IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 4, April 2021

DOI: 10.17148/IARJSET.2021.8427

Secure Anonymous Authentication with Location Privacy for IOT-based WSN

JAYANDHI.G[1], A.DIVYADHARSHINI[2], J.GAYATHRI[3], K.UMAMAGESWARI[4], M.N. VIJI[5], S.YUVARANI[6]

Assistant Professor, Department of Electronics and Communication, Velammal Engineering College,Chennai,India[1]

B.E Final Year, Department of Electronics and Communication, Velammal Engineering College,Chennai,India[2,3,4,5,6]

Abstract: Internet of Things (IoT) may be a new technological paradigm which will connect things from various fields through the web . For the IoT connected sensor applications, the IOT based sensor network is gaining popularity into the market. In the recent years, numerous anonymous authentication schemes were proposed to supply security in sensor networks. However, many of those schemes aren't computationally efficient during anonymous authentication. Moreover, the previous schemes did not provide location privacy for both the sender and receiver. In order to overcome these limitations, in this work, we propose an efficient and secure anonymous quantum encryption-based authentication framework with location privacy preservation for IoT-based sensors. The comprehensive analysis section shows that the proposed scheme overcomes the safety weaknesses within the existing schemes and also provides low computation cost during anonymous authentication.

Keywords : Internet of Things (IOT),Sensor Networks,Quantum Encryption,etc.,

I. INTRODUCTION

Research and technology advances incessantly extend and diversify wireless sensing element network (WSN) relevance. As a consequence, WSN designers visaged associate increasing vary of applications and needs beneath rising value and time pressures since the net of Things (IoT) paradigm was coined over fifteen years before. “Typical” needs for WSN hardware and software system square measure more and more troublesome to outline [2] as a result of the incessantly adapt to terribly various application needs and operative conditions at a rate that doesn't appear bogged down by standardization efforts. Moreover, though WSN solutions square measure used for varied applications, the implementations usually disagree beneath numerous aspects that considerably cut back the economies ranking. Consequently, each hardware and software system of WSN solutions square measure usually application-specific prototypes that carry vital non-recurrent engineering (NRE) prices and risks (e.g., dependableness, improvement, development time). in addition, for numerous sensible reasons WSN deployments square measure generally developed at lower abstraction levels, which may have 2 vital undesirable effects. First, this will divert a vital development effort from application logic implementation, that will increase development time and price, and customarily decreases ability.Second, lower abstraction level development usually needs competencies that square measure rarely found among application domain consultants, which may cause higher development value and a lot of reluctant adoption of WSN based solutions. The physical vulnerability is that the incontrovertible fact that sensors square measure scattered in insecure place like public places, the natural environments (mountainous region) similarly because the buildings, sensible homes and museums (smart environment), thus assaulter have the physical access to the node, and with applicable tools, he will browse the key info (like keys, programs, etc) hold on within the node.Alternative vulnerability is said to wireless technology. in contrast to the standard wired networks, the attackers might simply capture the information packet as a result of the information transmissions square measure bushed the air. Whoever having the adequate receiver will doubtless hear or disturb the changed messages. sensing element nodes square measure themselves routers. Packets have totally different nodes in multi-hops routes to hit their destination. thanks to the potential of violation of such nodes, this feature presents a significant vulnerability.Sensing element nodes square measure liable to failure, that create topology dynamic. Dynamic configuration may be caused additionally by the quality of nodes and addition of latest nodes. A variety of attacks against WSNs is documented within the literature. To face these attacks, numerous against measurements were planned. A classification of the attacks consists in characteristic the passive attacks from the active attacks. The passive attack (eavesdropping) is restricted to listening and analyzes changed traffic. This sort of attacks is less complicated to comprehend (it is enough to own the adequate receiver), and it's troublesome to sight. Since, the assaulter doesn't create any modification on changed info.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 4, April 2021

DOI: 10.17148/IARJSET.2021.8427

II. RELATED WORK

Gandino et al have planned a practical anonymous user authentication in wireless device networks. The planned theme is appropriate for the situation that the legitimate user is allowed to access device knowledge from any specific device node within the surroundings of resource unnatural wireless device network.

