A PUBLICLY VERIFICABLE SECURE AND EFFICIENT CLOUD-CENTRIC INTERNET OF MEDICAL THINGS ENABLED SMART HEALTH CARE SYSTEM

First Author:

V. Chandra Sekhar, Associate Professor, Dept of MCA, ASCET, Gudur.

Second Author:

U. Prathibha, PG Scholar, MCA, ASCET, Gudur.

ABSTRACT:

Using the chosen message attack (EUF-CMA) and the chosen cypher text assault, we have suggested an escrow-free identity-based aggregate signcryption (EF- IDASC) scheme that is secure against existential forgery attacks (IND- CCA2). It uses the least amount of energy for communication and computation when compared to other systems. We have created a cloud-centric, internet of things-enabled smart healthcare system based on the proposed EFIDASC. Without disclosing any information to a third party, the healthcare system has secured patient PHI both inside and outside the BAN and ensured the public integrity of PHI kept on the cloud. Additionally, we have examined how well the suggested cloud-centric, IoMTbasedhealthcare system performs in terms of compute and communication energy usage.

I INTRODUCTION:

The Industrial Internet of Things (IIoT) is a well-known, rapidly developing technology that consists of several intelligent, interconnected devices that perceive, process, and share data via sensors implanted all around them. A patient's health can now be remotely monitored in real- time using IIoT-connected medical monitoring equipment, such as Wireless Body Area Network (WBAN). WBAN is a network of various tiny sensors, each with a limited amount of power, compute, and storage. A sensor that gathers patient personal health information (PHI) and transmits it to a medical practitioner (data consumer) over a wireless (cellular) network is implanted on or within the patient's body. Any assault on a sensor or illegal access to a patient's PHI could endanger the patients' lives. Therefore, the challenge deriving from the resource limitations behaviour is the security and privacy of a patient's PHI over a public network. Smart healthcare has recently benefited from mobile technology, but daily growing data transmission is taxing the cellular network. Device-to-Device (D2D) communication, which can function at the same time/frequency resources at small distances, is one of the most alluring solutions. Cloud-enabled IoT may have recently provided the storage and processing power for large amounts of IoT data. However, the benefits that cloud technology brings to IoT come at the expense of additional security vulnerabilities that were not present in the traditional IoT system. In reality, a cloud is an honest-but-curious creature that uses

legitimate methods to compute and store the vast amounts of data gathered, but is curious enough to access the data inadvertently for a competitive edge. Although the cloud offers a user-delegated facility, handling the security of user data has proven to be difficult. The benefit of incorporating these technologies into the e-health monitoring system is to provide a practical platform that enables a patient's ailment to be remotely diagnosed by an authorised medical body. Additionally, ensuring the accuracy of the data stored in the cloud is a crucial issue with cloud-enabled medical systems. Public auditing, however, can offer a practical way to remotely check the accuracy of recorded data. It is still difficult to provide a secure data transmission system for cloud-centric IoMT-enabled healthcare, despite the fact that several privacy- preserving solutions [8]– [10] have been suggested. In a public-key setting, the two fundamental cryptographic primitives of signature and encryption are used to ensure the authenticity and privacy of data, respectively. To assure data privacy and authenticity at the same time, these two fundamental building blocks can be combined in a number of ways, including sign-then-encrypt, encrypt-then-sign, digital signature with message recovery, and signcryption (authenticated encryption). The simple structures of the sign-then-encrypt and encrypt-then-sign schemes give data privacy and authentication at a cost equal to the sum of the costs of signature and encryption systems. Anyone can extract the embedded message in a signature utilising message recovery scheme without knowing a secret. Signcryption, a more effective alternative to signthen-encrypt and encrypt-then-sign techniques, has recently been developed to provide a system that simultaneously accomplishes privacy and authenticity. Additionally, it enables a specified receiver to use his private key to decrypt themessage and access it.

