An E-Office Application Using a Lightweight and Quick Authentication Using IoT

Mr. Krishna Kumar P R [1]
VTU Research Professor,
Cambridge Institute of Technology,B-lore-36
rana.krishnakumar@gmail.com

Dr Chandramouli H[2]
Professor,EPCET
Bangalore-49.
hcm123cool@rediffmail.com

Dr Udaya Kumar K[3]
Prof & Director,CITNC
Bangalore
udaykumark@gmail.com

***Abstract*:** Internet of Things (IoT) is a thought of sharing electronic information over a network, which consists of physical objects are being networked with the web. IoT contains an honest set of "smart" devices and sensors which transfer data at the network through IoT applications. The rapid expansion of IoT and wireless technologies cause finding new opportunities for growth in various fields like Transportation, Education, Agriculture, Health care and particularly within the building management application sector. However, the growing use of IoT services, especially in office organization applications will increase security challenges, like authentication of several connected objects and exchanged data. Thanks to the sensitivity of office applications, the aspect of authenticity is one among the foremost significant challenge, which should be addressed effectively. Therefore, E-office applications require an authentication scheme to guard data transfer, use and exchange between sensor nodes and Base Station. E-office applications are susceptible to several hacks, and this is often thanks to all communication occurred through a wireless medium. So, one of the most goals of building security protocols are to reinforce using of the network, which allows node sensors to avoid wasting lots of energy and cause extend the network's lifetime and to be resistant against several kinds of attacks. At this research, we are proposing an efficient secured group-based lightweight authentication scheme for IoT based E-office applications, this scheme authenticates and establishes secure channels through sensor nodes and Base Station. The proposed scheme with a feature of the group-based node will reduce distance and consumed energy, also as leads to reduce communication cost. additionally, it'll be resistant against hacks by using elliptic curve cryptography(ECC).

***Index Terms* - E-office applications; Authentication; Lightweight; Group-based node; Energy; ECC.**

I. INTRODUCTION

With the IoT, nowadays it is considered as one of the newest, fastest and reliable spreading mechanisms in the wireless network communication. IoT is built on the devices of integrating sensors at daily smart objects that linked to the Internet through wireless sensor networks that lead to evolution of new methods for exchanging the data which were not potential before. IoT has several applications and one of the most effective is E-office applications, e-office applications are radio-frequency that based on wireless networking technology and consist of wearable sensors which connected to Base Station [1]. Currently, a great number of researches are learning IoT applications at e- office field. E-office term had been recently established which handles management of organization with the backing this will provide many advantages like cost saving, identification of person in a premise, and authentication of the person in organization. Therefore, this will lead to achieve the goal of facilitating secure interactions among people and management, which leads to better quality of behavior, and save the time of in person [2].

E-office applications are an exhibition to hack data and increasing issues at issues in security aspects due to rising a number of access points and critical data through online records as well as the growing of use wearable technology[3]. So, one of the main issues of IoT is the high level of security that needed to keep all communications secured. The concerns of security are extended due to the rapid deployment of IoT [4]. At IoT, Security is mainly part of E-office applications, which provide a high level of security for log data [5]. There is a need for more efforts and more researches to handle security problem. However, many of researchers had searched about an open issue at IoT [6].

Researches aim to meet the requirements for making security a major factor to build IoT E-office applications to protect data communication mechanisms [7]. Based on the above brief discussion, our paper is proposing an efficient secured group-based lightweight authentication scheme for IoT based E-office applications. The proposed scheme will be resistant against several types of hacks. Also, with a feature of the group-based node will reduce distance and energy and as well as lead to reduce communication cost. At the beginning, we discuss briefly IoT security challenges, especially at E-office applications. The rest of the paper ordered in four parts. In section II, we present Literature review. In section III, we proposed our scheme and explained it in detail. In section IV, we discussed and presented results analysis. Finally, Section VI, we end with the main contributes to this paper.

