International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

INTERNET OF THINGS IN HEALTHCARE

Rajeev, Ravi

Department of Computer Application

Chandigarh School of Business

Chandigarh Group of Colleges, Jhanjeri,Mohali,India

rs.rajeevsingh786@gmail.com, ravi.j2659@cgc.ac.in

Abstract

One particularly potent area where gadgets and embedded sensors can exchange data and communicate over the Internet is the Internet of Things. One of the most crucial methods for guaranteeing data privacy and security is authentication. Because internet of things devices and data might be extremely significant, security barriers are required to keep internet of things data safe from hackers.

Devices that need certain authentication processes without requiring a lot of processing power are included in the category of internet of things devices. In addition to reviewing IoT applications in the healthcare industry, this study suggests a novel authentication method for IoT communication. There is a suggested structure for trustworthy and secure medical care. The suggested authentication technique offers a very secure and effective authentication mechanism.

I. INTRODUCTION

One of the most common study areas is the Internet of Factors (or Internet of Things). The Internet of Things is developing thanks to developments in electronics, IPv6, and wireless network adoption. As Internet of things devices and technology continue to advance rapidly [1]. The internet of things is now widely employed in unique settings like homes, hospitals, airplanes, and many forms of transportation. One of the main concerns of researchers is controlling systems and the Internet of things combination. Different strategies for regulating Internet of things devices have been put forth. Security for the Internet of Things is the top priority problem and is now the primary focus of research on the topic [2].

For network devices, protecting information is a critical concern. In the realm of Internet of Things applications, security plays a crucial role since malevolent attacks or disruptions to IoT devices pose a threat to human life. Authentication is a key component of the Internet of Things data safety solution. Identity verification is required in order to comply with commands from the manage device. Various studies have been suggested to offer authentication methods for both traditional networks and the Internet of things. These processes are not made to fully meet the demands of the Internet of Things ecosystem and devices, which have limited electrical, memory, and computing capacity. The Internet of things management device has specifications of its own[3].

The end devices that may be used to control Internet of Things devices generally possess superior storage, memory, processing, and strength capabilities compared to standard Internet of Things devices. These capabilities allow the end devices that control Internet of Things gadgets to have novel capabilities for controlling Internet of Things devices. In order to create an authentication method that is acceptable, secure, and suitable for the Internet of things, researchers working on identification want to combine the characteristics of end devices and strike an appropriate equilibrium between the sources that are available.

II. Literature Reviews on Internet of things

Developing novel authentication mechanisms and endorsing an authentication that works with a variety of Internet of things devices are two of the most difficult challenges facing the researchers. Authentication techniques for cellphones are also being used to watches, thermostats, and a wide range of sensing and semiconductors [9, 10]. Both physical security and authentication based mostly on cryptography are significant types of device identification security solutions that have been put forth. Physical protection techniques use physical concepts to prevent devices from breaking or being attacked within the physical layer [11, 12].

On the other hand, the Internet of Things' radio frequency identity devices (RFID) tools identifying safety area is the foundation for the cryptography-based authentication technique. Due of its excellent security features, numerous algorithms based solely on Iot of Things RFID have recently been developed [13]. Devices connected to the internet that have limited resources are known as internet of things devices. These expose those devices to a wide range of threats and render them vulnerable. To ensure security and recognize identities in order to thwart attackers and malicious attacks, authentication is required [14]. Conventional network authentication methods and approaches need a lot of processing resources [15]. The Internet of Things is viewed as a limited resource environment with constrained processing and power sources.

It takes a light authentication method with strong security features to maintain processing power and shape. Therefore, in this thesis, we will suggest a strong and lightweight authentication method to meet the requirements of an Internet of things environment and offer a reliable protection function to keep your privacy safe and prevent harmful attacks.

