ISSN: 2278-4632
Vol-13, Issue-08, August 2023

SECURE AND EFFECTIVE HEALTHCARE SOLUTION FOR THE INTERNET OF MEDICAL THINGS WITH PUBLIC VERIFICATION

[#1]GUNTUKA SWETHA, ***Department of MCA,***

[#2]Dr.G.S.CHOWHAN, ***Associate Professor,***

[#3]Dr.V.BAPUJI, ***Associate Professor& HOD,***

Department of Master of Computer Applications,

VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA.

ABSTRACT: Using the chosen message attack (EUF- CMA) and the chosen cypher text assault, we suggested an escrow-free identity-based aggregate signcryption (EF- IDASC) method that is secure against existential forgery attacks (IND- CCA2). It uses the least amount of energy for computing and communication when compared to other systems. We created a cloud-centric, internet-of-things-enabled smart healthcare system based on the planned EFIDASC. The healthcare system has preserved the public integrity of PHI kept on the cloud and protected patient PHI both inside and outside the BAN without disclosing any information to a third party. Furthermore, we assessed the suggested cloud-centric, IoMT-based healthcare system's compute and communication energy efficiency.

1. INTRODUCTION

The IIoT is a popular and rapidly developing field of technology. It consists of a network of interconnected, sensor-equipped smart devices that can gather, analyze, and disseminate information. A patient's health can now be tracked online and in real time with the help of medical monitoring tools like Wireless Body Area Network (WBAN) that are linked to the Industrial Internet of Things (IIoT). The WBAN network's small sensors have limited processing and storage capabilities. A sensor worn by the patient or implanted within the patient's body collects PHI. A clinician (the data consumer) receives this data over a cellular wireless network. A patient's life may be in jeopardy if their PHI is examined without authorization or if a sensor is compromised. Due to resource constraints, patient PHI is less secure and private over a public network. However, the increasing volume of everyday data exchange is putting stress on the cellular network, despite the fact that mobile technology has recently helped make healthcare smarter. One of the most promising concepts is device-to-device (D2D) transmission, which, over relatively short distances, makes efficient use of the same time/frequency resources. compatible with cloud computing Many months' worth of IoT data may have been analyzed and stored thanks to the IoT. Cloud computing has several advantages for the Internet of Things (IoT), but these are outweighed by new security concerns. In reality, a cloud is a benign but inquisitive entity that employs ethical means to process and store massive amounts of data, but which may, out of sheer curiosity, get unauthorized access to that data and exploit it to its advantage. Although cloud computing facilitates delegation, protecting user information has proven challenging. Adding these tools to the e-health monitoring system will allow a licensed medical center to diagnose a patient's condition without ever having to leave their office. Data stored in cloud-connected healthcare systems cannot be trusted to be accurate. The accuracy of data stored in remote locations can be verified, however, by public auditing. It is challenging to develop a secure data transmission system for cloud-based IoMT-enabled healthcare, despite the availability of a variety of privacy-protecting alternatives [8-10].

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

Data confidentiality and authenticity can be safeguarded using the public-key system's two linchpin cryptographic operations: signing and encrypting. Many different combinations of these two fundamental building blocks exist, such as "sign then encrypt," "encrypt then sign," "digital signature with message recovery," and "signcryption" (authenticated encryption). The combined price of signing and encryption systems is the same as that of the sign-then-encrypt and encrypt-then-sign approaches. Anybody, even if they don't know the secret, can recover the message hidden in a signature using a message recovery method. Signcryption was recently developed to allow for both privacy and authenticity to be attained concurrently, making it a more efficient alternative to sign-then-encrypt and encrypt-then-sign. Additionally, it permits a single recipient to read an encrypted message by using his own private key.

