IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secure Communication Using Mutual Authentication Light IOT: A Case Study

1TEJAS D P, 2TEJVIN VISHAL EDA, 3VARUN G M, 4YATHIN G N, 5UMESH M
1Student, 2Student, 3Student, 4Student, 5Assistant Professor
1Visvesvaraya Technological University,
2Visvesvaraya Technological University,
3Visvesvaraya Technological University,
4Visvesvaraya Technological University,
5Visvesvaraya Technological University

1.Abstract: It is believed that the Internet of Things (IoT) greatly helps the field of health informatics. For in-hospital and at-home patient monitoring, biological data such as blood pressure, electrocardiography (ECG), blood sugar levels, body temperature, etc. are collected and transmitted by IoT-enabled devices. Among these devices with numerous healthcare applications are wearables. These devices generate data continually, which they forward for processing and visualisation to remote servers and adjacent gateways. These devices are vulnerable to many hostile threats, thus it is important to safeguard the confidentiality and integrity of the data they communicate. A Light IoT, a small and safe communication solution, is recommended for data sharing across the healthcare infrastructure's equipment.

1. Introduction:

The term "Internet of Things" (IoT) was coined in 1999 by the originator of the RFID research group, and it has recently become more well-known in the real world as a result of the growth of mobile devices and integrated, pervasive connectivity. Imagine a world where billions of objects, each capable of sensing, communicating, and exchanging data, are linked by IP networks that are either privately or publically owned. The most popular definition of the Internet of Things (IoT) is a network of physical items. These days, everything is online, including automobiles, cellphones, household appliances, cameras, medical devices, and industrial systems, many kinds of wildlife, people, buildings.

The Internet of Things (IoT) is a concept and methodology that considers the pervasiveness of different types of objects in the environment that are able to cooperate and communicate with one another through other entities in order to develop new applications and accomplish common objectives through cabled and wireless connections as well as unique addressing schemes.

In this regard, developing a smart environment presents significant R&D obstacles. A time when the combined forces of the physical, digital, and virtual realms create intelligent environments that increase the processing capacity of cities, transportation, energy, and numerous other industries.

1.1 Objectives:

Mutual authentication plays a major role in strengthening the secure communication paradigm in the context of the Internet of Things. This strategy aims to accomplish a two-pronged authentication procedure, guaranteeing the authenticity of both communication parties prior to the transmission of private data. In the context of the Internet of Things, there are numerous main goals for integrating mutual authentication and safe communication. In order to reduce the dangers associated with unauthorised access, device authentication is crucial in confirming the authorization and legitimacy of the device within the network.

The comprehensive security architecture includes effective key management, robustness against replay attacks, and compliance with privacy requirements. Maintaining the integrity and confidentiality of transmitted data while ensuring efficient performance requires finding a balance between security protocols and IoT device resource limitations.

2. Related Work:

Research and development efforts in the Internet of Things have focused on mutual authentication as a means of assuring secure communication. The opportunities and difficulties of putting strong security measures in place that are suited to the particulars of IoT contexts have been covered in a wide range of research and publications. Numerous scholars have investigated authentication protocols created especially for Internet of Things devices with limited resources. By mutually authenticating and confirming the identities of both communication entities, the goal is to build trust between devices. Numerous key management techniques and cryptographic protocols have been investigated to improve the security of Internet of Things communication channels.

The development of efficient and lightweight encryption techniques has been another main objective. It is crucial to maintain data secrecy while reducing the burden on the constrained computing power of IoT devices. Researchers have looked at methods that Additionally, efforts have been made to overcome the particular difficulties brought on by the heterogeneity of IoT devices. Security solutions must be flexible and scalable due to the wide range of device types, communication protocols, and application domains available. Scholars have put forth frameworks that are able to meet the diverse needs of various Internet of Things implementations while guaranteeing a mutual authentication. approach that is consistent and platform-neutral. Studies also emphasise how critical it is to defend against new dangers in the Internet of Things environment, such as sophisticated assaults that aim to compromise the authentication procedure. Researchers stress that in order to keep ahead of emerging dangers, security procedures must be continuously evaluated and improved as IoT networks grow.

3.1 Services

(1) Transport Layer Security (TLS)/Secure Sockets Layer (SSL):

Use TLS/SSL protocols to ensure secure connection between servers and Internet of Things devices. These protocols offer reciprocal authentication, data integrity, and encryption.

(2) Public Key Infrastructure (PKI):

Create a PKI to handle public-private key pairs and digital certificates. IoT device secure identification and authentication are made possible by this architecture.

