu which is connected to the laptop or computer via USB cable(com ports) and the nodemcu prints the information 'open my computer' on the Arduino serial monitor , then the printed information is taken by the python script and the pyautogui function 'pyautogui.locateOnScreen( )' import the particular image from the database and search the image on the screen and gives the co- ordinates of the image on the screen. Then by using pyautogui function 'pyautogui.locatecenterOnScreen( )' the mouse cursor is centered on the image or screenshot and then by using pyautogui function 'pyautogui.doubleClick( )' the cursor double clicks on that icon and the required file is opened. optionally we can also pass 'grayscale=True' to locate functions to give slight speed up for detection of image on the desktop screen. This grayscale matching desaturates the color from the images and screenshot and locates the image on the screen.



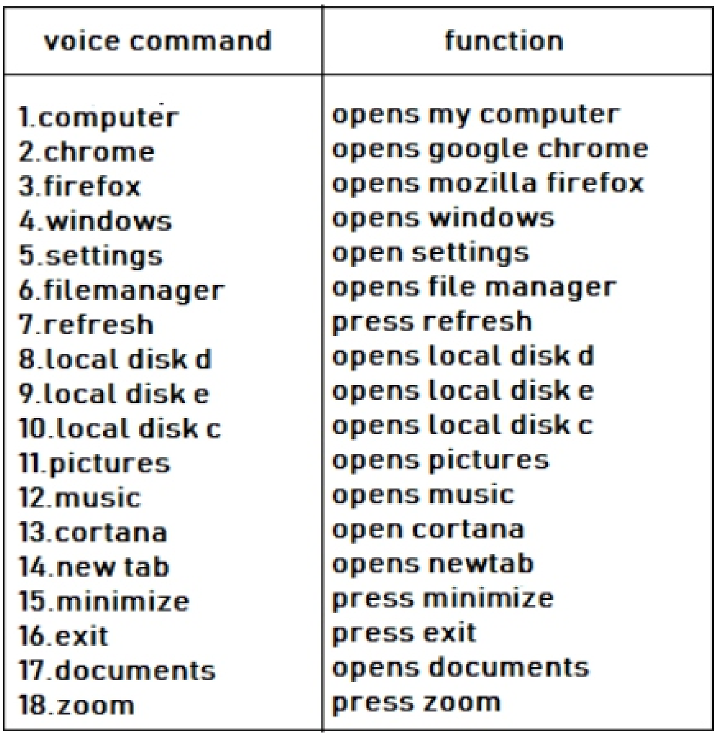
```
when Button102 .Click
do  call SpeechRecognizer1 .GetText

when SpeechRecognizer1 .AfterGettingText
  result
do  set Button102 . Text to  get result
    if    compare texts  get result  =  " computer "
    then  set Web1 . Url to  join  " http:// "
                                   join  TextBox1 . Text
                                         " /102a/on "
          call Web1 .Get
```

Fig 3. voice controlled request to server

III. RESULTS

After doing all the process and connections the experiment has been tested and experiment showed expected results. The computer keyboard and mouse has been controlled from phone using an android app and all the keys and mouse buttons has functioned. By using speech, the keyboard and mouse worked with image recognition. And the speech recognition also worked for different languages.



voice command	function
1.computer	opens my computer
2.chrome	opens google chrome
3.firefox	opens mozilla firefox
4.windows	opens windows
5.settings	open settings
6.filemanager	opens file manager
7.refresh	press refresh
8.local disk d	opens local disk d
9.local disk e	opens local disk e
10.local disk c	opens local disk c
11.pictures	opens pictures
12.music	opens music
13.cortana	open cortana
14.new tab	opens newtab
15.minimize	press minimize
16.exit	press exit
17.documents	opens documents
18.zoom	press zoom

