Securing Sensor Data on Internet of Things (IoT) Devices

R. Aparna, Abhinav Kumar Mallick, and Utkarsh Sahay

Abstract The amount of personal devices has been increasing at an unprecedented rate for the past few decades. Also, all these devices are becoming smarter (containing microprocessor, AI enabled), and all are having Internet connectivity. This has made the life much simpler and smarter, but it has also increased the privacy risks. One such sensitive data is health data. There has been multiple cases of breach into health data storage systems. Personal IoT devices such as fitness bands are very close to the user and keep track of many sensitive data such as heart rate, number of steps walked, and the places visited. Efficient methods to secure Internet of Things in medical services are a need of the hour. The innovation and research in the field of Internet of Things for health care promise to meet that demand. It has brought rapid developments in medical treatment, services, and health care, but the improvements in this field are facing challenges related to security and authentication. In this paper, we propose a novel method of securing sensor data on IoT devices. We make use of RSA encryption technique; the public key of the user is transferred to the IoT device at the time of connection, and this key is used to encrypt the sensor data. Only, this encrypted data are synchronized with the user's account.

Keywords Internet of Things · Internet of Medical Things · RSA · Public-key cryptography

1 Introduction

The *Internet of Things* (*IoT*) is a collection of interrelated devices, comprises of mechanical and digital systems, the user, and the ability to transfer data over a network without requiring any human interaction.

Personal IoT refers to the overall system (devices and their communication with the sensors) and related results, usance and services that relate to direct use by a

R. Aparna (✉) · A. K. Mallick · U. Sahay
Department of Information Science and Engineering, Siddaganga Institute of Technology, Tumakuru, Karnataka, India
e-mail: raparna@sit.ac.in

A. Kumar et al. (eds.), *Proceedings of the International Conference on Cognitive and Intelligent Computing*, Cognitive Science and Technology,
https://doi.org/10.1007/978-981-19-2350-0_40

person and/or for the direct benefit of humans. Difference between IoT and personal IoT can be something like a person may not be involved directly. A device that is used by a consumer for various purposes including entertainment, education, information, and lifestyle enhancement is referred as connected consumer device. Personal IoT data may be used for a variety of purposes including marketing for the respective industries involved as well as leveraged by various third parties.

Across the globe, demand for secure and faster IoT medical services is on the rise. The IoT for medical services promise innovation to meet that demand. It is dramatically redefining medical services, and patient outcomes. The *Internet of Medical Things (IoMT)* is a humongous revolution in the healthcare industry, and with IoT, it has quickly established itself as an important and critical part of modern healthcare [1–3].

In currently available personal IoT devices, the sensor data are not encrypted; instead, it is directly transferred to the mobile app using Bluetooth. This kind of implementation raises concern about the security of personal data. This paper describes a novel mechanism to secure data from different sensors of an IoT device so that even if there is a hack, the data remain secure. The sensor data are encrypted using RSA encryption and then stored on the device [4]. Only, this encrypted data are synced with any other device or the cloud [5]. The mobile app allows the user to register and access the sensitive data. The main contribution of our research is an encryption mechanism for data transmitted from IoMT such as fitness bands. Another contribution is the android application to display the decrypted data only on the devices logged in by the user. For security purpose, the transmitted data must be encrypted at the IoT device itself, and the decryption process will be done at the user end, i.e., the android application [6, 7]. Encryption transforms the original data (Plaintext) into an 'unreadable' data (Ciphertext, which is scrambled data), whereas decryption performs the reverse operation, i.e., transforms the ciphertext into plaintext. Encryption and decryption processes require random cryptographic keys shared between sender and receiver, and these keys can be generated using a key generation function.

The paper is organized as follows: Literature survey is discussed in Sect. 2, Problem definition and proposed solution to the problem are discussed in Sects. 3 and 4 give implementation details, and Sect. 5 concludes the paper.

