Research Article

IOT BASED SINGLE IDENTIFICATION DATABASE MODEL FOR UNDER DEVELOPMENT COUNTRIES

Syma Kamal Chaity Md. Estiak Ahmed, MD. Tanzin-Ul-Islam, Samira Sobhan and Shahrin Chowdhury
Computer Science, American International University-Bangladesh,American International University-Bangladesh, Dhaka, Bangladesh, chaitysymakamal97@gmail.com, estiak97@gmail.com, tanzin.8897@gmail.com, samiramila100@gmail.com and shahrin.chowdhury@gmail.com

ABSTRACT
The Internet of Things is becoming one of the most primary topics of conversation in the World of information Technology. There is a huge revolution that comes with the internet of things. With its multi-disciplinary application growth, the Internet of Things has changed our lifestyle. In regular life, people need to provide their user information multiple times for creating any national or international document. In this paper, a simple central server-based database model is proposed to reduce people's struggle of providing the same information multiple times and also reduces the chance of redundancy of data. According to this proposed model, users need to provide their information only once, and can use the same information in multiple sectors. Users need to provide their identification number which is provided by the central server and fingerprint only to access previously stored personal data. Users can easily create or update any national or international document using those data. The goal of this proposed model is to make a central database model for people to reduce the hassle of creating or updating national or international documents.

Keywords— Biometric system, central database, IoT, central server modal, Fernet encryption.

I. INTRODUCTION

The emergence of the internet of things (iot) is the most progressive development in information and communication technology. Basically, it relates the connection between some physical objects and those embedded with sensors, software and other technologies. It indicates a system of interrelated, internet-connected objects that are able to capture and transmit data over a wireless network without human interaction. It can reach a broad range of devices that are not internet-enabled. They are activated and can connect with each other via the internet once the devices are already integrated with technology. This implies that they can remotely be tracked and managed. Most devices that have not been connected to the internet previously can be networked and react in the same way as smart devices. It increases the risk of losing privacy because of the transmission of data through iot. Although in the context of information technology, security issues are not new, the attributes of many IoT applications present new and specific security challenges. It must be a fundamental priority to resolve these challenges and ensure protection for IoT products and services. Users need to trust that IoT devices and related data services are protected from vulnerabilities, especially as this technology becomes more prominent and incorporated into our daily lives. Currently the use of IoT has increased a lot and gradually the reliance on it is also increasing day by day.

In our country, we need to provide the same personal information everywhere repeatedly which is a waste of time. This system helps to reduce the inconvenience of the general people. In our system, we tried to store all the information in a central server and wherever they need these types of information, they can easily collect that information from the central server. Here a person does not need to give the same information every time. They just need to provide additional information if that is not provided previously for storing in the central database. So, this system will reduce not only the troubles of a user but also it can reduce the wastage of time. Here, we also have covered the security issue of the data as the user has to provide personal information which is confidential. Another feature that we have implemented in the system is, accessing relevant information only. For example, the personal information which is required in the banking related works may not be essential for the hospital visit for health related issues. Here we have ensured that, when different organizations request for specific information, only that information will be provided by the central server and the information will be encrypted while sending back to the receiver which ensures confidentiality.

II. LITERAURE REVIEW

Parthasarathy Panchatcharam et al. have discussed the impact of Internet of Things in the field of Healthcare and also reviewed different parts of IoT based healthcare services as well as showed different health care network architectures based on efficient data transfer and several security issues [1]. Here, a detailed survey has been shown about the security issues in this platform. For handling MITM attack in IoT scenarios, a low latency high reliable security mechanism was implemented by combining Radio frequency fingerprint (RFF) technology with IoT application [2]. As security issues are most important in IoT platforms, a hybrid model has been proposed for securing the data transmission. 2D discrete Wavelet Transform steganography technique and their proposed encryption schema were used for developing that hybrid model. The proposed

hybrid model had higher PSNR value and Smaller MSE value that ensured better performance compared to other work in the same sector [3].

Now, IoT is widely used in healthcare platforms. Ensuring efficiency in the performance of IoT devices has become more important and for that reason a lightweight authentication scheme was proposed. Elliptic curve cryptography was used to ensure this feature and several attacks are handled by their lightweight authentication scheme [4]. For providing more features (reducing energy, less cost), they planned to create group-based authentication in future. The fundamental benefit of ECC is that it provides for the same level of security with a smaller key size than RSA, which saves processing overhead [5].