(3) Device Authentication Services:

To confirm an IoT device's identification, use device authentication services. This may entail utilising API keys, secure tokens, or other methods of authentication.

(4) Secure Boot and Firmware Updates:

Secure boot procedures should be used to guarantee that only approved firmware is run. Establish safe procedures for firmware updates to address vulnerabilities as well.

(5) Role-Based Access Control (RBAC):

Implement RBAC to control permissions and access for various IoT devices. This guarantees that every device has the rights required for the functions for which it is designed.

(6) Secure Element Integration:

To offer a secure execution environment for cryptographic operations, key storage, and secure bootstrapping, think about integrating secure elements in Internet of Things devices.

The various use cases of Secure Communication are listed below –

(1) To safeguard sensitive user data, including account and transaction information, secure communication is essential for online banking and financial activities.

(2) For e-commerce platforms to protect consumer data, including credit card numbers and personal information during online transactions, secure communication is

essential.

(3) Secure communication is essential in the healthcare industry for the exchange of sensitive health information, medical histories, and patient data between insurance companies, laboratories, and healthcare practitioners.

(4) Secure communication is essential in the healthcare industry for the exchange of sensitive health information, medical histories, and patient data between insurance companies, laboratories, and healthcare practitioners.

(5) To prevent unwanted access, guarantee user privacy, and guard against cyberattacks that target linked devices, secure communication is crucial for smart home appliances and Internet of Things ecosystems.

Conclusion:

Biological insights in IoT-enabled medical IT are the main emphasis of Light IoT, a portable and highly secure method of environmentally friendly communications. for wearable technology that uses less power. With a mobile gateway and a remote server, simple registration and authentication procedures may be started more easily thanks to Light IoT's three steps. The three stages of Light IoT operation are pairing, authentication, and initialization. Through the establishment of secure sessions between the connecting entities, these acts guarantee the reliability of the data transmission. Using a MAC 802.11g communication radio optimises the device's power usage and speeds up data transmission. Optimising the energy requirements of wireless transmission can lead to longer battery life for nodes. Light IoT uses lightweight hash functions and XOR operations to complete these steps, which makes it incredibly successful at delivering time-sensitive and delay-sensitive data instantaneously.

References

[1] R. Amin and G. Biswas, “A secure lightweight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks,” Ad Hoc Netw., vol. 36, pp. 58–80, Jan. 2016.

[2] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K. R. Choo, “Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks,” Comput. Netw., vol. 129, pp. 429–443, Dec. 2017.

[3] M. A. Jan, M. Usman, X. He, and A. U. Rehman, “SAMS: A seamless and authorized multimedia streaming framework for WMSN-based IoMT,” IEEE Internet Things J., vol. 6, no.2, pp. 1576–1583, Apr. 2019.

[4] P. Gope and T. Hwang, “A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks,” IEEE Trans. Ind. Electron., vol. 63, no. 11, pp. 7124–7132, Nov. 2016.

[5] K. H. Wong, Y. Zheng, J. Cao, and S. Wang, “A dynamic user authentication scheme for wireless sensor networks,” in Proc. IEEE Int. Conf. Sensor Netw. Ubiquitous Trustworthy Comput. (SUTC), vol. 1, 2006, pp. 244–251.

[6] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, “Certificateless remote anonymous authentication schemes for wireless body area networks,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 332–342, Feb. 2014.

[7] A. K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, and X. Huang, “Provably secure user authentication and key agreement scheme for wireless sensor networks,” Secur. Commun. Netw., vol. 9, no. 16, pp. 3670–3687, 2016.

[8] F. P. Diez, D. S. Touceda, J. M. S. Camara, and S. Zeadally, “Toward self-authenticable wearable devices,” IEEE Wireless Commun., vol. 22, no. 1, pp. 36–43, Feb. 2015.

[9] J. He, Z. Yang, J. Zhang, W. Liu, and C. Liu, “On the security of a provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 14, no. 1, pp. 1–11, 2018.

[10] S. F. Aghili, H. Mala, P. Kaliyar, and M. Conti, "Seclap: Secure and lightweight RFID authentication protocol for medical IoT," Future Generation Computer Systems, vol. 101, pp. 621–634, 2019.

[11] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust based provable secure authentication protocol with privacy preservation for industrial Internet of things," IEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3599–3609, 2018.

[12] M. A. Jan, F. Khan, R. Khan, S. Mastorakis, V. G. Menon, P. Watters, and M. Alazab, "A lightweight mutual authentication and privacy preservation scheme for intelligent wearable devices in industrial-cps," IEEE Transactions on Industrial Informatics, 20