II. LITERATURE REVIEW

This section will briefly discuss the literature review mainly in the authentication and security area for IoT E- office based applications. After that, I will list a summary of comparisons of related studies. In a study [2], the effects of IoT in establishing of E-office successfully and indicating, the barriers that will contribute to reducing the chance of successful deployment of IoT-based e-office applications have been analyzed. Considering the adoption of Big data, cloud computing and implementation of IOT that may improve the industry in several benefits: help the people by reducing cost and need of visiting the physically, travelling cost, human resources and finally time which will contribute directly to improve the quality of communication. Barriers that should be focused on in order to have successful adoption of IoT base E-office are security, privacy as they will become big vulnerable especially in open networks. A study [3], they discussed the recent topics and issues related to the E- office applications, and how developers and programmers deal with them. These security issues came from wide use and rapidly evolve of IoT e-office systems. After that, they specify the causes and what is the proper solutions to minimize them. Later, they will discuss what may occur in future regarding security and privacy issues and how to handle them. Finally, they list some other issues such as Smart office and cities, Cloud computing, Biometrics, and social networks. They noted that these mentioned problems are out of their study limits and will consider them in the future. A study [8], they offer a technique that it's good to use in connected office environment due to their need to less power, this technique is Narrowband IoT (NBIoT). In addition, they consider it good for E-office system because it's unified. The big challenge of this technique is security. In addition, there is another issue, which is absent; offering service at the needed time. Therefore, this may prevent using it at E- office applications. Because of above the reason, they offer a solution by using Constrained Application Protocol (CoAP) and IPv6 through 6LoWPAN. A study [9], they offer secured model, that help to minimize problems related to security and how we take advantages from wearables. They also offer various areas of mechanisms of architectures of IoT e-office and how it assists to provide easy access and sending and receiving e-office data. In addition, they present precise search regarding how e-office applications of IoT deal with several patient's services. A study [10], they searched and studied IoT nodes and offer virtual network cloud system security framework. one of the main defects of cloud networks of IoT are the issues of nodes usage over virtual network cloud system. These nodes can be connected but they need surveillance from a Cloud Service Provider (CSP). CSP need to take attention from malicious node because of they not able to be disconnected from the network. They offer protocol with secured key management for clients and CSP. After that, they established a technique for lightly weighted cryptography which offers a protocol for key exchange and able to build a secured connection for nodes. They used Diffie-Hellman algorithm because it offers variety benefits such as less power consumption, robust and lightweight. The authors in [11], search about the major problems that occurred at the usage of IoT applications. They discussed how to offer the best solution for surveillance of nodes. This project collects data from multiple sensors, this leads to offer needed safety for IoT application. But there are still some issues need to be fixed at this project, such as non-attendance of infrastructure authentication of transmitting data. At this paper [1], they provide a scheme for an secure authentication application which is light weighted and authenticated. It will be led to protect data information by applying an authentication feature for Base Station and Sensors. To achieve authentication exchanges integrity; they depend on nonces and Keyed-Hash message authentication (HMAC) at their scheme. Based on the results of their scheme; it shows that its maintained energy pulses its resistance against several attacks. At future, their goal is to evaluate their protocol in the realistic case to get more results about consumption of memory and time execution. This paper [12], presented mechanisms for encrypting, sign and authenticate communications of sensor devices which are: a collection of cryptographic Subscriber Identity Module (SIM) card. The goal of this study is to handle the problems that present at IoT, which lead to robust, fixed and secured technology to make IoT be realistic at provider environments. So, they offer RFID/NFC and they consist of cryptographic SIM card to improve safeness, and they developed a protocol to mobility for 6LoWPAN. Thus, they focus on some of the schemes to handle issues that face IoT at healthcare areas. At future, they are planning to introduce specific algorithms to know more about characters of architecture that established chronobiology algorithms and health science. In this paper [13], they discussed various issues that related to IoT applications, such as remote surveillance of elderly pulse privacy and security. All of them connected to e- application information records. Therefore, they introduced and developed an approach of rating of consuming energy that used the process of Holt-Winters by guessing. This will be beneficial if they want to know the more secured lightweight solution of ASSET project. In future, they will evaluate security algorithm consuming of energy performance and communication prices by using their testbed. This paper [15], focuses on IoT quick and light weight authentication which covers specifically the level of security and searches their advantages of network and protocols. UT-GATE interest in security level, precisely at the establishment of the architecture of gateway and network. A project of Fault Tolerance focuses deeply on the architecture of the network, real-time and skilful system. In addition, there are extra efforts of studies that work over current security protocols. In their future work, they plan to add more solutions for IoT E-application techniques.