Filippo Gandino et al have study associate degree in-depth analytical on the progressive key distribution schemes supported random predistribution. A brand new protocol, known as q-s-composite, is planned so as to use the simplest options of random predistribution and to boost it with lower necessities.

Uluagac et al introduce associate degree energy-efficient Virtual Energy-Based encoding and Keying (VEBEK) theme for WSNs that considerably reduces the amount of transmissions required for rekeying to avoid stalekey.

Anuja et al focused-on knowledge aggregation technique is to assemble and cluster knowledge packets in a very well-organized and co-effective approach thus on minimize power consumption, to accentuate network life time, delay, hold up. In wireless body space network knowledge aggregation with high delay tolerance is of utmost importance.Dynasty.

III. PROPOSED SYSTEM

This project is that specialize in a singular key generation technique referred to as Quantum key distribution, that is employed to form bilaterally symmetric key methodology by mistreatment quantum properties of optics to transfer data from one consumer to a different in One-TimePad manner. The special feature of the technique is to ensure that the key cannot be intercepted throughout transmission while not alerting the users to produce high authentication for received info.

A. Secure Key Management Technique

The planned & enforced system is that the Wireless Body space Network mechanism for secure key management. It having the Wireless Body space Networks set that is connecting to server of backend. With the assistance of net, the device measured data of biometric from node of the device to the server of master with the relay of Backend server.Supported a id of a node each device ascertain the server of the master. A secret key that is exclusive will be generated master server for each node of the device. If a node wish to travel for a network then that node send request to master server that is protected with mack through server of backend. The mack will be verified by master server provides message& passkey thereto node and once more it transmitted to the backend server. The key belongs of the message & master will be encrypted by backend server and transmitted the actual node of the device for beginning the method of the connection. when completion of receiving the keys by all nodes, the rekeying time will be scheduled by baccalaureate for refreshing the passkey. Wireless Body space Networks set that consists of, Server of Backend (BS) & Server of Master (MS). Fig describes a network of Wireless Body space Network having a device that's deployed in body. Of these are having the communication with Backend Server. Wireless Body space Networks connected to the Backend Server ar having a communication network with the Master Server.

a) Message Key (Kmsg): It is used for providing communication between backend server & nodes of all sensors.
b) Passkey (Kmas): With facilitate of rekeying planning, its refresh message key.
c) Secret key (Ksec): Security key is unique key. it can be sharable to master server. Each is node having a separate security key.

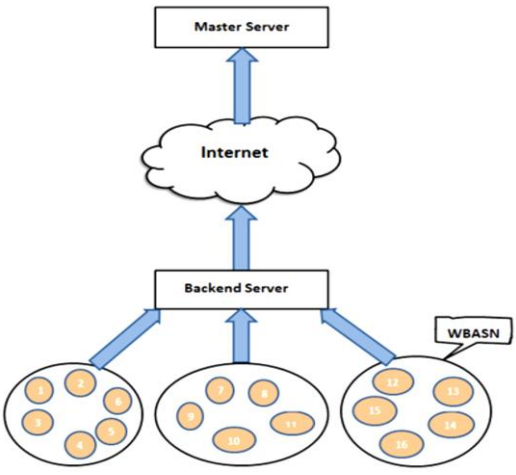

Fig 4.1 System Architecture

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 4, April 2021

DOI: 10.17148/IARJSET.2021.8427

B. STORAGE SERVER ARCHITECTURE

A storage server can method the information and stores the information in storage devices or servers. A streaming server readying needs a minimum of one information server (the primary storage server). All the information is saved in storage devices or servers (files, blocks, object storage) or folders, is conferred to each the system storing it and also the system retrieving it within the same sort. Install the information server before putting in any traditional servers. File storage design is additionally known as as file-based storage design, that stores knowledge in a very information server. knowledge may be accessed exploitation the Network filing system (NFS) protocol. Parallel Network filing system (PNFS) is a component of the Network filing system that permits all the shoppers to access storage devices directly. this ~~can~~ be achieved by separating knowledge and information and moving the information server out of the information path.

C. MANUAL AUTHENTICATION TECHNIQUE

For transmittal the manual knowledge among the all devices, it uses the wireless devices & wireless channel authentication. copy of output knowledge to 1 appliance to a different device, 2 devices output comparison; enter same data in each device may be wiped out transfer of knowledge manually. Here no would like of coming into the information by user. Usually, the person has got to enter thirty-two binary digits.