Novel strategies have been employed in the most recent authentication proposals to enable secure communication [18]. Techniques that rely on the HTTP protocol stack for authentication conversations suffer from significant overhead as a result of the protocol's inefficiency in resource-constrained Internet of things environments. Alternative approaches encrypt conversations using AES [19].
In order to meet the demands of the Internet of Things with limited power resources, AES uses extensive encryption keys and complex calculations, which led to high power consumption [20]. A better approach of reciprocal authentication has been presented in [21] for environments using Internet of things. For the challenged answer on RFID authentication protocol in the distributed database environment, they suggested various enhancements to the authentication algorithm [22]. It was improved to better manage system environments for the Internet of things. Their methodology consists of three key components: first, upload an extra device to every terminal that that is used for control; second, upload monitor device to ensure that terminal devices are compliant and shown; and third, upload a push-in alarm mechanism to sound an alert in the event that an authentication system fails. Throughout [23]in decentralized Internet of things applications, a two-section authentication protocol has been suggested for wireless sensor networks. This protocol is based on certificates and uses two-segment authentication to enable safe data transfer and authentication between Iot of Things gadgets and manipulating stations. A reliable connection is established. In order to address the scalability and heterogeneity of the community, they employed a protocol that provides sensor node assistance. In the past, certificates were issued by certificate authority (CA). Once they have their own certificates, established nodes are free to move around and change regions. Connecting with various community entities, CA can verify the authenticity of the sensors.

To establish a connection, network contributors first establish a connection with the CA in order to authenticate the identification of the vacation site. This strategy is based on many lower layer safety features and is regarded as a give up to cease utility layer authentication method. A safe authentication system for cloud servers and the Internet of things was suggested in [24]. It primarily relies on algorithms based on elliptic curve encryption (ECC), which offers superior security results when compared to other publicly accessible cryptography (PKC) methods [25] due to its short key length. When used with embedded devices that use the HTTP protocol, this authentication protocol leverages EEC. Authenticating smart devices with HTTP cookies is a novel approach.

TCP/IP configuration is what these devices desire. The HTTP cookies that have been implemented to fit into devices with limited surroundings and managed by cloud servers are used in the design of the proposed authentication protocol. Three main steps make up the suggested protocol. Phases of registration, authentication, and pre-computed sections are followed. In the registration phase, the embedded devices register with the cloud server, and it then stores a cookie on the embedded devices. The devices want to issue a login request during the Pre-computation and Registration Phase before communicating to the server [26]. In the authentication segment, all embedded tools and cloud servers work together to authenticate each individual user's use of the EEC set of rules.

Even if the EEC set of regulations uses a modest encryption key, the encrypted message is much larger. In addition to being more complex and challenging to construct than other cryptographic algorithms, the ECC algorithm requires more computer power.

A suggested Group Authentication (TCGA) mechanism for the Internet of things is based mostly on threshold cryptography. This version, which is entirely based on the organization communication paradigm, provides legitimacy for every Internet of Things devices. TCGA is intended to be used in Wi-Fi environments. For each group authentication, it generates a secret channel or consultation key; it can also be applied to group software. To prevent organizational key leakage, every group has a team leader who is in charge of keeping track of keys and distributing new ones whenever a new member is added. This person is known as the group authority. The five main modules of the proposed algorithm are message decryption, authentication listener, organization credit era, key distribution, and key replace.

SEA [28] has the potential to be a safe and effective architecture for smart gateway-based authentication and authorization in internet-based healthcare. This particular structure is reliant on a fully DTLS handshake protocol that is certificate-based. The following are the main components of this structure: the clinical sensor community, which collects data from patients' bodies or rooms to support the clinical prognosis and treatment plan. The Smart e-Health Gateway, which facilitates device-to-device connection and serves as a conduit for MSN and the internet, is the second feature. The back-end system, or 0.33 element, obtains, stores, and processes accumulated records prior to participating in the community, an efficient shared authentication model has been developed in [29]. This schema verifies the identity of Internet of things devices that are present in the surroundings. They suggested lessening the overhead of communication. The protocol that provides communication between Internet of Things devices has been chosen as the lower layer, Constrained Application Protocol (CoAP). The Advanced Encryption Standard (128-bit) is used to complete the authentication process (AES). Initial diagnosis is done by identifying the clients and server. Following that, it gives clients unique assets mostly according to the particular circumstances specified in the request.