Fig 4. Table for voice commands

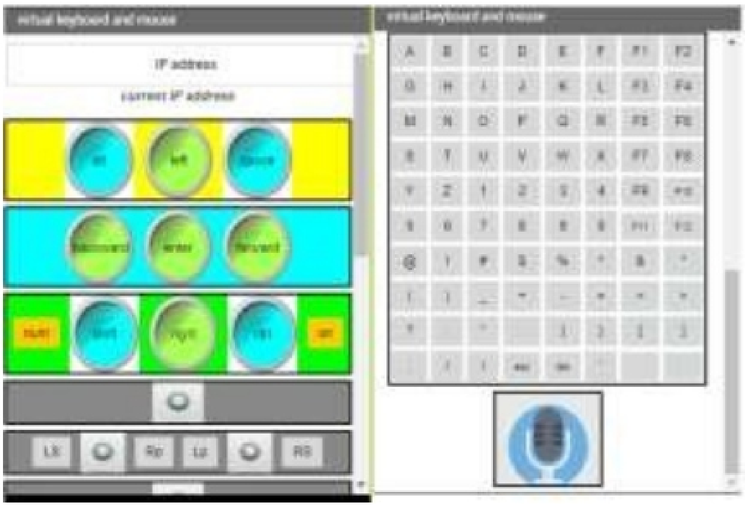


Fig 5. Android app

Fig 6. Android app code

CONCLUSION

So finally we can control the keyboard and mouse functionalities with voice recognition and image recognition by programmatically using Wi-Fi. And we connected the arduino serial and python code with serial module for serial communication and pyautogui module for keyboard and mouse functionalities and time module for time delays. We have communicated the Smart phone and nodemcu using HTTP protocol.

FUTURE WORKS

We can also extend this project more by using deep learning techniques and image recognition to control the keyboard and mouse automatically from the given inputs by the smart phone. And we can also interfacing with amazon alexa, google assistant and siri for more automated process. This project more can be developed by using cognitive IoT so that all appliances can sense, store, analyze, and learn according to user.

REFERENCES

[1] AI Sweigart - Automate the boring stuff with python, practical Programming for total beginners

[2] Handson Technology ,Nodemcu espn8266 wifidevkit ,user manual v1.2

[3] Julien Bayle – C Programming for Arduino , learn how to program Arduino boards with a series of engaging examples ,illustrating each core concept

[4] David Wolber, Hal Abelson , Ellen Spertus , Liz looney – app inventor , create your own android apps

[5] David Hanes, Gonzalo salgueiro, Patrick grossetete –Iot fundamentals networking technologies, protocols, and their use cases for internet of things.

Psoc Based Implementation of Bluetooth Low Energy Mesh Network

[1] Sayani Singha, [2] Santashraya Prasad

[1,2]Department of Electronics and Communication, Birla Institute of Technology, Mesra, Ranchi, India

E-mail: [1]sayani.singha93@gmail.com, [2]santashrayaprasad@gmail.com

ABSTRACT

This paper presents an analysis of the implementation of Bluetooth low energy (BLE) mesh network using flooding mechanism and directed addressing mechanism. Several studies have shown the shortcomings of Bluetooth low energy due to its peer to peer architecture. With Bluetooth mesh, all nodes can communicate with one another. Thus, mesh architecture can provide a large, scalable and reliable network for data transmission. In this work, common data is relayed over the network using flooding mechanism. Two methods are implemented. In the first one, data is relayed from one node to another in the network without the need to know the node address. The second implementation is based on the assignment of node address and transmitting the data to that node only.

Keywords - Bluetooth Low Energy (BLE), Internet of Things (IOT), Mesh Network.

I. INTRODUCTION

The Internet of Things (IOT) is a rapidly growing area due to the constant digitization of data and the ever-increasing number of devices using the data. Many IOT devices are available in the market which support Bluetooth connectivity. Bluetooth operates in a personal area network (PAN) consisting of two devices. The communication is peer to peer with one device known as a Master which can establish connection with seven other devices known as slave. Due to one to one connection supported by Bluetooth, the network becomes short ranged. To overcome this drawback, Mesh network is being implemented which can provide many to many connections among the nodes present in the network.

Mesh topology is very popular with Zigbee but very few devices have a Zigbee chip. Since most devices available in the market are Bluetooth compliant, it is very easy to implement mesh topology. The inclusion of mesh networking support is a fundamental change for Bluetooth technology. The mesh network will make it easier to take control of building services and to wirelessly interact with them and automate their functionality.