On the other hand, lightweight asymmetric cryptography is also used in some cases. For example: to handle software, hardware and network attacks. This can also establish mutual authentication by generating key pairs from the unique device ID. R Vijaysanthi et al. have proposed fingerprint authentication based on detailed matching is proposed in order to satisfy the authentication [6]. On the contrary, M-G, a SDN based data transfer security model was proposed by another group of researchers to manage dataflow so that stability and security of the network should improve [7]. For supporting elderly people who are living alone, an IoT based information system was proposed and evaluated by a case study of real-life scenarios [8].

III. PROPOSED METHODOLOGY

3.1 PROPOSED MODEL:

In this research, a simple central database system model is proposed for under-developed countries that have started adapting digitalization. In general, people need to submit their personal information every time a citizen needs a national or international document. So, in this work a simplified model is proposed so that citizens do not need to submit information redundantly. Login authentication of this model is based on fingerprint and user ID which is unique.
For each type of documents (i.e. passport, national ID card, etc.), there is a database model declared to the server end. So that only requested data will be provided to the specific organizations.

3.2 SYSTEM SPECIFICATION:

For creating and testing our model raspberry pie 4 is used which is a 4 GB version. For storage a 32 GB SD card is used. For collecting fingerprint data R305 fingerprint module is used. As an operating system, raspberry pi OS is used. This model user demo is built with python's web framework 'Django'.

3.3 Model layer:

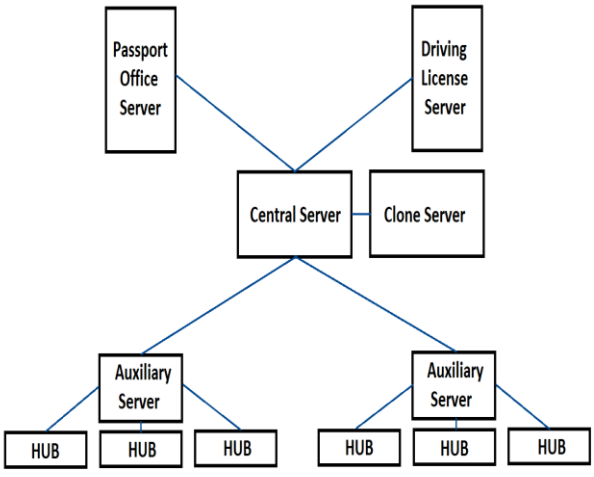

Figure 1: Model Layer

In the system, a citizen gives his/her information for the very first time. In this model, the whole country is divided into many local servers. In each local server there will be many hubs. When people submit their information, their information will be stored in a hub-based server. At the end of the day, the data collected from all hub-based servers will be transfer into the local server. From the local server data will be transferred into the central server. There will be a clone server created for the backup of the central server. In the central server, all data of a user will be stored. But for a specific national or international

document user will not need all the information. So, in this model a dedicated server will be created for each purpose. Like passport server, driving license server etc.

3.4 WORKFLOW

From two sections, the first one is storing data and another one is retrieving data. In the storing part, the user needs to give his/her fingerprint and other information for storing. In the retrieving part the user gives his/her fingerprint and ID, and all the information collected from the server.