2. LITERATURESURVEY

The CLS system is proven to lack the advertised security characteristics using a total of four forged signatures. To sign documents without a certificate, we also propose a robust certificate-less signature (RCLS) mechanism. According to the standard model, RCLS is impervious to assaults from both active and passive third parties, as well as public key replacement attacks. It merely requires usable routes. The study's findings suggest that RCLS is superior to other CLS approaches and can be employed for IoT. This research paper is titled "A Reliable and Effective Certificate-free Signature for Data Crowd Sensing in Industrial IoT with Cloud Support." It was co-authored by Robert H. Deng and Yinghui Zhang. Year: 2019. The IBAAKA protocol (identity-based anonymous authentication and key agreement) is presented in this research to facilitate user authentication while maintaining anonymity in a cloud-based WBAN setting. Provable safety and adequate security for the proposed IBAAKA method have been demonstrated using the well-known computational Diffie-Hellman assumption and random oracle model. This paper discusses a protocol for establishing secure wireless body area networks that relies on anonymous authentication and key agreement and uses cloud computing for its implementation. It was authored by Satish Chand and Mahender Kumar. Year: 2020. A patient's vital signs can be monitored remotely, in real time, whenever they visit a hospital for treatment. Sending this data to a medical data center for processing and storage has similar benefits to cloud computing for the health care industry. As Internet of Things (IoT) devices become more efficient at data management, sensitive information is more at risk. Concerns have been raised over how safe and private information obtained from Internet of Things (IoT) devices will be when it is transferred to and kept in the cloud. The importance of protecting the privacy and security of IoT data flows is discussed here. An overview of the implications of the medical IoT for data privacy and protection Authors credit goes to Cai Zhiping and Sun Wenchang. Year: 2018

EXISTINGSYSTEM

Cloud-based, IoMT-based, publically auditable, and secure health care systems already exist. The system employs the escrow-free identity-based aggregate signcryption (EF-IDASC) technique, which is supported by this component. Prior to being merged and transmitted to a medical cloud service via smartphone, the patient's medical data is encrypted using the EFIDASC technique. The proposed intelligent health care system collects data from a variety of implanted sensors.

A patient's identity and health records are shielded from prying eyes by the system. The claim is made by Li et al. that identity-based signcryption is feasible for low-power devices (sensors). Without individually verifying the public keys of each recipient, it satisfies the authentication and secrecy requirements. Omala et al. proposed a straightforward certificateless signencryption (CLSC) technique for securing data transmission in the WBAN system. WSNs can use hybrid sign-encryption to communicate securely without certificates, as demonstrated by Yin et al. Contrary to popular belief, key escrows

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

are not vulnerable to assault. Certificateless generalized signcryption (CLGSC) is utilized by Zhang et al. to transmit and receive data in an electronic health care system. According to Caixue Zhou, Zhang and his pals have hatched a disastrous scheme. Internal attacks should be taken very seriously. This creates security and privacy concerns with the method.Zhou has recently revised the CLGSC strategy for the mobile healthcare system in presentations. In an identity-based scenario, Selvi et al. examine three aggregated signcryption algorithms that provide public verifiability with lower transmission costs and verification overhead. The first identity-based combined sign-encryption technique for the standard model is demonstrated by Wang et al. Kar proposes a novel aggregate-based sign-encryption technique for low-processor systems. While Eslami et al. have provided a solution to the key escrow problem in a certificate-less setting, it is still possible for this issue to arise when using alternative techniques of encryption. In order to send k messages from k senders without certificates to m recipients using heterogeneous devices in an IBC configuration, Niu et al. [24] provide a method for doing so that is both safe and scalable. Kumar et al. proposed an identity-based signcrypted P2P VOD system to ensure user privacy. The health IoT system developed by Yang et al. [30] is equipped with a robust keyword search engine and safe data management. Elhoseny et al. [31] unveiled a hybrid encryption approach for shielding diagnostic text data in medical photographs, employing both the Rivest, Shamir, and Adleman (RSA) and Advance Encryption Standard (AES) algorithms. We have shown that it is challenging to create a smart healthcare system that is simultaneously secure, efficient, makes use of the Internet of Things (IoT), and permits public verification.