Let's consider a case where a smartphone has established connection with a heart-rate monitor. The same smartphone can establish connection with another pressure sensor. The smartphone can establish connection with each of the devices, but the two devices cannot communicate with each other. In such a scenario the mesh network comes into play where each device can relay messages to any other device so that the end-to-end communication range is extended beyond the radio range of each individual device.

Bluetooth Mesh is a networking technology and not a communication technology. This network does not make use of a central hub. All the nodes in the network are free to communicate with every other node. The terms used in mesh networking are as follows:

Nodes: The devices which form the mesh network are known as nodes.

Un-provisioned Device: Devices which are not a part of the mesh network.

Provisioning: The process to turn un-provisioned devices to a node.

Elements: Multiple constituent parts of a node.

Messages: Messages are sent by one node to another to query about the status or control them.

Publishing: The act of sending a message from nodes in the network.

Subscribing: The act of selecting messages sent to certain addresses by the nodes for processing.

II.IMPLEMENTATION

A.SYSTEM OVERVIEW

All the nodes are programmed with the same firmware for easy identification of the nodes in the network. Flooding mechanism is implemented in the network which eliminates the need of separate processing to deal with the changes in the network parameters. There is no limit to the number of nodes that can be a part of the network without considering interference on the BLE channels. This implementation also prevents connection between nodes which has the new relayed data or has already received data from some other node thus making it a reliable network.

B. REQUIREMENTS

The hardware CY8CKIT-042-BLE Bluetooth Low Energy BLE Pioneer Kit is used. The design tool used is PSOC Creator 4.2 and CySmart 1.0.

III. EXPERIMENTAL SETUP

The data among the nodes is relayed after the establishment of a connection. The node which hasthe data transmits it to all the nodes or a node whose address has been selected. Each node is made to switch between GAP central and peripheral roles.

Each node supports both GAP central and GAP peripheral role. The GAP peripheral device advertises its data which contains the ADV data counter value ranging from 0-255. Every time a new data reaches the node, the counter is incremented. The GAP central device will scan for the advertisement packets. It will read the value of the counter and determine if the node has received a new data. The central node will connect to the peripheral node only if it has old data.

Once connection is established between the scanning node and advertising node, the scanning node is known as a GATT Client and the advertising node is known as a GATT Server. Once the client writes the data to the server, the server will disconnect and switch its role to that of a central device. Every GAP central node is assigned an internal timer which will trigger a role switch after specified intervals of time. Five BLE pioneer kits are used for implementation.

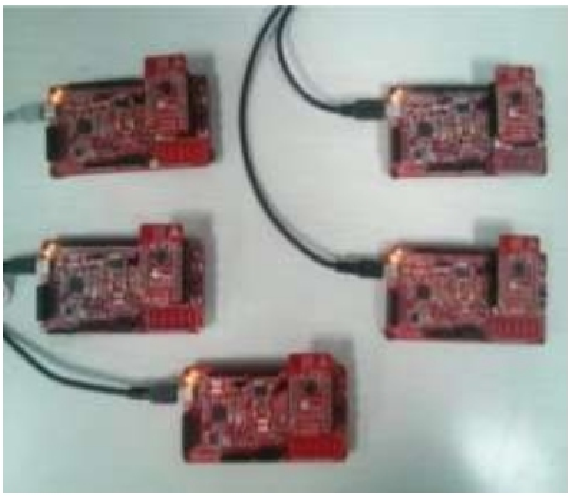
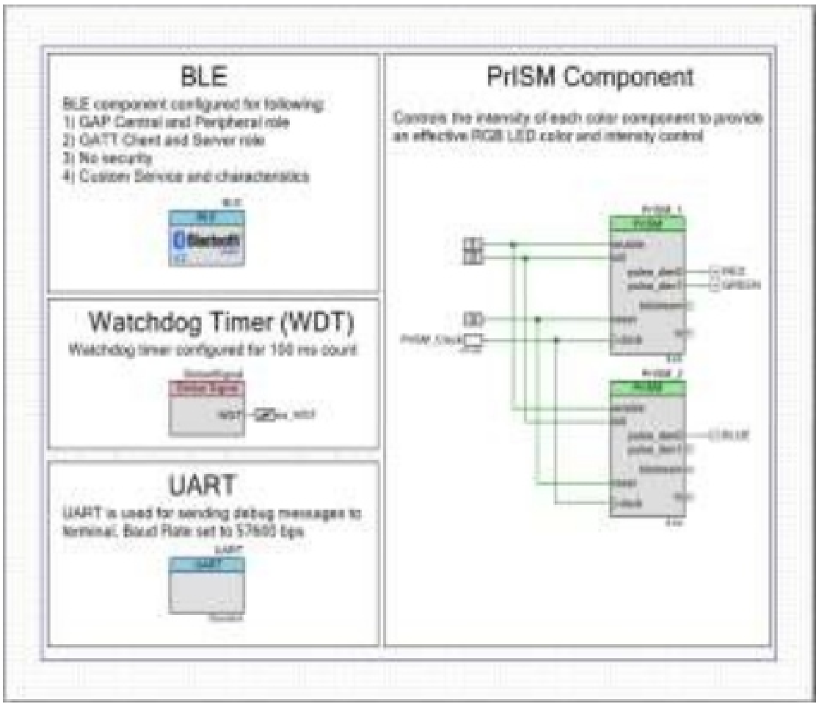