II.LITERATURE SURVEY

showing four different forms of signature forgery attacks to show that the CLS system does not achieve the advertised security features. recommending a strong certificate- less signature (RCLS) system as well to address the problems highlighted above.RCLS is secure against both public key replacement attacks and malevolent but passive third parties in the standard model and simply requires public channels. According to performance evaluation, RCLS performs better than other CLS schemes and is appropriate for IoT. Title: Effective and Reliable Certificate-free Signature for Data Crowd Sensing in Cloud-Assisted Industrial IoT Authors: Robert H. Deng and Yinghui Zhang Year: 2019. In this work, they suggest the IBAAKA protocol (identity-based anonymous authentication and key agreement), which enables user anonymity and mutual authentication for WBAN in a cloud-assisted context. The suggested IBAAKA technique is demonstrated to be provably secure in the security analysis, as well as achieving the necessary security features, under the well-known computational Diffie Hellman assumption and random oracle model. Title: A Lightweight Identity-Based

Anonymous Authentication and Key Agreement Protocol for Secure Wireless Body Area Network Assisted by the Cloud Authors: Satish Chand and Mahender Kumar Year: 2020. When a patient goes to the hospital for assistance, the hospital can monitor their health-related parameters remotely, continuously, and in real time. This information is processed and transferred to a medical data centre, like cloud storage, which significantly improves the effectiveness, convenience, and cost performance of healthcare. The exponential growth of MIoT devices' data handling capacity increases the exposure of sensitive data. There are still many open questions regarding the security and privacy of data acquired from MIoT devices, both during transmission to the cloud and while being stored there. Here, they emphasise the needs for data flow security and privacy in MIoT. Title: A overview of security and privacy issues in the medical Internet of Things Wenchang Sun and Zhiping Cai wrote this. Year: 2018

III.EXISTING SYSTEM

Modern secure and effective cloud-centric IoMT enabled smart health care system with public verifiability is available in the current system. The system novelty uses the escrow-free identity-based aggregate signcryption (EF-IDASC) approach, which is also suggested in this article, to secure data transfer. The suggested smart healthcare system gathers the patient's medical data from a variety of implanted sensors, encrypts it using the proposed EFIDASC method, aggregates it, and sends it to a medical cloud server via smartphone. The patient's identify and medical details are kept secret by the system. Li et al. introduce Identity-based signcryption, which simultaneously satisfies the authentication and secrecy requirements without verifying a recipient's public key individually, for low-power devices (sensors) in an online/offline scenario. For the WBAN system, Omala et al. presented a simple certificateless signcryption (CLSC) mechanism for secure data transmission. For secure communication between WSNs, Yin et al. provide an effective hybrid signcryption technique in a certificateless environment. Schemes and are resistant to key escrow attack, in contrast to scheme. Zhang et al. go through a certificateless generalised signcryption (CLGSC)-based data communication technique for the e-health system. Caixue Zhou argues that Zhang et alplan .'s is flawed. vulnerable to insider assault. As a result, the scheme lacks security and is exposed to data confidentiality risks.Recent presentations by Zhou for the mobile healthcare system include an improvised CLGSC scheme. Selvi et al. explore three aggregated signcryption techniques in the identity-based environment that provide public verifiability to lower the transmission costs and overhead of verification. A first identity-based aggregated signcryption technique utilising multi-linear mapping in the standard model is proposed by Wang et al. For low-processor systems, Kar suggests a brand-new identity-based aggregated signcryption technique. Eslami et al. solve the key escrow issue and then provide an aggregate-signcryption strategy in the certificateless scenario, however approaches

are still vulnerable to this issue. When using heterogeneous devices, Niu et al. [24] present a secure transmission strategy that sends k messages from k senders in certificateless settings to m recipients in the IBC setting. The identity-based signcryption system proposed by Kumar et al. for secure peer- to-peer video on demand protocol. For the Internet of Things in health, Yang et al.

[30] proposed a distributed safe data management system with a productive keyword search mechanism. Elhoseny et al. [31] presented a hybrid encryption method for maintaining the diagnostic text data in medical photographs that combines the Rivest, Shamir, and Adleman (RSA) and Advance Encryption Standard (AES) algorithms. We concluded from the discussion above that it is difficult to create a safe and effective smart healthcare system that is enabled by the Internet of Things (IoMT) and achieves public verifiability.