By minimizing the large range of transmitted packets, conditionally precise facts transmission reduces computation and energy usage. The communication's bandwidth usage is also decreased. Presented a novel CoAP option in [30]. Information from devices, including as metadata and sensor measurements, can be retrieved over the software-layer Constrained Application Protocol (CoAP). These data are utilized by a number of real-time applications. Yet, there are instances where retrieving unprocessed verbal interaction details is required for security reasons. However, the most basic abstractions, in addition to the overly staged kingdom of the observable creatures. Apart from the restricted gadgets that are accessible to everyone via the Internet, the power usage discount method plays a crucial role.

The suggested mechanism helps to meet these two conditions, which may cause readings from the raw sensor to be created in extreme-degree situations. The suggested option shortens the messages' range while focusing on a sensor that may cut energy consumption and extend the device's lifespan.

III. THE FUTURE OF INTERNET OF THINGS IN HEALTHCARE

A. Remote Patient Monitoring (RPM): Internet of things devices allow medical professionals to view patients' vital signs and symptoms, medication compliance, and general health status in real-time from a distance. Early identification of health issues, improved management of ongoing illnesses, and a decline in readmissions to medical facilities are all potential outcomes of this.

B. Wearable Health Tech: Heart rate, sleep habits, exercise levels, and other health parameters can be tracked using wearable technology that has Internet of things capabilities. These gadgets give people the tools to be proactive about their health and fitness while also giving medical experts useful information for individualized treatment.

C. Predictive Analytics: Large volumes of data can be collected by internet-connected sensors that are incorporated into hospital infrastructure, medical equipment, and even patient wearables. This data may be analyzed to find patterns, trends, and possible health hazards using machine learning algorithms and sophisticated analytics. This enables early detection and predictive healthcare solutions.

D. Enhanced Patient Experience: From making appointments and checking patients in to creating customized treatment plans and conducting remote consultations, internet of things technology may simplify many parts of the patient experience. Better results, more engagement, and higher levels of patient satisfaction may result from this.

E. Smart Healthcare Facilities: By controlling inventory levels, keeping an eye on equipment performance, and making sure the environment is safe and comfortable for patients, internet-connected gadgets *and sensors may maximize the effectiveness of healthcare facilities. The Internet of Things can also assist in automating* maintenance and sanitation operations, which lowers the chance of hospital-acquired illnesses.

F. Data Security and Privacy: Ensuring strong cyber security protocols and adherence to data privacy legislation will be crucial given the widespread use of internet of things gadgets that gather sensitive health data. To protect patient data from breaches or unwanted access, healthcare institutions need to have access controls, authentication, and encryption in place.

G. Collaborative Healthcare Ecosystem: All the parties involved in the healthcare ecosystem—patients, providers, insurers, and researchers—can communicate and share data more easily and seamlessly thanks to the Internet of Things. The emergence of innovative, cooperative, and comprehensive methods for managing and delivering healthcare is encouraged by this interconnection.

H. Personalized Medicine: Advanced analytics in conjunction with Internet of things devices can make it possible to provide personalized medicine that is suited to each patient's particular characteristics, such as genetic composition, lifestyle choices, and environmental influences. With this strategy, the one-size-fits-all model can be replaced with personalized interventions that maximize therapeutic effectiveness, decrease adverse responses, and enhance overall patient outcomes.