Figure 1: Initial Kit Setup



BLE

BLE component configured for following:
1) GAP Central and Peripheral role
2) GATT Client and Server role
3) No security
4) Custom Service and characteristics

Watchdog Timer (WDT)

Watchdog timer configured for 100 ms count

UART

UART is used for sending debug messages to terminal. Baud Rate set to 57600 bps

PrISM Component

Controls the intensity of each color component to provide an effective RGB LED color and intensity control

Figure 2: PSoC Creator Schematic

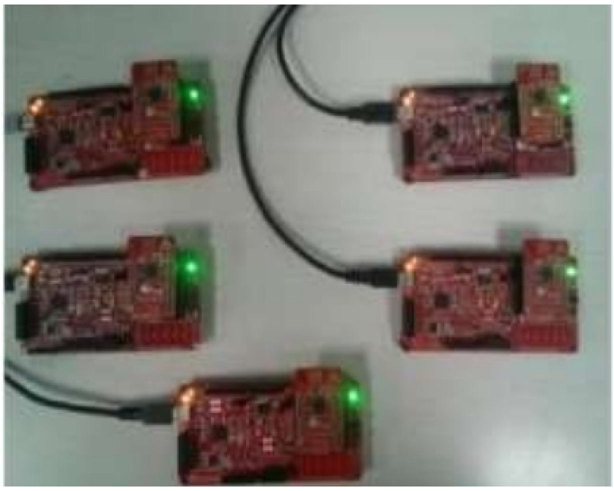
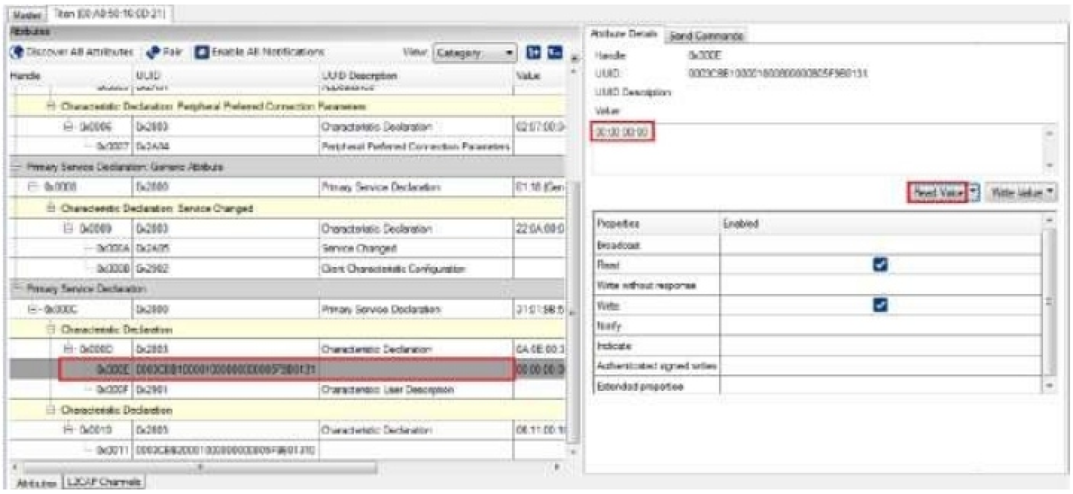