2 Literature Survey

To provide privacy and security for the data, different types of cryptographic techniques are used, among which encryption and decryption techniques are most common. Encryption techniques are divided into asymmetric and symmetric encryption. The asymmetric encryption technique uses two keys, a public key (for encryption) and a private key (for decryption). The symmetric encryption technique uses only one key which is the private key which is used for both encryption and decryption. Symmetric encryption [8] is extremely secured, simpler, and faster as it uses only one key for both encryption and decryption.

There are other symmetric encryption techniques, e.g., data encryption standard (DES), double DES, and triple DES. DES makes use of 64-bits block size plaintext at a time and a 56-bits key to generate a 64-bits ciphertext. Analysis on DES algorithm shows that it is quite weak encryption algorithm, and it can easily be cracked using brute-force technique [9, 10]. Thus, one cannot consider it as a secure technique for encrypting sensitive medical data. The triple data encryption standard (3DES) technique is similar to DES except the key size can be 112 or 168 bits, but it considers the same 64-bits block size as input and produces 64-bit ciphertext. It is stronger than DES, but still, it can be easily cracked.

This paper utilizes RSA encryption system [11], which is one of the awry encryption procedures. It utilizes two keys, open key, also called as public key and private key dependent on two enormous prime numbers. Any user can make use of the open key to encrypt the message; however, just somebody with the information of the private key can decrypt the message. Breaking RSA encryption is known as the RSA problem. The intricacy of the RSA encryption depends on the calculating issue, i.e., to locate the prime elements of a number. There are as of now no distributed strategies to overcome the framework if a huge enough key is utilized. The usage of RSA is less regularly used to straightforwardly encode client information.

The IoT application depends on a system including a progression of heterogeneous sensors and gadgets, which can continually watch the encompassing condition and gather the information. This heterogeneity is reflected in the crude information gathered by that sort of framework. Accordingly, IoT's significant level application assignments to decipher the information and identify true occasions are increasingly perplexing. What's more, information heterogeneity prompts an absence of interoperability between IoT applications. Semantic Web (SW) innovation has been generally embraced for displaying and incorporating information from different sources on the Web. Be that as it may, this sort of procedure requires a lot of processing assets, particularly in situations including countless sensors. To address such a test, Al-Osta et al. [12] proposed a lightweight semantics comment approach that can be actualized on asset-compelled IoT passage associating with constrained sensors. To assess the methodology, a progression of tests utilizing middleware model has been finished.

3 Problem Definition

In this section, first, existing system is discussed, and then, the system we are proposing will be elaborated.

3.1 Existing System

The Internet of Things is the augmentation of Internet network into physical gadgets and regular articles. It is installed with several physical gadgets that connects to the

Internet and different types of equipment (for example, sensors). These gadgets can impart and associate with others over the Internet, and one can operate the gadgets from remote locations, verify their status, and can be controlled remotely [8].

The meaning of the Internet of Things has developed because of the intermingling of different innovations, continuous examination, AI, commodity sensors, and embedded systems. Conventional fields of embedded systems, remote sensor systems, control frameworks, computerization (counting home and home automation), and others all add to empowering the Internet of Things. In the consumer market, IoT innovation is most synonymous with items relating to the idea of the "smart home," covering gadgets and apparatuses, (for example, lighting installations, indoor regulators, home security systems and cameras, and other home appliances) that help at least one normal biological systems, and can be controlled by means of gadgets related with that environment, for example, cell phones and smart devices [8].

Providing security and privacy to these devices (gadgets) is one of the important task, and the concept of IoT has faced prominent criticism, in this regard [8].

Security concerns have been raised about the rapid development and growth in usage of IoT devices without ample focus on the complex security challenges involved and the dearth of regulatory changes required to handle this phenomenon. The technical security concerns have commonalities with those of network servers, workstations, and smartphones. But, with the increasing usage and popularity of IoT devices, challenges distinctive to these have surfaced. The concerns can arise due to various reasons; the prominent causes are insecure Web interface, insufficient authentication/authorization, insecure network services, lack of transport encryption, insufficient security configurability.