At this study [16], to block facing issues at distributed IoT applications, they present framework secured, which applies secured adaptive contexts to help with the right monitor information. This will be led to follow data and meet responsibility; also, it involves taking legal responsibility. The main idea to have the privacy of E data is to execute a secured context linked with each resource. Therefore, at any establishment of data; the secured context needs to be automatically generated.

At this study [17], they are prepared to select solve AKA which is good for IoT environment, and this can apply by test schemes free-escrow lightweight that provide benefits for performance and safety plus consumption of power. In addition, they confirm and offer a collection of certificates implicit plus strengthened-Menezes-Qu- Vanstone (SMQV) which result in lightweight and secret protocols. As they said, if you want longer network life; design secured schemes of WSN for a network using improvement and handling and protect energy. In fact, even when they said that schemes of AKA more effective than SMQV, but later it presented some security errors. Therefore, it's not easy to add ant refinements to SMQV. In this paper [18], there are some protocols as if Transport Datagram Layer Security (DTLS) premise on some ethics of internet field that used and proposed at this paper, which is the execution of whole scheme of implementation of two-way secured authentication for IoT. They used DTLS handclasp authentication that based on RSA keys to implementing the verification. They offer an algorithm that always used public key cryptography, which relies on RSA, and module of security depends on it. They found that it can be applied through broad at the platform of hardware which is appropriate with IoT, so they discover that after applying it over DTLS. This wide support is relying on systems of the internet of things. Therefore, their proposed scheme supply privacy and authenticity, integrity of SMS plus end 1. 2 end latencies, memory prices and minimum power. Finally, they conclude that the best solution for safety to evolve IoT is the usage of DTLS. A paper [4], they proposed a method of encryption depend on XOR manipulation, instead of using the hash function because it's complex encryption, using this will lead to prevent counterfeiting and protect privacy. The absence of cryptography in RFID is the main challenge in designing security. When RFID connect to the internet, the items of tags will move through many readers fields after that, linked to RFID communication protocol. Therefore, due to RFID not having anti-counterfeiting features, hackers can scan EPC from the tag. Therefore, their proposed lightweight cryptography protocol can solve this issue and their simulation results show that they can improve it, also this protocol can be used to build procedure to mutual authentication of RFID for IoT applications. At this paper [19], they proposed energy-efficient, lightweight and robust security protocol for Wireless Sensor Networks (WSN) systems. As we know, at WSN if there is any new device will link to the network, initially, it needs to ensure mutual authentication step. After that, establishing a secured and protected channel to protect transmitted data. Therefore, at their work, they implemented the secured protocol with lightweight and energy efficiency features, which lead to protect most WSNs. In addition, it will guarantee mutual authentication of communication objects and secured privacy and secrecy of transmitted data. The technique of personalization will fix the issue of internal identity usurpation. This protocol offers lightweight and robust security encryption symmetric algorithm (CCM/AES GCM) and this leads to a very rapid build of a secure channel. In the end, this protocol is resistant to replay attacks and cryptanalysis. At this paper [20], they suggested secure authentication and key management protocol, with the usage of hybrid cryptography which includes certificate-less and symmetric cryptographic public key algorithms.
Their performance comparison results and evaluation present that they are able to meet the requirements of security at IoT e-office sector. We know, one of the main challenges at the environment of networking IoT is constrained resources. Based on that, they suggested mutual authentication protocol build key through sensor node resource constrained at IoT e-office areas and entity of remote users that linked to IoT over the internet. This protocol usage Key Generation Center (KGC) that it's not necessary to be completely trusted. Their protocol is lightweight which has low computational cost and low overhead message. Based on their mathematical analysis; their protocol shows that it's secured and protected against various attacks in IoT.
.