DISADVANTAGES: As a result of the lack of a Trust Model Based on Fuzzy Comprehensive Evaluation Method in the current work, the system is less effective. Due to the Bilinear Diffie-Hellman (BDH) Problem, the system is less secure.

IV.PROPOSED SYSTEM

First, based on the concept provided in the current system, we provide an escrow-free identity-based aggregated signcryption (EF- IDASC) technique that tackles the key escrow problem. The system demonstrates that the proposed EF-IDASC scheme in the random oracle model (ROM) and well- known Bilinear Diffie-Hellman Problem is existentially un forgeable under chosen message attack (EUFCMA) and adaptively indistinguishable under chosen cypher text attack (IND-CCA) (BDHP). The suggested EF-IDASC approach is compared to other relevant signcryption schemes in the system, and we demonstrate that it uses the least energy when compared to the others. Then, based on the proposed EF-IDASC scheme, we present a secure D2D aggregated data transmission protocol in the cloud-centric IoMT context for smart health care. Additionally, we assess the cost of energy usage (in mJ) for processing, storage, and communication. By achieving patient anonymity, public auditing of the cloud-stored data's integrity, and mutual authenticity of patient data with public verifiability, the proposed secure healthcare system accomplishes patient privacy.

ADVANTAGES: Data cannot be changed or modified by any adversary because to an efficient system design. The During decryption, the SD will detect any alterations or forgeries in the signed data. If the BDH problem is challenging to answer, a hostile attacker won't be able to change the original data.

V.SYSTEM ARCHITECTURE

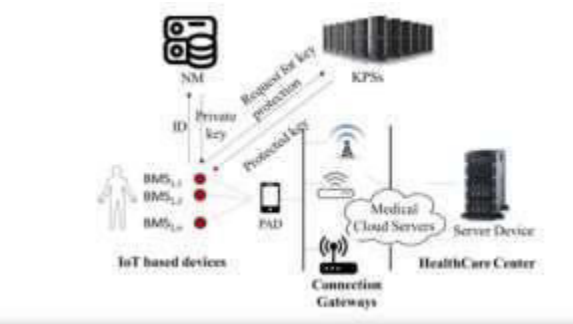

Fig 1: Architecture of face expression recognition system.

VI.MODULES DESCRIPITION:

IOT Device

This module requires an IOT device to register with a cloud, log in, encrypt a file, and upload it to a cloud server. It also requires the device to register with departments and specialists, such as cardiology, nephrology, and kidney. Log

into view your profile. Upload the patient's information (pid, pname, paddress, DOB, email, age, hospitalname, disease, blood group, symptom, attach disease file, attach
user image), with the exception of pname, which is encrypted. the patient's name and any submitted information Select Department, Profession, and other factors to customise Access Control permissions. View the date and time for every patient detail that has been uploaded. View all information provided by Access Control along with the date and time. MEDICAL CLOUDSERVER: The cloud will approve both the owner and the user in this module, as well as carry out the following actions: View all patient's information in decrypt mode, and View all Access Control Information See every transaction, including uploads, downloads, and searches, and View information on requests for secret keys, including dates and times. View the chart's number of the same ailment, View the chart's Patient Rank to View the number of attackers on the patient who entered the erroneous secret key. KPS The KPS Authority carries out the following actions in this module, including logging in, viewing Owners and approving them, and viewing Users and approving them. List all attacker information with date and time using the incorrect secret key, as well as the details of the secret key request, generation, and authorization. Healthcare centers: The healthcare centre user must register to the cloud in this module, log in, and completethe following tasks: view profiles, search patient details by content keyword (display patient files and details if access control is given), request secret key, and list all secret key permitted responses from authority with download option only here.