Implementation of Quantum Key Cryptography
1.The coding & authentication is critical foreach trans-mitted message in network. The biradial key shared with Sensor Nodes and Master Server is given by

SNi K k (SN)sy sec i = λ, Ksec (SNi) is a secret key. SNi - the server of master sent a passe-partout to every node that is exclusive once authentication victorious.
2.Two sub keys holed by Ksec, those square measure key for coding key (ke) & key for Message Authentication Code (kmac): K k K M e mackintosh = --- (2) Ksec Sn MS i ← (3).
If the a knowledge transmitted from device node to Master server, then it may be encrypted with the assistance of ke & signed; by exploitation mackintosh key Kmac - before transmission. Format for this can be Sn MS : t mac(K t) i s ke, mackintosh s ke → (4) If any node knowledge received by Master Server. it verifies knowledge and so decrypted. With the assistance of Key of coding and mackintosh, a secure association may be established. Initialization

For connexion into a network, with the assistance of Master Server. The nodes of every device has been initialized. Here, sharing of biradial key done between Master Server& Backend Server. By exploitation the non-public & channel of out band all this method may be done. looking on the nodes of device physical characteristics, attest & non-public channel creation may be done. with confidence we are able to transmit the information via channel, integrity of knowledge & authentication square measure all obtained during this technique. Here, the entry perform done by backup server. The communication in between nodes of WBNS & server of master activates the node of device SNi firmly during this non-public channel. Out-of-band channel transfer-ring of knowledge involves the subsequent steps.
1. Master server receives the ID of SNi from device node – ID Sn MS i → ---------- - (5)
2. In express nature, this may be done. as a result of special proper-ties of Out of band channel, SNi ID may be done implicitly.
3. the key key that is willy-nilly generated by Master server send to the Sni -Ksec SN MS i ←-------- (6) Ksec stores in device node likewise as in Master server of memo-ries. therefore we are able to say that the every nose of device SNi having a separate KSec Secrete key. And it additionally having a singular Counter (C) that have the zero initial values that is (CTR→0) is in buffers of device.. to forestall attacks reply & consistency guarantee, counter values square measure useful.when the worth of the counter in-creased by one once accessing it.
A join request (JREQ) forwarded by Sensor Node i to Base station
1.Device Node sends a be a part of request to the bottom Station. JREQ Sn baccalaureate i ← (7)
2. With facilitate of Ksec generated by mackintosh whereas SNi connexion, The protection of JREQ done -sec
JREQ : mackintosh nine K baccalaureate sends JREQ to MS: JREQ baccalaureate MS → MS (8)

Verification of the mackintosh and message key Kmsg generated initial-ly and Node of passe-partout Kmas causation to baccalaureate - MS baccalaureate K K flavorer mas + → baccalaureate - (9) Kmsg with Kmas encrypts & forward to the device Node EK mas flavorer baccalaureate Sn Sn.

D. One-Time Pad Manner

A One-time pad could be a symmetrical cryptosystem that's a style of cryptosystem that has been verified as indestructible albeit it's forced to use. every character or little {bit of} the plaintext is encrypted with a regular addition of a personality or bit of a secret random key (or pad) of the same length because the plaintext, dynamical it into a cipher text. OTP can

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 4, April 2021

DOI: 10.17148/IARJSET.2021.8427

not be unbreakable if any of the subsequent conditions is vulnerable. If key data of Master Server received by SNi, The fundamental quantity of rekeying in deep trouble refreshing the key of the master server. The rekeying amount may be broad-casted by Bachelor of Science with Kmsg that is freshly updated, encrypting through with Kmas to Nodes of sensors metali - EK mas flavoring Bachelor of Science SN metal i rekeying request (RE_REQ) may be send by detector Node i, within the amount of rekeying request (RE_REQ) send via Backend Server to the Master Server - RE nine REQ i RE nine REQ metal Bachelor of Science (Authentication channel) MS → → MS updated is freshly generated sends to Kmas which will be encrypted with Ksec for All Sni respectively :

Ek ' mas MS metal ------- (11)

E. PROPOSED ALGORITHM:

Step 1

WSNs set,; Server of Master; server of Backend; included in the .network of WSN having the some detectors consists of few sensor devices deployed on a person's body that are connected to a Backend Server (BS).