Figure 3: RGB data relayed to all nodes

IV. RESULTS AND DISCUSSIONS

After we program the device with the appropriate firmware, the device acts as a peripheral and starts advertising. The central device which is CySmart Tool, scans for all the peripheral devices which are advertising. The central is made to connect to our peripheral device. The RGB value needs to be located and it is observed that it is a 4 byte value. This value is modified and written to the peripheral device. The format of the value field is [Red:Green:Blue:Intensity]. On writing a value, the device will be disconnected immediately and all the nodes will show the same colour on the led. So, when we changed the RGB led colour on one peripheral node, it got relayed to all the other nodes. In this way, the range of the Bluetooth network can be increased. From a simple point to point link, we demonstrated a mesh architecture.

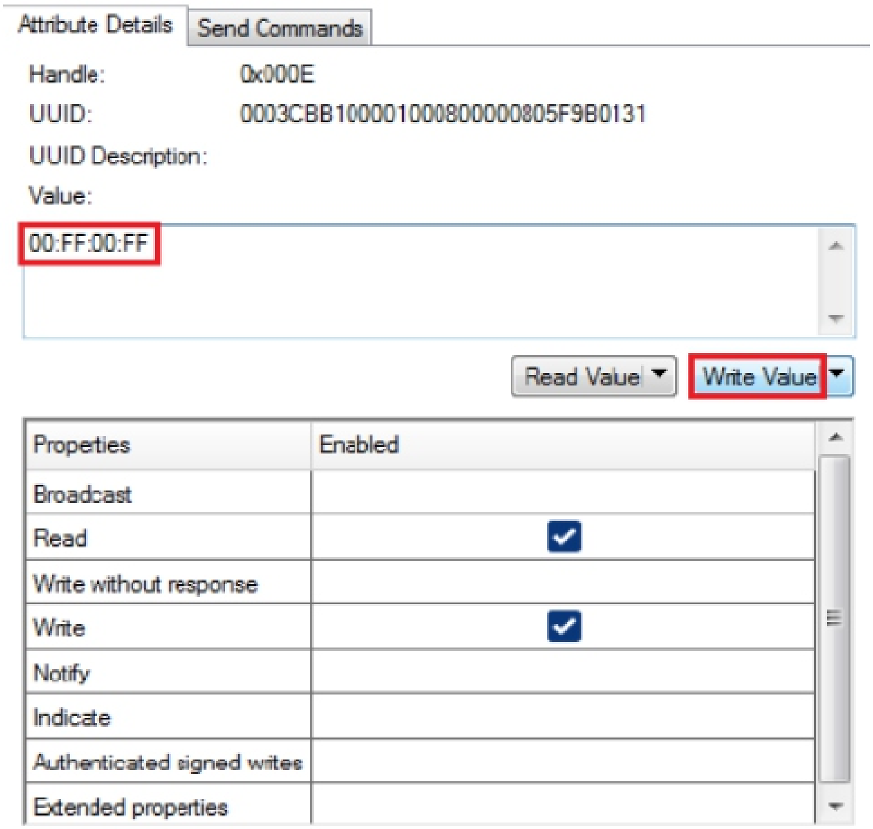


Handle	UUID	UUID Description	Value
Characteristic Declaration: Peripheral Preferred Connection Parameters			
0x0006	0x2803	Characteristic Declaration	02:07:00:0
0x0007	0x2A04	Peripheral Preferred Connection Parameters	
Primary Service Declaration: Generic Attribute			
0x0008	0x2800	Primary Service Declaration	01:18 (Gen
Characteristic Declaration: Service Changed			
0x0009	0x2803	Characteristic Declaration	22:0A:00:0
0x000A	0x2A05	Service Changed	
0x000B	0x2902	Client Characteristic Configuration	
Primary Service Declaration			
0x000C	0x2800	Primary Service Declaration	31:01:9B:5
Characteristic Declaration			
0x000D	0x2803	Characteristic Declaration	0A:0E:00:3
0x000E	0003CBB100001000800000805F9B0131		00:00:00:0
0x000F	0x2901	Characteristic User Description	
Characteristic Declaration			
0x0010	0x2803	Characteristic Declaration	08:11:00:1
0x0011	0003CBB200001000800000805F9B0131		