III. PROPOSED SYSTEM

This section provides a detailed description of the proposed scheme, which is consisted of sensor nodes that distributed around the organisation of the proposed system and single group node linked to Base Station (BS) then server finally to a monitor room or reception centre, ex: E-office applications.

The problem for the clients or customers communicating with the company respective heads finds a difficulty. Since, their might be different kinds of issues like change over in the position heads, department position change in the organisation, representative presence or absence in the chamber and mainly monetarisation of a respective person in the organisation.

A. A structure of typical organisation

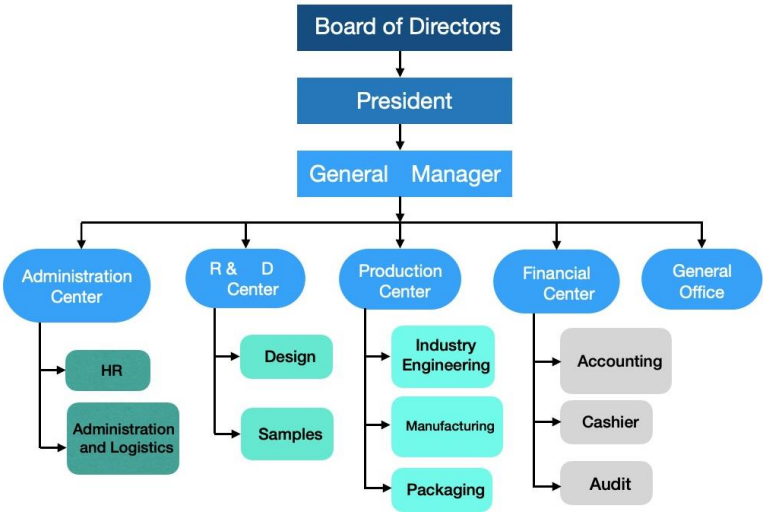

Figure -1: A sample company infrastructure

A well grown company infrastructure will be having many sub sections in their organization. Our proposing system is having a basic infrastructure, which follows the private limited structure, defining from Board of directors, president, general managers and sub sections like Administration center, Research and development center, production center, financial center, general office and respective sub sections like HR department, Administration and logistics, design team, a block of sample holding team, industry engineering team, manufacturing team, packaging team, financial management teams like accounting, cashier and audit teams. General office like reception, foreman, security and building infrastructure management team.

B. Lightweight scheme flow diagram/sequence diagram

The below flow chart and sequence diagram as shown in Figure. 2 and Figure. 3 explains the whole workflow of our proposed secured authenticated lightweight scheme, it will start at the side of the sections and if sensors nodes able to communicate with a group node and receive authentication scheme or not. After that node, registration phase will be initiated over group node with Base Station to establish a secure channel. Then, as we mentioned before group node will gather data from sensors nodes to Base Station, then forward them to the server and finally to a monitoring person or receptionist of the organization to inform the client or customers. The presence of group node at out proposed scheme and handle the process of registration phase and it will decrease channel distance of sensors nodes and lead to reduce consumed energy, secured communication. In addition, enhanced efficiency of scheme (it explains in detail at below section).