VII. RESULT

User Registration page IOT Device loging

View All Users

View All Transaction

VIII. CONCLUSION

In this research, we offer an escrow-free identity-based aggregate signcryption (EF- IDASC) method that is protected from existential forgery attacks under the chosen message attack (EUF-CMA) and undetectable under the chosen cypher text assault (IND-CCA2). It uses the least amount of energy for communication and computation when compared to other systems. We have created a cloud-centric, internet of things-enabled smart healthcare system based on the proposed EFIDASC. Without disclosing any information to a third party, the healthcare system has secured patient PHI both inside and outside the BAN and ensured the public integrity of PHI kept on the cloud. Additionally, we have examined how well the suggested cloud-centric, IoMT-based healthcare system performs in terms of compute and communication energy usage. Future enhancement: By encrypting all characteristics and creating an attribute-based search technique, an efficient key-policy attribute-based encryption is put into practise.

REFERENCES:

[1] Y. Zhang, R. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, “Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT,” IEEE Trans. Ind. Informatics, 2019.

[2] M. Kumar and S. Chand, “A Lightweight Cloud-Assisted Identity-based Anonymous Authentication and Key Agreement Protocol for secure.Wireless Body Area Network,” IEEE Syst. J., vol. Early acce, 2020.

[3] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, “Security and privacy in the medical Internet of Things: A review,” Secur. Commun. Networks, vol. 2018, 2018.

[4] A. Zhang, J. Chen, R. Q. Hu, and Y. Qian, “SeDS: Secure data sharing strategy

for D2D communication in LTE-Advanced networks,” IEEE Trans. Veh.

Technol., vol. 65, no. 4, pp. 2659–2672,
2016.

[5] Z. Li, Z. Yang, and S. Xie, “Computing Resource Trading for Edge- Cloud-assisted Internet of Things,” IEEE Trans. Ind. Informatics, 2019.

[6] W. Wang, P. Xu, and L. T. Yang, “Secure data collection, storage and access in cloud-assisted IoT,” IEEE Cloud Comput., vol. 5, no. 4, pp. 77–88, 2018.

[7] D. He, S. Zeadally, and L. Wu, “Certificateless public auditing scheme for cloud-assisted wireless body area networks,”IEEE Syst. J., vol. 12, no. 1, pp.64–73, 2015. [8] V. Sureshkumar, R. Amin, V. R. Vijaykumar, and S. Rajasekar, “Robust secure communication protocol for smart healthcare system with FPGA implementation,” Futur. Gener. Comput.Syst., 2019.

[9] H. Xiong and Z. Qin, “Revocable and scalable certificateless remote authenticationprotocol with anonymity for wireless body area networks,” IEEE Trans. Inf. forensics Secur., vol. 10, no. 7, pp. 1442–1455, 2015.

[10] J. Shen, S. Chang, J. Shen, Q. Liu, and IX. Sun, “A lightweight multi-layer authentication protocol for wireless body area networks,” Futur. Gener. Comput Syst., vol. 78, pp. 956–963, 2018.

[11] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. J. Peterson and A. D. Rubin, “Securing electronic medical records using attribute-based encryption on mobile devices,” in Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, 2011, pp. 75–86.

[12] C. Hu, H. Li, Y. Huo, T. Xiang, and X Liao, “Secure and efficient data communication protocol for wireless body area networks,” IEEE Trans. Multi-Scale Comput. Syst., vol. 2, no. 2, pp. 94–107, 2016.

[13] B. Chandrasekaran, R. Balakrishnan, and Y. Nogami, “Secure Data Communication using File Hierarchy Attribute Based Encryption in WirelessBody Area Networks,” 2018.

[14] F. Li, M. K. Khan, K. Alghathbar, and T. Takagi, “Identity-based online/offline signcryption for low power devices,” J. Netw. Comput. Appl., ., vol. 35, no. 1, pp.340--347, 2012.

[15] A. A. Omala, N. Robert, and F. Li, “A provably-secure transmission scheme for wireless body area networks,” J. Med Syst.,vol. 40, no. 11, p. 247, 2016.

Author's Profile:

 Mr. V. CHANDRASEKHAR

has received him MCA degree from Sri Venkateswara University in 2001, Tirupati respectively. He is dedicated to teaching field from the last 21years. He has guided P.G students. At present he is working as Associate Professor in Audisankara College of Engineering and Technology, Gudur, Tirupati (Dt), Andhra Pradesh, India

U. PRATHIBHA has Pursuing his MCA from Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, affiliated to JNTUA in 2022. Andhra Pradesh, India