I. Telemedicine and Remote Care: Access to medical expertise is extended beyond traditional healthcare venues with the help of the Internet of Things and telemedicine technologies, which enable healthcare experts to give high-quality care remotely. In addition to audio conferencing and secure channels of communication, The web of things-enabled monitoring devices allow individuals to receive quickly evaluations, follow-ups, and ongoing assistance from the comfort of their homes. This is especially advantageous for those who live in rural or underserved areas.

J. Health Data Interoperability: Healthcare interoperability is still a major problem that makes it difficult for various systems and stakeholders to communicate patient data seamlessly. This problem might be solved by the internet of things by standardized formats for data, protocols, and interfaces, which would make it possible for many platforms and devices to interact with one another. A patient's capacity to securely communicate their health information with numerous clinicians and locations, improves care coordination, and allows for full health records to be created, all of which support patient autonomy and continuity of treatment as well as well-informed decision-making.

All things considered, the IOT for healthcare has the potential to completely change the way patients are treated, enhance clinical results, and increase efficiency throughout the entire healthcare system. To reach its full potential, though, a thorough analysis of the moral, legal, and technological issues involved will be necessary.

VI. CONCLUSION

In conclusion, the future of the Internet of Things (Internet of things) is exceptionally bright, as it continues to reshape the way we interact with technology and the world around us. This transformative paradigm, characterized by the interconnectedness of everyday objects and devices to the internet, is poised to bring about profound changes across industries and aspects of daily life. Several key trends and developments are driving the evolution of Internet of things. The deployment of 5G networks is set to enable faster and more reliable connectivity, unlocking the potential for real-time communication and applications such as autonomous vehicles and remote surgeries. Edge computing is becoming integral to Internet of things systems, allowing for localized data processing and quicker decision-making, which is crucial for applications like industrial automation and smart cities. The integration of artificial intelligence (AI) and machine learning into Internet of things devices and platforms is enhancing their ability to analyze and interpret data intelligently. AI-driven Internet of things applications can optimize energy consumption, predict equipment failures, and provide personalized user experiences. Healthcare is being revolutionized through remote patient monitoring and the management of medical equipment, leading to more efficient and personalized care. Smart cities are embracing Internet of things technologies to improve urban sustainability and efficiency. These technologies are being employed in traffic management, waste collection, environmental monitoring, and more. In the industrial sector, Industrial Internet of things (Internet of things) is driving predictive maintenance, quality control, and supply chain optimization, reducing downtime and enhancing productivity. While the future of Internet of things holds immense promise, it also presents challenges. Security and privacy concerns are paramount, necessitating ongoing advancements in Internet of things security protocols and block chain-based solutions. Interoperability standards are crucial to ensure that the diverse array of Internet of things devices and platforms can work seamlessly together.

REFRENCES

[1] M. Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A Review on Internet of Things (Internet of things)," International Journal of Computer Applications, vol. 113, 2015.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, pp. 2787-2805, 2010.

[3] R. H. Weber, "Internet of Things–New security and privacy challenges," Computer Law & Security Review, vol. 26, pp. 23-30, 2010.

[4] M. Hassanalieragh, A. Page, T. Soyata, G. Sharma, M. Aktas, G. Mateos, et al., "Health monitoring and management using internet-of-things (Internet of things) sensing with cloud-based processing: Opportunities and challenges," in Services Computing (SCC), 2015 IEEE International Conference on, 2015, pp. 285-292.

[5] H. Abie and I. Balasingham, "Risk-based adaptive security for smart Internet of things in eHealth," in Proceedings of the 7th International Conference on Body Area Networks, 2012, pp. 269-275.

[6] N. Bui and M. Zorzi, "Health care applications: a solution based on the internet of things," in Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, 2011, p. 131.

[7] B. Lee, "Healthcare Framework on the Internet of things open Platform," Service Model, Architecture, International Journal of Applied Engineering Research, vol. 9, pp. 29783-29792, 2014.