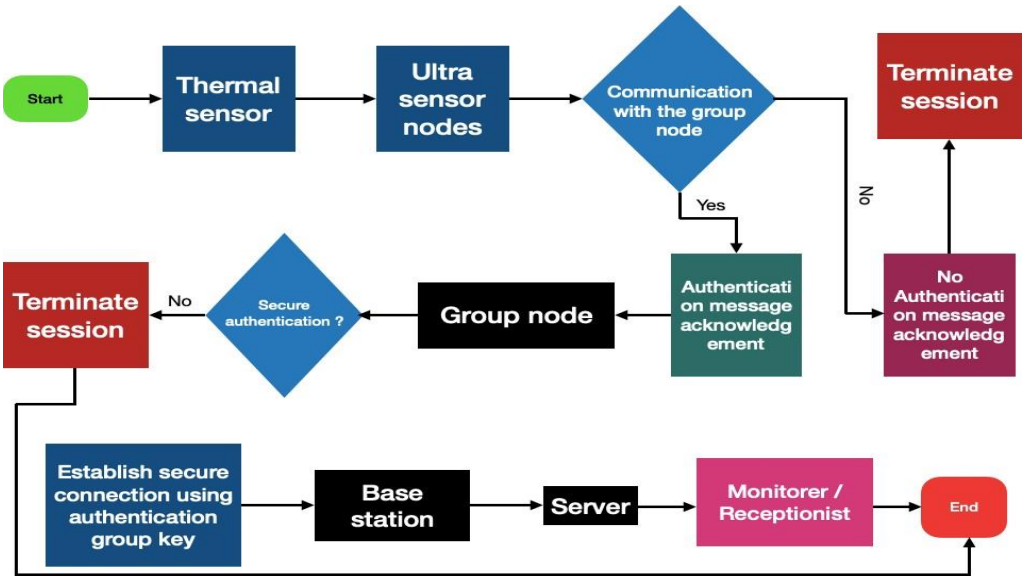

Figure -2: Flow chart

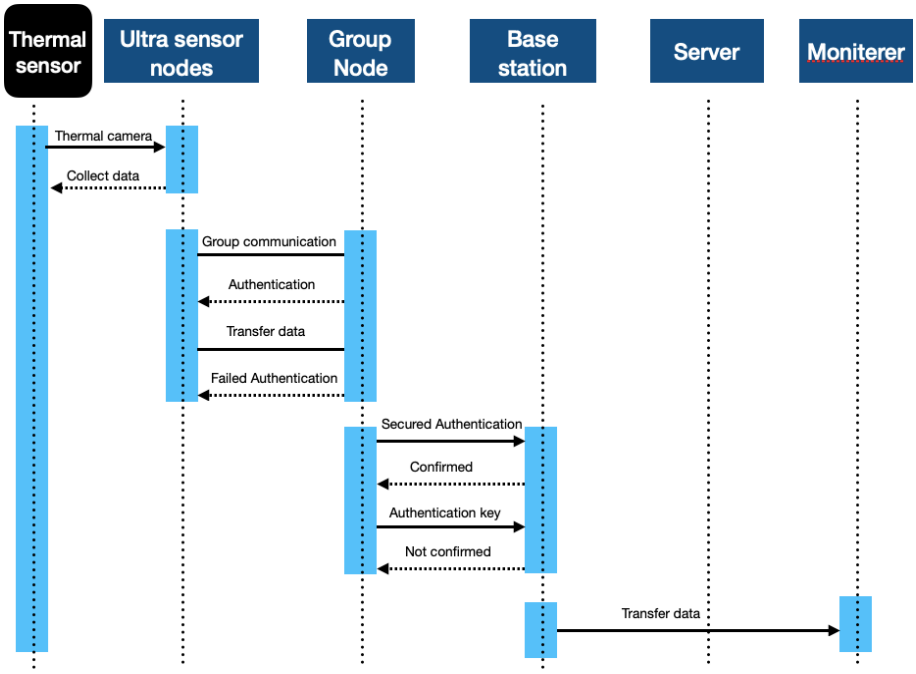

Figure -3: Method of achieving the process / sequence diagram

IV. IMPLEMENTATION

C. Lightweight scheme scenarios

At first, we will discuss the scenario if there is no application of group node, if sensor nodes directly forward all data to Base Station then to the server. This will produce several channels because each node will establish its own connection to the base station and they will be prone to attacks and security will be reduced. In addition, due to far distance between sensor nodes and the base station, this will lead to consume more energy and reduce the lifetime of nodes. In addition, the process of key authentication will increase, because if we have eight sensors nodes; they will authenticate eight times to get key from the server, so it will be costly. In our proposed scheme, we are trying to address this issue by applying group node as interface in- between sensor nodes (ultra-sensors) and the base station. These sensor nodes send collected data to group node then group node forwards all data to Base Station then to the server. This will reduce the distance that established between sensor nodes and group node. Therefore, this will reduce energy consumption and increase the lifetime of nodes. On another hand, it will increase security because there are no long distances and will reduce the probability to attack. In addition, it will reduce the key authentication process, because just group node that will authenticate one time to get key from the server, so it will save costs. In this part, we will present a comparison between the two scenarios of our scheme, which will both of them apply and run through simulator. The achievement of this work undergone a process of simulation and practical approach using a Docker software for running the application locally.

V. RESULT ANALYSIS

