Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7697608

UNTRACEABLE AND SECURE SENSOR NETWORK AUTHENTICATION WITH PRIVACY REGARDING LOCATION

Dr.Kalyankumar Dasari
Associate Professor, Chalapathi Institute of Technology, Mothadaka, Guntur,Andhra Pradesh, India. dkkumar123@gmail.com

Pagidi Premchand
Assistant professor, Chalapathi Institute of Technology, Mothadaka Guntur, Andhra Pradesh, India, premchand.pagidi@gmail.com

Devarapalli Sekhar Babu
Assistant Professor, Chalapathi Institute of Technology, Mothadaka Guntur, Andhra Pradesh, India, sekhardevarapalli11@gmail.com

Abstract: The Internet of Things (IoT) has the potential to usher in a brand-new era of web connectivity, bringing together physical objects from all walks of life. The IoT-based sensor network is becoming increasingly popular for use in IoT-connected sensor applications. Several anonymous authentication systems have been presented as a means of providing security for sensor networks in recent years. Many of these techniques, however, suffer from a lack of computational efficiency when used for anonymous authentication. In addition, prior techniques did not ensure that both the sender and the receiver's locations were kept secret. In this work, we present an anonymous quantum encryption-based authentication framework for IoT-based sensors that is both secure and efficient, and that also protects users' right to geographic anonymity. The extensive research demonstrates that the suggested approach not only provides reduced computing cost during anonymous authentication but also eliminates the safety issues present in existing schemes..
Keywords : Internet of Things (IOT),Sensor Networks,Quantum Encryption,etc.,

I. INTRODUCTION

The importance of wireless sensing element networks (WSNs) is always growing and changing as a result of research and technological advancements. Since the internet of things (IoT) concept was defined over fifteen years ago, WSN designers have faced a growing variety of applications and needs while under increasing cost and schedule pressures. As WSNs continue to rapidly adapt to a wide variety of application requirements and operating situations, it becomes increasingly difficult to define "typical" needs for WSN hardware and software systems [2]. And even while WSN technologies are employed in different contexts, implementations frequently diverge in numerous ways that substantially lower economies' overall rankings. Thus, WSN systems' hardware and software are typically application-specific prototypes with high non-recurring engineering (NRE) costs and risks (e.g., dependableness, improvement, development time). In addition, there are a variety of practical reasons why WSN

installations are typically built at lower abstraction levels, which can have two significant unintended consequences. For starters, this will take valuable time and resources away from implementing the actual logic of the programme, which will increase costs and reduce efficiency. Second, increased development costs and scepticism towards WSN-based solutions may result from the lack of expertise in developing at lower abstraction levels, which is uncommon among application domain consultants. The physical vulnerability is that sensors are dispersed in insecure places like public spaces, natural environments (mountainous region), buildings, smart homes, and museums (smart environment), so an attacker can gain physical access to the node and, with the right tools, can access any sensitive data stored there. Others have pointed out that wireless technology is susceptible to attacks. The information transmissions in wireless networks are open to interception by hackers, unlike in traditional wired networks. Anyone with a sensitive enough receiver will pick up on the altered transmissions. The nodes of a sensing network act as routers. In multi-hop pathways, packets pass via a variety of nodes before arriving at their final destination. This feature is particularly vulnerable because such nodes can be violated. Nodes in the sensing element are vulnerable to failure, which makes the topology itself dynamic. Changes in node quality or the introduction of new nodes can also contribute to a network's dynamic configuration. In the literature, numerous attacks against WSNs are described. There were many countermeasures devised in anticipation of these assaults. Classifying attacks involves distinguishing passive attacks from aggressive ones. Eavesdropping, or a passive attack, consists solely of listening to and analysing altered traffic. It takes only a good receiver to understand these attacks, but they are difficult to spot. Since the attacker makes no further alterations to the altered data.

II. RELATED WORK

In order to implement anonymous user authentication in wireless device networks, Gandino et al. The proposed concept works well in the context of a resource-unnatural wireless device network, where a legitimate user may obtain device knowledge from any given device node.

There has been a lot of research and analytical work done by Filippo Gandino & co. on the topic of progressive key distribution techniques that use a random predistribution. To take advantage of the basic features of random predistribution and improve it with less constraints, a new protocol called q-s-composite is being developed.

Uluagac et al. provide a new, energy-saving WSNs with the Virtual Energy-Based encoding and Keying (VEBEK) theme can drastically minimise the number of rekey transmissions needed to avoid stalekey.