3.2 Proposed System

In the proposed system, an android app has been developed that allows the users to share their health-related information with the doctor in a secure manner and uses cryptographic approach to provide security for the users. In the implementation, when the user registers on the app, a key is generated for the login id. Only, this key can be used to decipher the data. The data received from the sensors are encrypted and stored on the device. Only, this encrypted data are synced with the server. It can also be decided by the user to share the information with a doctor or with any person of trust. Once the data are shared, the key for that data is also attached with the ID of the person with whom it is shared with. This is achieved by ensuring that all the sensor data flow through the user-authorized app to any other place (app or user) on the OS level.

In the proposed implementation, a cryptographic approach is used to introduce security, authentication/authorization to improve the non-existent data security in IoT devices. We also aim to improve data confidentiality by providing users with the option to encrypt data being collected by the devices and provide permissions for a third party to access the data. The data can be stored on cloud-based platform to improve its portability and hence making it accessible on other devices (which are authorized by the user).

The implementation uses Rivest–Shamir–Adleman (RSA) algorithm to provide encryption of data on target devices. In RSA algorithm, the encryption key is public and is different from the decryption key which is kept private. In the proposed system, as soon as the user registers on the platform, encryption and decryption keys would be generated for that user. The system is then ready to perform cryptographic operations on user's data. The data would then be encrypted with the public key or the encryption key thus generated. This encrypted data would then be synchronized with the data storage servers or database. Users will be able to view their data on demand as it will be decrypted with their personal private keys on their devices.

We also have an option to share data with third parties, based on user authorization of the same. The user would be able to authorize several other users or applications to use his/her data, pertaining to which the private key or the decryption key for that data will be attached with the ID of the concerned party. This will allow other users to view and utilize the shared data. Inculcating this keeps end-user data private, improves his/her data privacy and simultaneously allowing free usage of the concerned data by trusted parties to perform analysis, or however, they wish to manipulate it.

4 Implementation

An android application has been implemented for the problem defined above [6]. The implementation of the android application mainly consists of the following major parts.

The android app has a login/sign-up screen that allows users to register or to sign up. Whenever a new user registers or signs up on the android application, a pair of keys is generated for that particular user. The pair of keys thus generated is unique and only with the use of this key can the encrypted data be decrypted. The app then monitors data being collected by the specified IoT devices. This data, being collected, is then encrypted with the help of the keys assigned to the user at the time of registration. RSA algorithm has been used for performing cryptographic operations.

The encrypted data are then stored on the local system and are then synchronized with the cloud [13]. This makes the application portable and user data more secure and easily accessible on other devices of their choice. Here, a pair of keys are generated which act as a public key and a private key. The public key is used for encrypting the data and the private key for decrypting it. The private key is stored in such a manner that it can be accessed by the app only that too for the purpose of decrypting the data.

The android application also provides an option for sharing of data with third parties. The user would be able to authorize several other users or applications to use that data. After which, the private key or the decryption key for that data will be attached with the ID of the person or the application with which the data are shared. This will allow other users to view and utilize the shared data.

The graphs in Figs. 1 and 2 represent the relation between various parameters of original file and the encrypted file. There are four fields representing original file size, encrypted file size, percentage change in size, and time taken to encrypt the file, respectively. The original file size is the size of file before any cryptographical operations are performed on it. The encrypted file size column shows the size of