Step 2

The Server of backend server and master having a shared radially symmetrical key. All nodes of the sensors notice outs the sever of the master the master server with the assistance of a node id, then Ksec generated for every node by Master server.

Step 3

If a node would like to enter into a network, it requested the master server by causation the REQ. Message Authentication Code shield the REQ with the assistance of secret key of ksec for node change of integrity

Step 4

After getting the Message of request, it is transferred from rear to master (both rear and master are webservers).

Step 5

Raincoat is verified by master server initial message key kmsg is generated by passkey kmas for every node transferred to backend server.

Step 6

Kmsg is encoded with kmas in the backend server. Transmitted to detector nodes.

Step 7

After whole nodes receiving the information of key from server of master server, & BS scheduled rekeying time for refresing master key.

IV. RESULT AND DISCUSSIONS

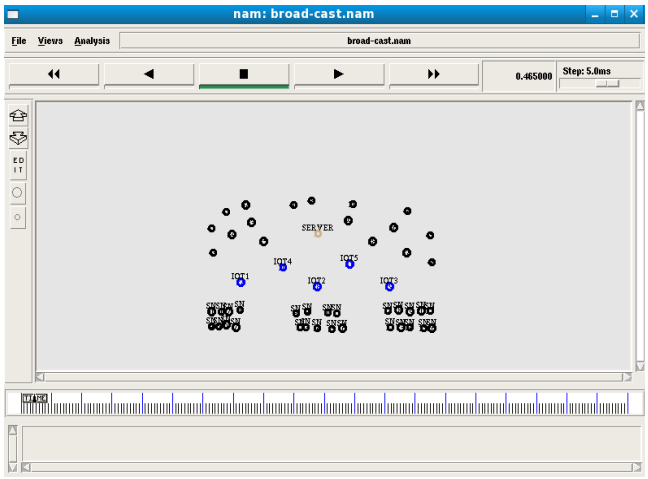

Fig node creation

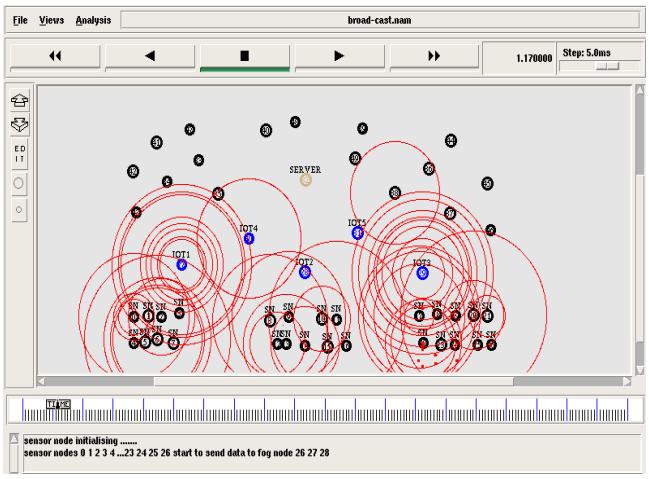

Fig Data collection from sensors

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 4, April 2021

DOI: 10.17148/IARJSET.2021.8427

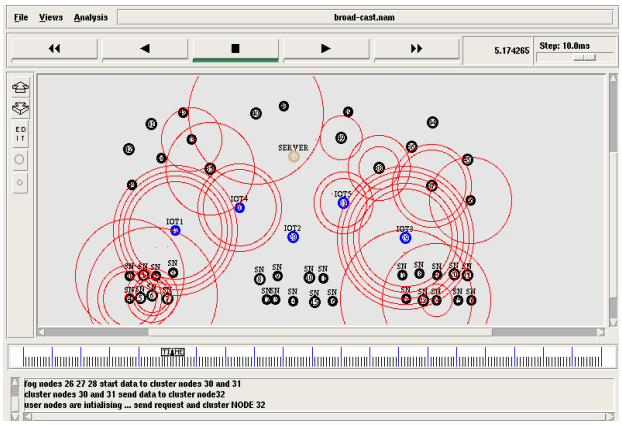

Fig IOT node to server communication

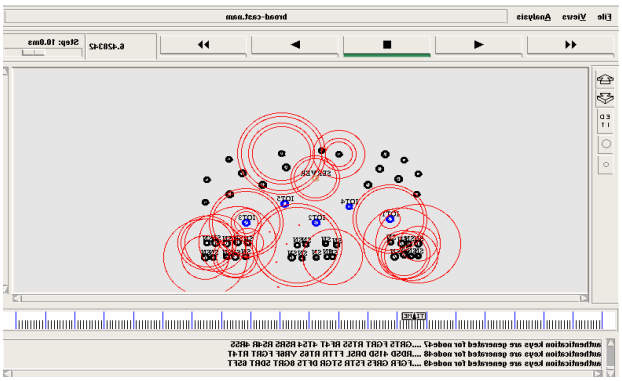

fig key generation and pairing

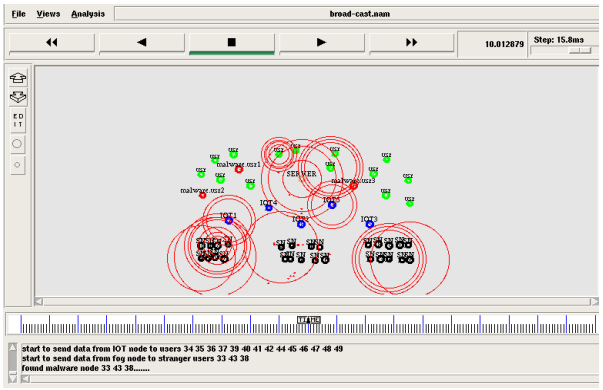

Fig Intruder detection

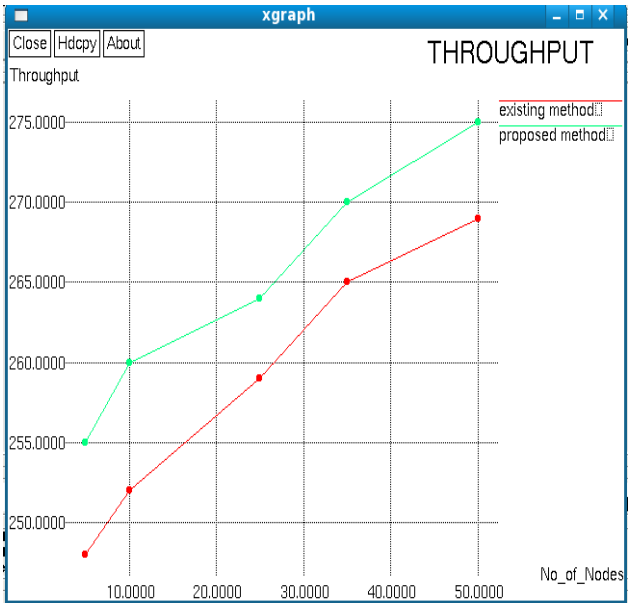

Fig through put analysis

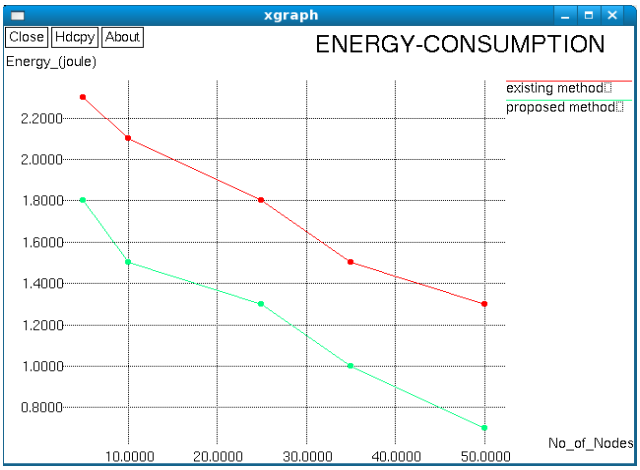

Fig energy consumption

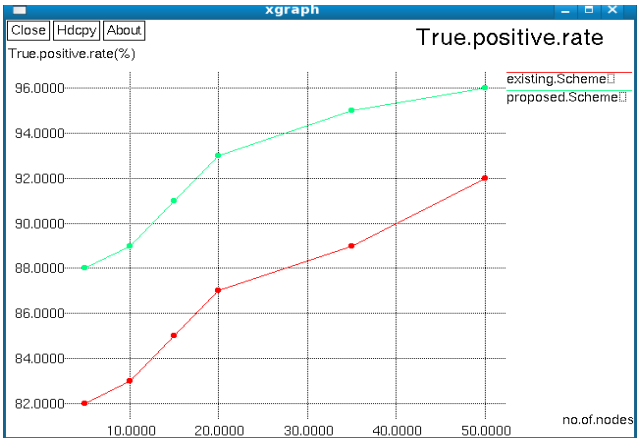

Fig True positive rate