To reduce power consumption, increase network life time, delay, and hold up, Anuja et al. prioritised knowledge aggregation, which involves assembling and clustering knowledge packets in a very well-organized and co-effective way. The ability to aggregate knowledge with a high delay tolerance is crucial in wireless body space networks. Dynasty.

III. PROPOSED WORK

This work focuses on a novel key generation method called quantum key distribution, which is used to create a bilaterally symmetric key approach by exploiting the quantum features of optics to perform a One-Time-Pad-style data transfer between users. The unique aspect of the method is that it guarantees the key is not intercepted during transmission without informing the users, leading to strong authentication of the received information..

A. Secure Key Management Technique

The Wireless Body Area Network mechanism for secure key management is the intended and enforced system. It is equipped with a set of wireless body area networks that can establish a connection with a backend server. Measured biometric data was relayed from the device's node to the master server through the internet. Each client uses the id of a single node as its own unique identifier when determining which server acts as the central hub. The device's master server will generate a unique secret key for each node. Each node that needs to leave the network must first make contact with the master server, which is protected by mack, using the backend server. After the master server sends a message and passkey to the node, the node verifies the mack and sends the data back to the backend server. To initiate the connection process, the backend server will encrypt the message and master key before sending it to the device's actual node. Baccalaureate will set up a time for rekeying after all nodes have finished getting their keys. Set of Wireless Backend (BS) and Master (MS) Servers for Body Area Networks (MS). An example of a wireless body area network (Fig) with an internally-deployed device is shown. All of these can talk to the backend server. Connected wireless body area networks talk to the main server through the backend 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.

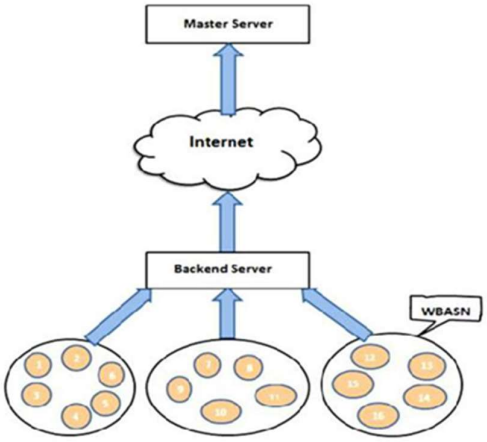

Fig 4.1 System Architecture

B. STORAGE SERVER ARCHITECTURE

A storage server can process the information and store it in storage devices or other servers. It can also store the information. A minimum of one information server is required for a streaming

server that is getting ready (the primary storage server). All of the information that is kept in storage devices or servers (files, blocks, or object storage) or folders is given to both the system that stores it and the system that retrieves it in the same format regardless of where it is kept. First, you should put in the information server, then you should install the traditional servers. A file storage design, also known as a file-based storage design, saves data on a specific information server. Another name for this type of storage design is file-based storage design. Using the Network File System (NFS) protocol, one can gain access to previously hidden information. Parallel Network filing system, also known as PNFS, is a component of the Network filing system that enables direct access to storage devices for all of the shoppers. This can be accomplished by isolating the knowledge component from the information component and removing the information server from 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)

Encrypting the mackintosh and message key Kmsg with Kmas and sending it on to the device Node EK mas flavorer baccalaureate Sn Sn requires first verifying that both the mackintosh and message keys were created correctly.

D. One-Time Pad Manner

A A one-time pad is an example of a symmetrical cryptosystem, which has been proven to be unbreakable despite the fact that its use is mandatory. Plaintext is transformed into cypher text by dynamically adding a personality or bit from a secret random key (or pad) of the same length as the plaintext to each character or little bit' of the plaintext on a regular basis. OT can not be impenetrable if any of the conditions that follow it are vulnerable. In the case that SNi is provided with access to the Master Server's vital information, The primary amount of rekeying in serious difficulty resetting the master server's key. A Bachelor of Science armed with newly updated Kmsg can make a rekeying forecast, encrypting data from sensor nodes using Kmas. materialistically - EK intense flavourings First-Class Honors B.S. in SN During the range of rekeying requests (RE REQ) sent from the Backend Server to the Master Server, detector Node I may transmit a rekeying request (RE REQ) for metal i. This would look like RE nine REQ I RE nine REQ metal. Diplomate in Science (Authentication channel) For Every Sni, a newly produced MS MS will be sent to Kmas and encrypted using Ksec. :

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

E. PROPOSED ALGORITHM:

Step 1

A few sensor devices worn on the body are linked to a Backend Server through a WSNs set,; Server of Master; server of Backend; included in the.network of WSN having the few detectors (BS).