The possible enquiries are done in the below possible method.
Consideration of number of blocks or section in organization is defined below.

1. Ultra-sensor node communication with Group node
2. Group node communication Base station
3. Base station communication with server
4. Moniterer/ Front end communication

VI. CONCLUSION

The proposed e-office applications with an authentication scheme to guard data transfer, use and exchange between sensor nodes and Base Station an efficient secured group-based lightweight applications, this scheme authenticates and establishes secure channels through sensor nodes and Base Station. The proposed scheme with a feature of the group-based node will reduce distance and consumed energy, also as leads to reduce communication cost. additionally, it'll be resistant against hacks by using elliptic curve cryptography (ECC). system is having a basic infrastructure, which follows the private limited structure, defining from Board of directors, president, general managers and sub sections like Administration center, Research and development center, production center, financial center, general office and respective sub sections like HR department, Administration and logistics, design team, a block of sample holding team, industry engineering team, manufacturing team, packaging team, financial management teams like accounting, cashier and audit teams. General office like reception, foreman, security and building infrastructure management team.

In proposed scheme, we are trying to address issues by applying group node as interface in- between sensor nodes (ultra-sensors) and the base station. These sensor nodes send collected data to group node then group node forwards all data to Base Station then to the server. This will reduce the distance that established between sensor nodes and group node. Therefore, this will reduce energy consumption and increase the lifetime of nodes.