[8] K. Zhao and L. Ge, "A survey on the internet of things security," in Computational Intelligence and Security (CIS), 2013 9th International Conference on, 2013, pp. 663-667.

[9] T. L. Koreshoff, T. Robertson, and T. W. Leong, "Internet of things: a review of literature and products," in Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration, 2013, pp. 335-344.

[10] A. Kulkarni and S. Sathe, "Healthcare applications of the Internet of Things: A Review," International Journal of Computer Science and Information Technologies, vol. 5, pp. 6229-32, 2014.

[11] K. Govinda and R. Saravanaguru, "Review on INTERNET OF THINGS Technologies," International Journal of Applied Engineering Research, vol. 11, pp. 2848-2853, 2016.

[12] P. Mahalle, S. Babar, N. R. Prasad, and R. Prasad, "Identity management framework towards internet of things (Internet of things): Roadmap and key challenges," in International Conference on Network Security and Applications, 2010, pp. 430-439.

[13] I. Toma, E. Simperl, and G. Hench, "A joint roadmap for semantic technologies and the internet of things," in Proceedings of the Third STI Roadmapping Workshop, Crete, Greece, 2009.

[14] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (Internet of things): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, pp. 1645-1660, 2013.

[15] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (Internet of things): A literature review," Journal of Computer and Communications, vol. 3, p. 164, 2015.

[16] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. Aswathy, "A state of the art review on the Internet of Things (Internet of things) history, technology and fields of deployment," in Science Engineering and Management Research (ICSEMR), 2014 International Conference on, 2014, pp. 1-8.

[17] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "Internet of things security: ongoing challenges and research opportunities," in 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, 2014, pp. 230-234.

[18] B. Khoo, "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy," in Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing, 2011, pp. 709-712.

[19] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, 2012, pp. 648-651.

[20] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: Perspectives and challenges," Wireless Networks, vol. 20, pp. 2481-2501, 2014.

[21] J.-c. YANG, P. Hao, and X. ZHANG, "Enhanced mutual authentication model of Internet of things," The Journal of China Universities of Posts and Telecommunications, vol. 20, pp. 69-74, 2013.

[22] K. Rhee, J. Kwak, S. Kim, and D. Won, "Challengeresponse based RFID authentication protocol for distributed database environment," in Security in Pervasive Computing, ed: Springer, 2005, pp. 70-84.

[23] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed Internet of things applications," in Wireless Communications and Networking Conference (WCNC), 2014 IEEE, 2014, pp. 2728-2733.

[24] S. Kalra and S. K. Sood, "Secure authentication scheme for Internet of things and cloud servers," Pervasive and Mobile Computing, vol. 24, pp. 210-223, 2015.

[25] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-key cryptography for RFID-tags," in Pervasive Computing and Communications Workshops, 2007. PerCom Workshops' 07. Fifth Annual IEEE International Conference on, 2007, pp. 217-222

[26] J. Liu, Y. Xiao, and C. P. Chen, "Authentication and Access Control in the Internet of Things," in ICDCS Workshops, 2012, pp. 588-592.

[27] P. N. Mahalle, N. R. Prasad, and R. Prasad, "Threshold Cryptography-based Group Authentication (TCGA) scheme for the Internet of Things (Internet of things)," in Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 2014 4th International Conference on, 2014, pp. 1-5.

[28] S. R. Moosavi, T. N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, et al., "SEA: a secure and efficient authentication and authorization architecture for Internet of things-based healthcare using smart gateways," Procedia Computer Science, vol. 52, pp. 452-459, 2015.

[29] M. A. Jan, P. Nanda, X. He, Z. Tan, and R. P. Liu, "A robust authentication scheme for observing resources in the internet of things environment," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on, 2014, pp. 205-211.

[30] R. Mietz, P. Abraham, and K. Römer, "High-level states with CoAP: Giving meaning to raw sensor values to support Internet of things applications," in Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014 IEEE Ninth International Conference on, 2014, pp.