Step 2

The master server and the secondary server both use the same radially symmetric key. The sensors at every node are aware

With the help of a node id, the master server is able to create Ksec for each node in the network.

Step 3

Nodes send a REQ to the network's master server if they want to join the network. The REQ is encrypted using a secret key of ksec generated by the Message Authentication Code in order to prevent a compromise in the node's integrity.

Step 4

Once the Request Message is received, it is forwarded from the slave to the master (both rear and master are webservers).

Step 5

Passkey kmas generates initial message key kmsg that is confirmed by the master server before being sent to the backend server..

Step 6

In the server's back end, kmsg is encoded with kmas. Radiated to the network's detector nodes.

Step 7

Time for rekeying and refreshing the master key is planned after all nodes have received the necessary key information from the master server..

IV. RESULT AND DISCUSSIONS

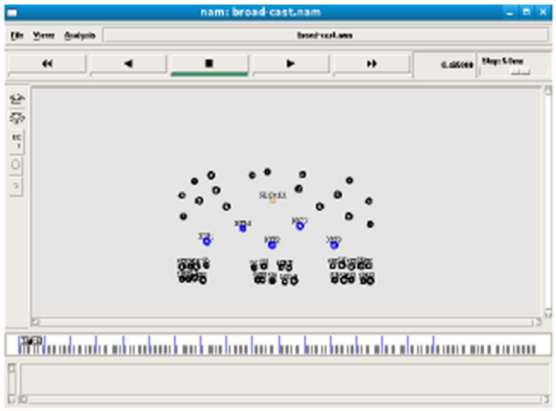

Fig node creation

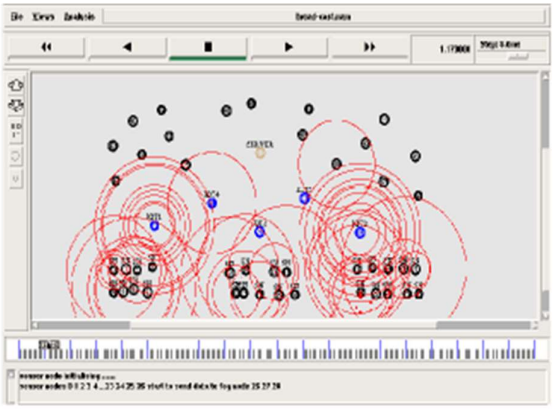

Fig Data collection from sensors

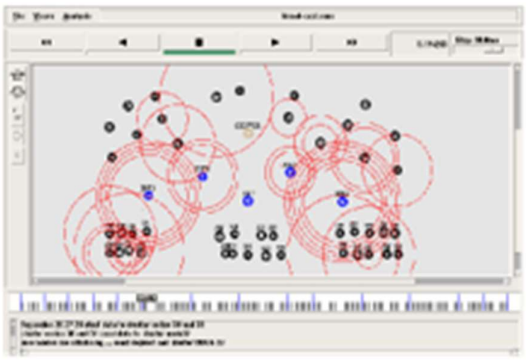

Fig IOT node to server communication

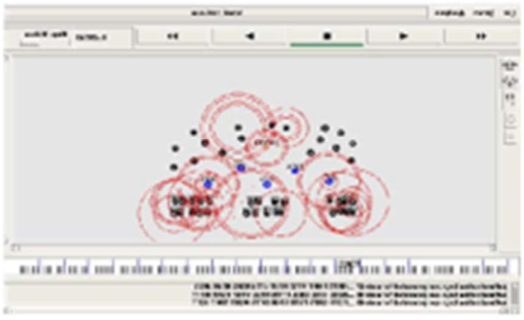

fig key generation and pairing

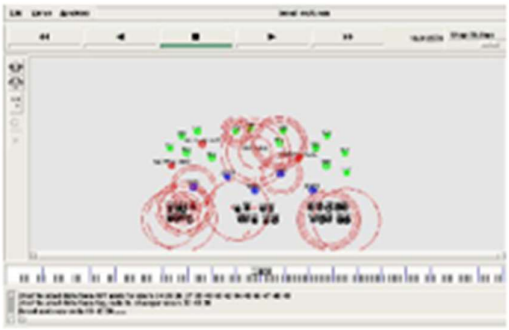

Fig Intruder detection

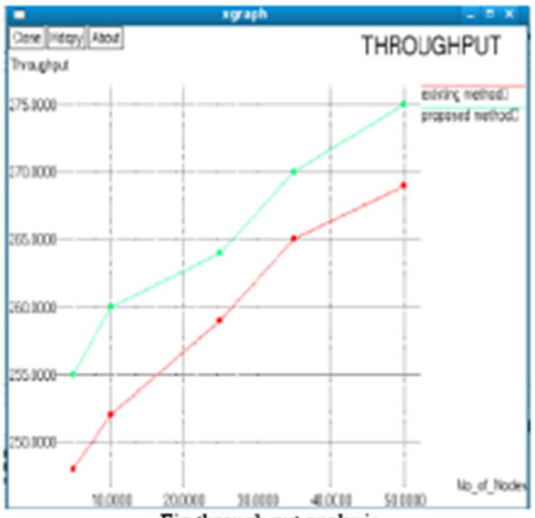

Fig through put analysis