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 4, April 2021

DOI: 10.17148/IARJSET.2021.8427

Fig False positive rate

V. CONCLUSION

Secure key management method of Wireless sensor Network is interfaced to the backend server . By using the internet, sensors node measure the data that is sent to a server which acts as master by Backend server. Based on Quantum Key Cryptography, data is security is maintained on the sensitive data during transmission with the help of quantum mechanics where photons are used for communicating with other location. Due to the usage of light medium for transmission of key through One Time Pad Manner, the results obtained in simulation in proposed work depict considerable packet delivery ratio, less overhead & delay and highly secured data with no loss.

VI. FUTURE WORK

Future proposed a revocable certificateless encryption (R-CLE) scheme against decryption key exposure, and a revocable certificateless signature (R-CLS) scheme against signing key exposure.

VII. RESULT

In this application, we proposed an efficient and secure anonymous authentication framework location privacy preservation for IoT based WBAN's.The future extensions of this work is to provide the batch authentication to the communicating users in an efficient manner.

REFERENCES

1.Dong Li, Yixian Yang, Yang Xin, & Bin Tian. (2010). A PRC based key management method for wireless sensor networks. 2010 IEEE International Conference on Information Theory and Information Security.
2.Bin Tian, Yang Xin, Shoushan Luo, Xiou Yang, Dong Li, Zhe Gong, & Yixian Yang. (2010). A novel key management method for wireless sensor networks. The third IEEE International Conference on Broadband Network and Multimedia Technology(2010) .