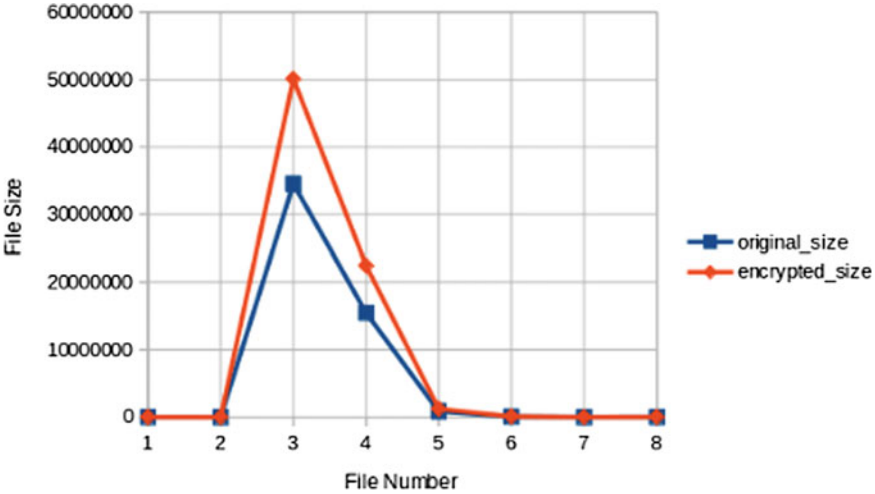

Fig. 1 Graph showing change in file sizes for image files before and after encryption

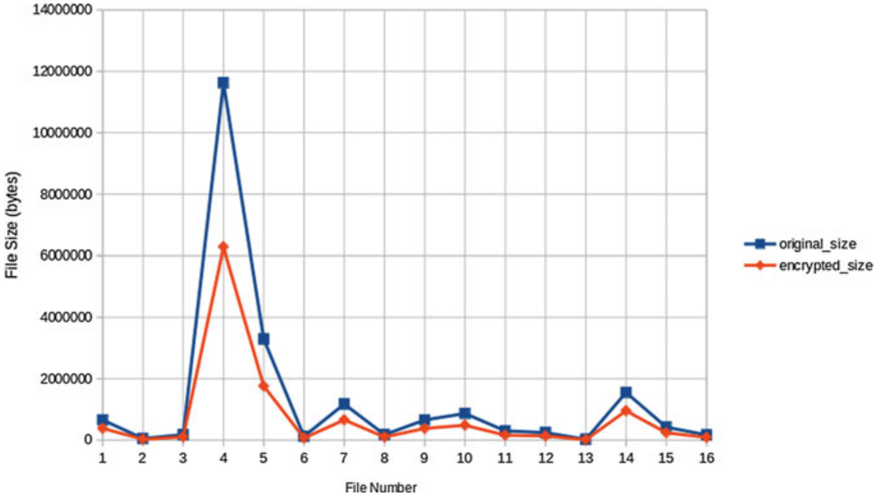

Fig. 2 Graph showing change in file sizes for and text files before and after encryption

the same file after encryption. The percentage change is calculated by calculating the difference between original file size and encrypted file size. The time taken to encrypt column shows the time required by the system to encrypt the file. In case of text files, the encrypted file size reduces by anywhere between 38 and 49%. This implies that after encryption, there is a reduction in the size of the file. The time taken to encrypt the files also varies proportionally with the original file size. The larger the file, more time it requires to encrypt. For very large text files, around 10 Mb, the time taken is around 20s (Tables 1 and 2).

Table 1 Details regarding encryption of image files

Original file size (bytes)	Encrypted file size (bytes)	Percentage change in size	Time taken to encrypt (seconds)
11,165	15,020	32.5275	0.0523400306702
4919	7512	52.7139	0.0245800018311
34,508,414	50,077,016	45.1153	157.187961817
15,478,214	22,462,464	45.1231	83.7759029865
860,513	1,239,724	44.0680	4.57197403908
71,706	104,448	45.6614	0.373322963715
3783	5464	44.4356	0.023008108139
23,744	32,768	38.0053	0.11828494072

Table 2 Details regarding encryption of text files

Original file size (bytes)	Encrypted file size (bytes)	Percentage change in size	Time taken to encrypt (seconds)
657,287	380,928	−42.04540	1.23898601532
52,139	29,356	−43.69665	0.112913131714
177,817	102,400	−42.41270	0.341831922531
11,626,439	6,278,488	−45.99818	20.0791721344
3,293,491	1,762,648	−46.48086	5.61558794975
123,783	66,904	−44.95057	0.21481900024
1,175,713	658,092	−44.02613	2.24571204185
177,817	102,400	−42.41270	0.409587144852
657,288	380,928	−42.04549	1.359126091
867,184	484,696	−44.10690	1.8191678524
300,788	160,428	−46.66409	0.596852064133
244,262	135,852	−44.38267	0.490957021713
25,267	12,972	−48.66030	0.075508117675
1,553,205	955,052	−38.51088	3.44151306152
421,335	240,300	−42.96699	0.833518028259
169,856	88,064	−48.15373	0.32085609436