VII. REFERENCES

1. *Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," Journal of Network and Computer Applications, vol. 42, pp. 120–134, 2014*
2. *J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues, "IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015.*
3. *S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E. J. Yoon, and K. Y. Yoo, "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications," IEEE Access, vol. 5, pp. 3028–3043, 2017.*
4. *F. Wu, L. Xu, S. Kumari, and X. Li, "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security," Journal of Ambient Intelligence and Humanized Computing, vol. 8, no. 1, pp. 101–116, 2017.*
5. *D. Wang, D. He, P. Wang, and C. H. Chu, "Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 4, pp. 428–442, 2015*
6. *X. Xu, P. Zhu, Q. Wen, Z. Jin, H. Zhang, and L. He, "A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems," Journal of Medical Systems, vol. 38, no. 1, pp. 1–7, 2014.*
7. *M. N. Aman, K. C. Chua and B. Sikdar, "A Light-Weight Mutual Authentication Protocol for IoT Systems," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, 2017, pp. 1-6, doi: 10.1109/GLOCOM.2017.8253991.*
8. *Gope, P., et al.: Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. In: Sloot, P., Cambria, E., Abramson, D., Altintas, I. (eds.) Future Generation Computer Systems, vol. 83, pp. 629–637. Elsevier, Amsterdam (2018)*
9. *Aman, M., Chua, K., Sikdarb, B.: A lightweight mutual authentication protocol for IoT systems. In: Proceeding of IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE (2017)*
10. *Wallrabenstein, J.: Practical and secure IoT device authentication using physical un- clonable functions. In: IEEE Proceeding of International Conference on Future Internet of Things and Cloud (FiCloud), pp. 99–106. IEEE (2016)*
11. *Liu, M., et al.: TBAS: enhancing wi-fi authentication by actively eliciting channel state information. In: IEEE International Conference on Sensing, Communication, and Networking (SECON), pp. 1–9 (2016)*
12. *Wang, W., et al.: Privacy-preserving location authentication in Wi-Fi networks using fine-grained physical layer signatures. IEEE Trans. Wirel. Commun 15(2), 1218–1225 (2016)*
13. *Van den Abeele, F., et al.: Scalability analysis of large-scale LoRaWAN networks in ns- 3. IEEE Internet Things J. 4(6), 2186–2198 (2017)*
14. *Odelu, V., Das, A., Goswami, A.: SEAP: secure and efficient authentication protocol for NFC applications using pseudonyms. IEEE Trans. Consum. Electron. 62(1), 30–38 (2016)*
15. *Lee, J., Lin, W., & Huang, Y. (2014). A lightweight authentication protocol for Internet of Things. 2014 International Symposium on Next-Generation Electronics (ISNE). doi:10.1109/isne.2014.6839375*
16. *Hossain, Md. Mahmud, et al. "Towards an Analysis of Security Issues, Challenges, and Open Problems in the IoT." 2015 IEEE World Congress on Services, 2015, doi:10.1109/services.2015.12 3*

17. *Williams, Patricia A H, and Vincent Mccauley. "Always connected: The security challenges of the healthcare IoT." 2016 IEEE 3rd World Forum on IoT (WF-IoT), 2016, doi:10.1109/wf-iot.2016.7845455 2*
18. *Anand, Sharath, and Sudhir K. Routray. "Issues and challenges in healthcare narrowband IoT." 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT), 2017, doi:10.1109/icicct.2017.7975247.*
19. *Chatterjee, S., et al.: Secure biometric-based authentication scheme using chebyshev chaotic map for multi-server environment. IEEE Trans. Dependable Secure*

    Comput. 15(5), 824–839 (2018)
20. *Odelu, V., Das, A., Goswami, A.: SEAP: secure and efficient authentication protocol for NFC applications using pseudonyms. IEEE Trans. Consum. Electron. 62(1), 30–38 (2016)*
21. *Amin, R., et al.: A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment. In: Sloot, P., Cambria, E., Abramson, D., Altintas, I. (eds.) Future Generation Computer Systems, vol. 78, pp. 1005–1019. Elsevier, Amsterdam (2018)*
22. *N. Nasser, L. Karim, A. Ali, M. Anan and N. Khelifi, "Routing in the Internet of Things," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, 2017, pp. 1-6, doi: 10.1109/GLOCOM.2017.8253955.*
23. *Kumbhar AD, Chavan MK (2017) An energy efficient ring routing protocol for wireless sensor network. In: 2017 international conference on I-SMAC (IoT in social, mobile, analytics and cloud) (I-SMAC)*
24. *Chhabra A, Vashishth V, Khanna A, Sharma DK, Singh J (2018) An energy efficient routing protocol for wireless internet-of-things sensor networks. In: Networking and internet architecture (cs.NI); Signal Processing (eess.SP), Cite as: arXiv:1808.01039 [cs.NI]*
25. *Roy, Sandip & Chatterjee, Santanu & Das, Ashok Kumar & Chattopadhyay, Samiran &Kumar, Neeraj & Vasilakos, Athanasios. (2017). On the Design of Provably Secure Lightweight Remote User Authentication Scheme for Mobile Cloud Computing Services. IEEE Access. PP. 1-1. 10.1109/ACCESS.2017.2764913.*