3.Guohua Ou, Jie Huang, & Juan Li. (2010). A key-chain based key management scheme for heterogeneous sensor network. 2010 IEEE International Conference on Information Theory and Information Security.
4.Wei Wang, Hempel, M., Dongming Peng, Honggang Wang, Sharif, H., & Hsiao-Hwa Chen. (2010). On Energy Efficient Encryption for Video Streaming in Wireless Sensor Networks. IEEE Transactions on Multimedia, 12(5), 417–426.
5.Younis, M. F., Ghumman, K., & Eltoweissy, M. (2006).s Combinational Key Management Scheme provides location awareness for Clustered Sensor Networks. IEEE Transactions on Parallel and Distributed Systems, 17(8), 865–882.
6.Gope, P., & Hwang, T. (2016). Lightweight Anonymous Authentication Protocol provides Security for Real-Time Application Data Access in WSN. IEEE Transactions on Industrial Electronics, 63(11), 7124–7132.
7. Yingshu Li, & Copeland, J. A. (2010). VEBEK: Virtual Energy used for Keying and encryption in WSN. IEEE Transactions on Mobile Computing, 9(7), 994–1007.
8.Gandino, F., Ferrero, R., & Rebaudengo, M. (2017). Mobile Wireless Sensor Networks uses Key Distribution Scheme: q - s - Composite. IEEE Transactions for the security and Information Forensics , 12(1), 34–47.
9.P. Vijayakumar, S. M. Ganesh, and L. Deborah, "A new smartsms protocol for secure sms communication in m-health environment," Computers & Electrical Engineering, vol. 65, pp. 265–281, 2018.
10. M. R. Ahmad , R. F. Malik, A. A. M. Isa and A. S. Al-Khaleefa, "Optimized authentication for WSN," Journal of Network and Computer Applications, vol. 10, no. 2, pp. 137– 142, 2018.