DISADVANTAGES: Because there is no Trust Model Based on Fuzzy Comprehensive Evaluation Method in place, the current approach is subpar. The Bilinear Diffie-Hellman (BDH) Problem threatens the system's security.

3. PROPOSEDSYSTEM

We begin by demonstrating an alternative to traditional key escrow systems, which we call escrow-free identity-based aggregated signcryption (EF-IDASC). The system demonstrates that the proposed EF-IDASC scheme is existentially unforgeable under a selected message attack (EUFCMA) and adaptively indistinguishable under a selected cipher text assault (IND-CCA) in the random oracle model (ROM) and the well-known Bilinear Diffie- Hellman Problem (BDHP). We demonstrate that the proposed EF-IDASC approach requires the lowest amount of energy compared to other viable signcryption methods. We then provide a secure D2D data transmission protocol based on the proposed EF-IDASC method in the context of cloud-centric IoMT for smart health care. The price of generating, storing, and transporting energy (in mJ) is also calculated. The anonymity of patients, the verifiability of cloud-stored data integrity, and the verifiability of mutual authentication of patient data are all ways in which the proposed secure healthcare system preserves patient privacy.

ADVANTAGES: A secure system architecture prevents adversaries from altering information. If there are any forgeries or alterations to the signed data, the SD will detect them during decoding. If the BDH problem is challenging, an adversary will have a hard time altering the data.

4.SYSTEM ARCHITECTURE

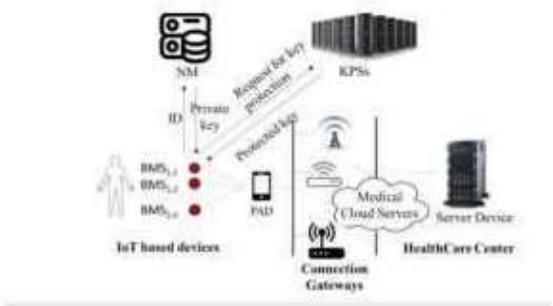

Fig1:Architectureoffaceexpressionrecognitionsystem.

5. MODULES DESCRIPITION

IOT Device

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

This module requires an Internet-of-Things device to create a cloud account, join an existing cloud, encrypt a file, and upload it to a cloud server. Cardiology, nephrology, and kidney specialists, among others, must all sign off on the device's registration before it may be used. In order to access your profile, you must first log in. All patient information (excluding the encrypted pname) should be uploaded, including the pid, pname, paddress, DOB, email, age, hospital name, disease, blood group, symptom, disease file, and user image. Patient names and other information, such as Department and Profession, can be used to modify Access Control permissions. Learn when each patient update was made and how long ago it was made. Examine the current time and date, as well as the rest of the information provided by Access Control. Components of a Cloud Health Server include: Here, the cloud will do the following, beginning with an authentication of both the owner and the user: Look at a complete log of access control information and the protected patient data. Verify any and all actions, including searches, downloads, and uploads. Examine data like requests for private keys and when they were made. view the associated graph item. If you want to know how many people tried to harm the patient who entered the wrong secret key, look at the Patient Rank graph. The KPS Authority is responsible for signing in, reviewing, and authorizing Owners, as well as monitoring, reviewing, and granting permission to Users. Document everything you can about the perpetrator, from the time and date the wrong secret key was used to details about who requested, created, and was granted access to the secret key. locations offering medical treatment In order to browse profiles, search for patient details by content keyword, request a secret key, and list all secret key permitted responses from authority with the option to download, the healthcare center user must first register for the cloud in this module and log in.

6. RESULT

UserRegistrationpageIOTDeviceloging

ViewAllUsers

ViewAllTransaction

7. CONCLUSION

In this research, we provide an escrow-free identity-based aggregate signencryption scheme (EF-IDASC) that is undetectable via the chosen cypher text attack (IND-CCA2) and secure against existential forgery assaults via the chosen message attack (EUF-CMA). When compared to other computing and communication devices, it consumes the least amount of power. We built an

advanced healthcare system using the cloud and IoT based on the EFIDASC recommendations. Protecting patient privacy both inside and outside of the BAN, the healthcare system has maintained the confidentiality of data stored in the cloud. We also investigated the cloud-based IoMT healthcare system's energy consumption during computation and transmission. In the long run: To implement key-policy attribute-based encryption successfully, it is necessary to encrypt each and every feature and to set up an attribute-based search algorithm.