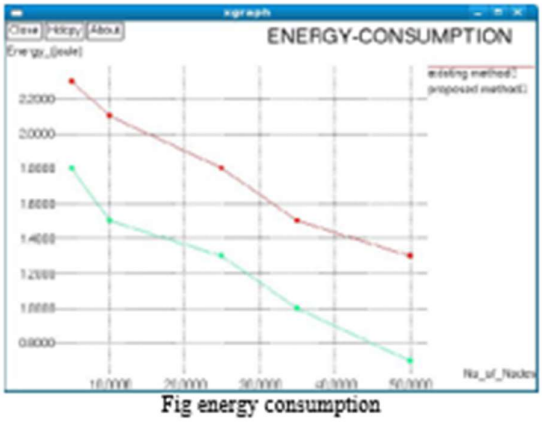

Fig energy consumption

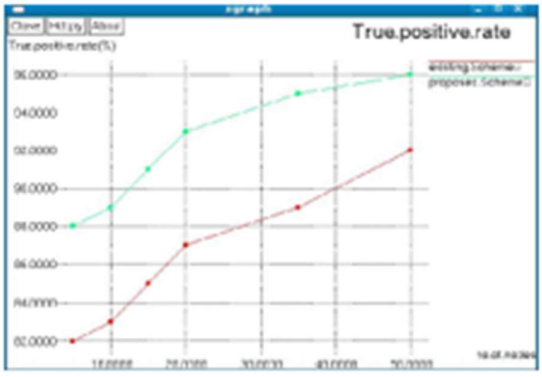

Fig True positive rate

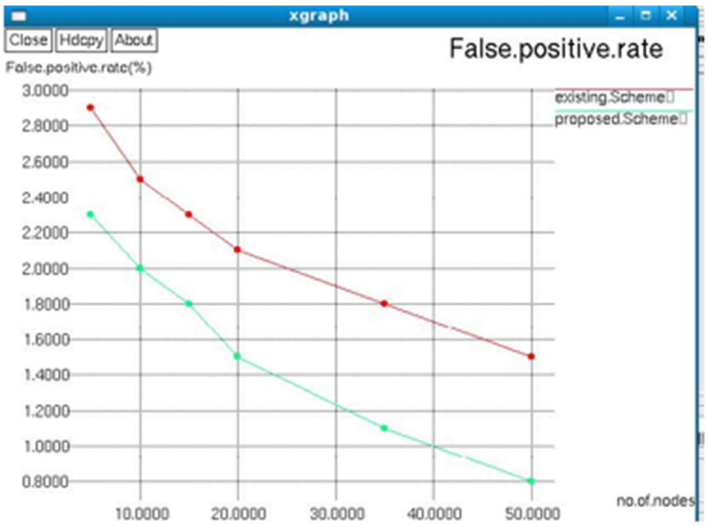

Fig False positive rate

V. CONCLUSION

A Risk-Free Approach to Key Management Connecting a sensor network that operates wirelessly to a server in the cloud. Data collected by each node is transmitted over the internet to a master server run by the system's backend. Quantum Key Cryptography is based on the use of quantum physics to encrypt and decrypt messages using photons to send and receive information securely from one point to another. Light medium for transmission of key through One Time Pad Method shows significant packet delivery ratio, reduced overhead & delay, and highly secured data with no loss, as shown in simulation results in proposed work..

VI. FUTURE WORK

In the future, a revocable certificateless encryption (R-CLE) method was proposed to protect against the disclosure of decryption keys, and a revocable certificateless signature (R-CLS) scheme was proposed to protect against the disclosure of signing keys..

VII. RESULT

The method we proposed for anonymous authentication in this application is both efficient and secure. IoT-based WBAN data storage and preservation. Extending this work in the future will allow for efficient batch authentication for communicating users..

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.