For images, the size of the encrypted files increases. The increase in size is directly proportional to the size of the original file size. The percentage change in the image size after encryption lies in between 32 and 52%. The percentage change does not depend on the image size. There is no direct correlation between percentage change in size and the original size of the image. The time required to encrypt an image also directly depends on the size of the image. The larger the image, more time it takes to encrypt. The maximum time elapsed for image encryption is 157 s for a file of 32 Mb.

5 Conclusion and Future Enhancements

In this paper, we have proposed an efficient approach toward securing the sensitive data on IoMT devices. This will secure the data present on these personal devices by encrypting them; it will restrict any unauthorized third-party access to personal sensitive data. It also provides platform independence by backing up user data on a cloud platform and also synchronizes the data so that it is easily accessible through other devices with permission to access the data. This will also remove the vulnerability of the data being stolen from the cloud services as all the files are encrypted using every user's private key and secure the data overall. This will also introduce a level of opacity between the user and the IoMT manufacturer and also mitigate the possibilities of breaches into medical data storage systems.

The proposed work can be extended to a lot of other personal IoT devices and can be used for securing data on them.

References

1. Wu F, Wu T, Yuce MR (2019) Design and implementation of a wearable sensor network system for IoT-connected safety and health applications. In: 2019 IEEE 5th world forum on internet of things (WF-IoT), Limerick, Ireland, 2019, pp 87–90
2. Garg N, Wazid M, Das AK, Singh DP, Rodrigues JJPC, Park Y (2020) BAKMP-IoMT: design of blockchain enabled authenticated key management protocol for internet of medical things deployment. IEEE Access 8:95956–95977
3. Merabet F, Cherif A, Belkadi M, Blazy O, Conchon E, Sauveron D (2020) New efficient M2C and M2M mutual authentication protocols for IoT-based healthcare applications. Peer-to-Peer Netw Appl 13(2):439–474
4. Ferencz K, Domokos J (2018) IoT sensor data acquisition and storage system using Raspberry Pi and Apache Cassandra. In: 2018 International IEEE conference and workshop in Óbuda on electrical and power engineering (CANDO-EPE), Budapest, 2018, pp 000143–000146
5. Huang S, Chang H, Pan J (2014) Sensor dispatching methods for gathering data in rechargeable wireless mobile sensor networks. In: 2014 IEEE world forum on internet of things (WF-IoT), Seoul, 2014, pp 479–484
6. Thiyagarajan M, Raveendra C (2015) Integration in the physical world in IoT using android mobile application. In: 2015 International conference on green computing and internet of things (ICGCIoT), Noida, 2015, pp 790–795

7. Sarkar S, Gayen S, Bilgaiyan S (2018) Android based home security systems using internet of things (IoT) and firebase. In: 2018 International conference on inventive research in computing applications (ICIRCA), Coimbatore, 2018, pp 102–105
8. Elminaam DSA, Kader HMA, Hadhoud MM (2008) Performance evaluation of symmetric encryption algorithms. IJCSNS Int J Comput Sci Network Security 8(12):280–286
9. Coppersmith D, Johnson DB, Matyas SM (1996) A proposed mode for triple-DES encryption. IBM J Res Dev 40(2):253–262
10. Stallings W (2011) Cryptography and network security-principles and practices, 7th edn. Prentice Hall of India
11. Rivest RL, Shamir A, Adleman LM (1983) cryptographic communications system and method. US Patents, Patent No. US4405829
12. Ajay DM, Umamaheswari E (2016) An initiation for testing the security of a cloud service provider. In: Smart innovation, systems, technologies. Springer, Switzerland, pp 35–41
13. Nikolov N, Nakov O (2019) Research of communication between IoT cloud structure, android application and IoT device using TCP sockets. In: 2019 X National conference with international participation (ELECTRONICA), Sofia, Bulgaria, 2019, pp 1–4