REFERENCES:

[1] Y. Zhang, R. Deng, D. Zheng, J. Li, P.Wu,andJ.Cao,"Efficientandrobustcertificateless signaturefordatacrowdsensingincloud-assistedindustrialIoT,"IEEETrans.Ind.Informatics, 2019.

[2] M.KumarandS.Chand,"ALightweight Cloud-Assisted Identity-basedAnonymousAuthenticationandKeyAgreement Protocolforsecure.WirelessBody Area Network," IEEE Syst. J., vol.Earlyacce,2020.

[3] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang,and G. Wang, "Security and privacy in themedicalInternetofThings:Areview,"Secur.Commun.Networks,vol.2018,2018.

[4] A. Zhang, J. Chen, R. Q. Hu, and Y.Qian,"SeDS:SecuredatasharingstrategyforD2DcommunicationinLTE-Advancednetworks,"IEEETrans.Veh.Technol.,vol.65, no.4,pp.2659–2672,2016.

[5] Z.Li,Z.Yang,andS.Xie,"ComputingResourceTradingforEdge-Cloud-assistedInternetofThings," IEEE Trans. Ind. Informatics,2019.

[6] W. Wang, P. Xu, and L. T. Yang,"Securedatacollection,storageandaccessincloud-assistedIoT,"IEEECloud Comput., vol. 5, no. 4, pp. 77–88, 2018.

[7] D. He, S.Zeadally,andL.Wu,"Certificateless public auditing schemefor cloud-assistedwirelessbodyareanetworks,"IEEE Syst. J., vol. 12, no. 1,pp.64–73, 2015.

[8] [8] V. Sureshkumar, R.Amin,V.R.Vijaykumar,andS.Rajasekar, "Robust securecommunicationprotocolforsmarthealthcaresystemwithFPGAimplementation,"Futur.Gener.Comput.Syst.,2019.

[9] H. Xiong and Z. Qin, "Revocableandscalablecertificatelessremote authenticationprotocolwithanonymityforwirelessbodyareanetworks,"IEEE Trans. Inf. forensicsSecur.,vol.10,no.7,pp.1442–1455, 2015.

[10] J.Shen,S.Chang,J.Shen,Q.Liu,andIX.Sun, "A lightweightmulti-layerauthenticationprotocolforwirelessbodyareanetworks,"Futur.Gener. ComputSyst.,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, "Securingelectronicmedicalrecordsusingattribute-basedencryptiononmobiledevices,"inProceedingsofthe1stACMworkshoponSecurityandprivacyinsmartphonesandmobiledevices,2011,pp. 75–86.

[12] C. Hu, H. Li, Y. Huo, T. Xiang, and XLiao,"Secureandefficientdatacommunicationprotocolforwirelessbodyareanetworks,"IEEETrans.Multi-Scale Comput. Syst., vol. 2, no.2, pp. 94–107, 2016.

[13] B.Chandrasekaran,R.Balakrishnan,andY. Nogami,"SecureDataCommunicationusing File HierarchyAttributeBasedEncryptioninWirelessBodyAreaNetworks,"2018.

[14] F.Li,M.K.Khan,K.Alghathbar,andT.Takagi,"Identity-basedonline/offlinesigncryptionforlowpowerdevices,"J.Netw.Comput.Appl., ., vol. 35, no. 1, pp.340--347,2012.

[15] A. A. Omala, N. Robert, and F. Li, "Aprovably-securetransmissionschemeforwirelessbody areanetworks,"J.MedSyst.,vol.40,no.11,p.247,201