Handle: 0x000E
UUID: 0003CBB100001000800000805F9B0131
UUID Description:
Value:
00:00:00:00

Properties	Enabled
Broadcast	
Read	☑
Write without response	
Write	☑
Notify	
Indicate	
Authenticated signed writes	
Extended properties	

Figure 4: Reading the existing colour value of RGB Led

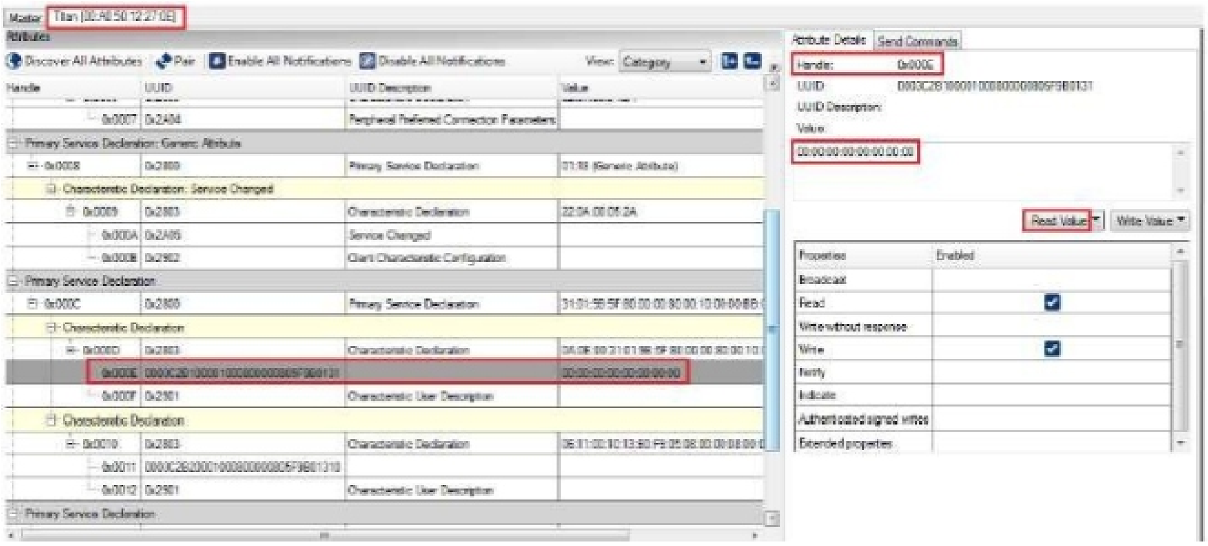


Handle: 0x000E
UUID: 0003CBB100001000800000805F9B0131
UUID Description:
Value:
00:FF:00:FF

Properties	Enabled
Broadcast	
Read	☑
Write without response	
Write	☑
Notify	
Indicate	
Authenticated signed writes	
Extended properties	

Figure 5: Writing a new RGB value to the peripheral

In case of the directed BLE mesh, the data is transmitted to the peripheral device with a particular device address. After establishing connection between the central and peripheral node, the attribute with a handle of 0x0015 is read from the peripheral and modified to set a unique node address. Each node is assigned a unique address. The 8 byte data is then read from the RGB custom characteristic.

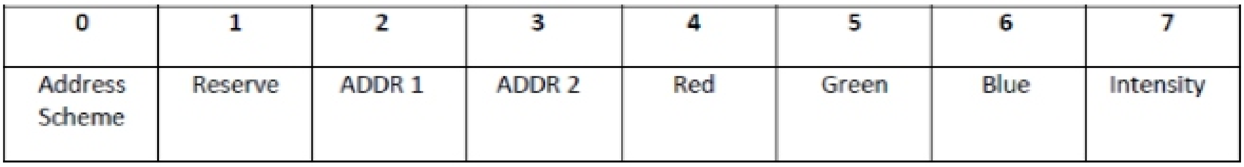


Handle	UUID	UUID Description	Value
0x0007	0x2A04	Peripheral Preferred Connection Parameters	
Primary Service Declaration: Generic Attribute			
0x0008	0x2800	Primary Service Declaration	01:18 (Generic Attribute)
Characteristic Declaration: Service Changed			
0x0009	0x2803	Characteristic Declaration	22:0A:00:05:2A
0x000A	0x2A05	Service Changed	
0x000B	0x2902	Client Characteristic Configuration	
Primary Service Declaration			
0x000C	0x2800	Primary Service Declaration	31:01:59:5F:80:00:00:80:00:10:00:00:B8:[illegible]
Characteristic Declaration			
0x000D	0x2803	Characteristic Declaration	0A:0E:00:31:01:59:5F:80:00:00:80:00:10:[illegible]
0x000E	[illegible]		00:00:00:00:00:00:00:00
0x000F	0x2901	Characteristic User Description	
Characteristic Declaration			
0x0010	0x2803	Characteristic Declaration	06:11:00:10:13:60:F9:05:08:00:00:08:00:[illegible]
0x0011	[illegible]		
0x0012	0x2901	Characteristic User Description	
Primary Service Declaration			

Handle: 0x000E
UUID: [illegible]
UUID Description:
Value:
00:00:00:00:00:00:00:00

Properties	Enabled
Broadcast	
Read	☑
Write without response	
Write	☑
Notify	
Indicate	
Authenticated signed writes	
Extended properties	

Figure 6: Attributes of the peripheral node



0	1	2	3	4	5	6	7
Address Scheme	Reserve	ADDR 1	ADDR 2	Red	Green	Blue	Intensity

Figure 7: Data format

The first byte represents either general addressing(0x00) or piconet addressing (0x01). The second byte is for future use. The next two bytes indicates the peripheral device address to which the data needs to be sent in the mesh network. We can set a broadcast address (0:00) so that all the nodes accept the data packets. Otherwise, the node whose address is set will receive the data packet. The next four bytes indicates the RGB colour and the intensity which needs to be transmitted to the mesh network. After writing the value to the node, it will be disconnected. Depending on the address field set, either all the nodes will receive the colour value or a particular node.

CONCLUSION

Bluetooth is a very popular technology in this century. But the shortcoming of a peer to peer network can limit its usages. So, the mesh network which can be easily implemented in the Bluetooth can expand the use cases of Bluetooth. It can provide longer range and allow communication between devices which are not in the direct radio range of each other. In this paper, mesh functionality has been demonstrated with PSoC Kit. The data is being relayed to a node which is not in the direct radio range of the transmitting node. Hence, extending the Bluetooth range can be a boon to a lot of IOT applications in today's world.

REFERENCES

[1] Julio León, Abel Dueñas, Yuzo Iano, Cibele Abreu Makluf, Guillermo Kemper, "A Bluetooth Low Energy Mesh Network Auto-Configuring Proactive Source Routing Protocol" , IEEE International Conference on Consumer Electronics (ICCE), 2017.

[2] Alexandre Adomnicai, Jacques J.A. Fournier, Laurent Masson, Hardware Security Threats Against Bluetooth Mesh Networks", IEEE International Workshop on Attacks and Defenses for Internet-of-Things (ADIoT), IEEE CNS, 2018.

[3] Comparing the energy requirements of current Bluetooth Smart solutions; Embedded World, February 2014, Nuremberg.

[4] Bluetooth Special Interest Group, "Bluetooth Core Specification Version 5.0," December, 2016.

[5] White Paper, "Bluetooth Mesh Networking", Ericsson, July 2017.

[6] Bluetooth Special Interest Group, "Bluetooth Mesh - What a Difference a Year Makes", July 2018.

[7] Bluetooth Special Interest Group, "Mesh Profile Specification 1.0", July 2017.

[8] Bluetooth Special Interest Group, "Mesh Technology Overview" July 2017.

[9] Cypress Semiconductors, "Getting Started with PSoC 4 BLE", An91267.

[10] Cypress Semiconductors, "PSoC 4 BLE Architecture, Technical Reference Manual"

[11] Cypress Semiconductors, "Bluetooth Low Energy Pioneer Kit Guide", 2015.

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).
2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);
3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);
4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.

The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Address of the Editorial Office:

Enriched Publications Pvt. Ltd.
S-9,IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR -5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-45525005

Note