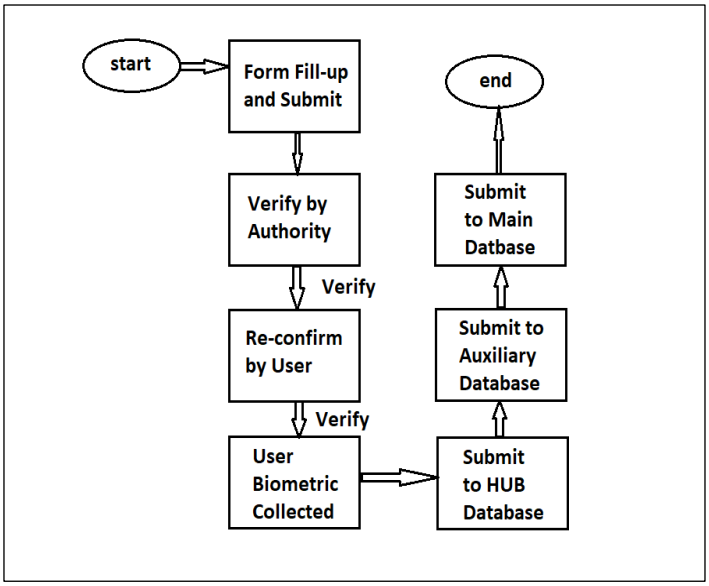

Figure 2: Workflow

3.5 STORING DATA

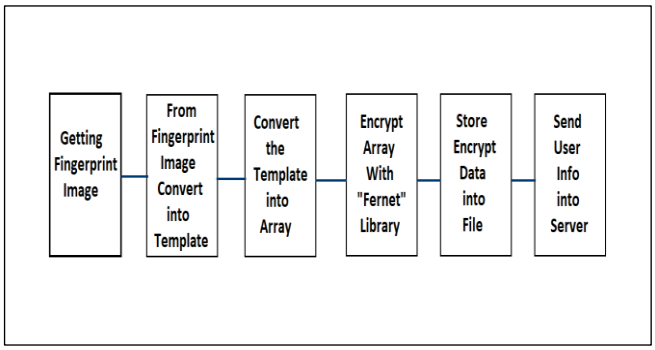

Figure 3: Data Store Process

In the storing section, the whole process is divided into three parts; getting fingerprint, encrypting fingerprint, write in a file and store in database.

3.5.1 GETTING FINGERPRINT:

The fingerprint sensor gives a 512-length array, which defines the user's fingerprint. For working purposes this fingerprint array needs to convert into a string.
At first the sensor tries to read the fingerprint image and if it is successful in reading the fingerprint image, then it will get fingerprint data from the (0x01) port of the sensor and convert the data into fingerprint data template object. At the end it will download the image data as an array from the template.

3.5.2 ENCRYPT FINGERPRINT DATA:

Earlier it was mentioned that the fingerprint sensor gives fingerprint value as an array. For the security purpose that cannot be stored directly. If the fingerprint is saved as plaintext it will be easily hacked by the attacker. For that reason, fingerprint data needs to be encrypted. In this model we have used an encrypting library of python which is "Fernet". This library encrypts the data with a secret key.

Fernet [9] is a symmetric authenticated cryptography library for python. It encrypts data with a URL-safe base64-encoded 32-byte key. It returns URL-safe base64-encoded data. Fernet is built on top of a number of standard cryptographic primitives. Specifically, it uses:

- AES in CBC mode with a 128-bit key for encryption; using PKCS7 padding.
- HMAC using SHA256 for authentication.

In this library, first a secret key will be generated; then the given fingerprint data needs to decode and add the secret key into the "Fernet" library object. Next, with the help of the "Fernet" library object the data will be encrypted. That's how the fingerprint data will be encrypted.

3.5.3 WRITE IN A FILE AND STORE:

The encrypted data is too large to store in the database. So, in this model fingerprint encrypted data is stored in a file. In the database, file name and the secret key of encryption is stored.

3.6 RETRIEVING DATA:

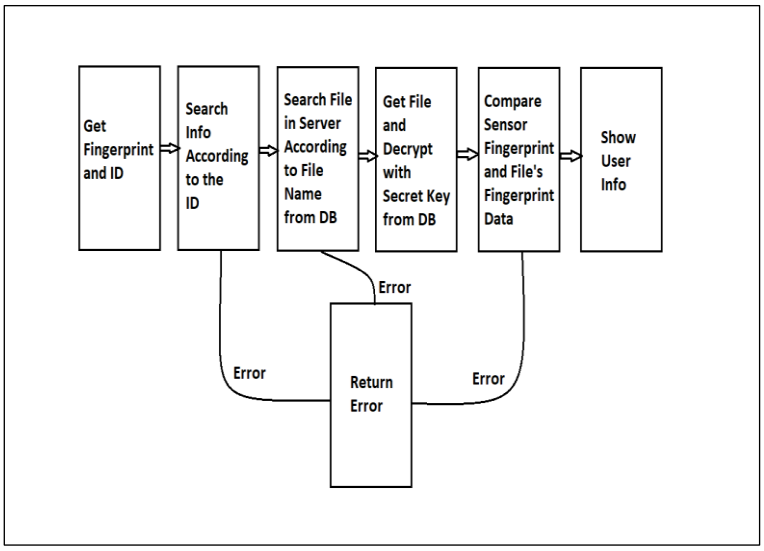

Figure 4: Retrieving Data from Server

All valid user information is stored in the database. When a user needs to create a national or international document like national ID card, passport, driving license etc. they need that data. To access the data users just need to provide their fingerprint and the ID number; the process will immediately start. The whole process is divided into following two parts:

3.6.1 GETTING USER DATA FROM SERVER

In the first step users need to provide their user identification number which was provided by the system when the user first time registered his/her personal information in any local server. After matching the ID with the database, the server will allow the user to provide their fingerprint. Subsequently successful match of the fingerprint data with the previous stored fingerprint, server will provide the user data as a response.

3.6.2 MATCHING FINGERPRINT DATA

Server gives user information according to the ID. With that server response file name and secret key is stored. Now with the file name, the user fingerprint file is activated and with the secret key that fingerprint data will be decrypted. Now there are two fingerprint data. One is given from the sensor and another one is received from the server. Upon receiving these two-fingerprint samples, sent to the fingerprint module to compare. Fingerprint module returns the result with percentage. When

the fingerprint data is matched; the system shows information according to the database model which is declared in the server end for the specific organization and there is an option to apply for the desired documents. With the help of the given secret key, file (encrypted fingerprint) data can be decrypted.

IV. ANALYSIS

This research was inspired from two biometric authentication systems; one of those is an improved voting system for a developing country. In that research previous biometric information of every citizen is stored under a unique ID (UID) and during election; when a voter enters the UID and looks into the camera or provides a fingerprint, the system authenticates the voter by matching previously stored fingerprint or facial recognition. If a match is found then the voter is able to vote otherwise the voter is reported as a fraud voter.

Another work in this biometric authentication field is 'Identity verification method using a central biometric authority' which performs biometric verifications to authenticate the identification of users using a central biometric authority (CBA) which allows parties to an electronic transaction to be assured of each other's identity.

In the first research work the proposed system was only implemented for voting [10]. But a similar kind of system can be implemented for applying to other government services like passports or driving licenses etc. Hence, our research proposed and implemented a system, where all the necessary data of the people of a country will be stored in a central database under a unique biometric specification and the central database will be able to provide limited access to the other service authority. Therefore, when a citizen will be in need to apply for a government service, he/she does not need to fill up any form manually; rather he/she can just verify themselves through biometric devices with the unique biometric entity stored in the central database. Also, through the proposed system the whole government services can be digitized.

In the second research the proposed system used a central biometric authority for authenticating the identification which is similar to the central database of this proposed system [11]. In this work for data transmission security an UMI (unique message identifier) is used which contains sender's id, receiver's id and a hash value. The hash value is used to ensure that the message/biometric has not been altered. But hash might have some security issues. With many advanced hacking tools, it is possible to crack hash within a couple of minutes. So, to get better data transmission security our system is using the Fernet encryption system. Fernet is a symmetric encryption that guarantees that a message encrypted using it cannot be manipulated or read without the key. Fernet is built on top of a number of standard cryptographic primitives. Specifically, it uses AES in CBC mode with a 128-bit key for encryption; it also uses PKCS7 padding.

V. CONCLUSION

In this paper, a proposed model with a simple central database has been presented; which is a simplified model that helps general people to avoid providing the same personal information redundantly. For identifying the users, unique id and fingerprint are used. This implemented system is divided into many local servers and the information of all local servers are stored in the central server. From the central server, different organizations (i.e. Driving License server, passport office server etc.) can get the information. Basically, two types of work are done in this model. First one is storing the data and another one is retrieving the data. Server provides information after comparing the given fingerprint and unique id with the previously stored fingerprint and id. For ensuring the privacy of the fingerprint data, a secret key has been used and the same secret key is used to decrypt the fingerprint data afterwards. This implemented system will solve the problem of input redundancy and assist the different organizations to easily access the central database and get that information according to their requirements. In future research, there is a plan to work with large scale data. As the system is still unable to identify duplicate data entry, in future a focus will also be on finding an efficient way for identifying and removing duplicate entries. In order to increase the accuracy; better fingerprint sensors can also be used and for large data sets latest encryption algorithms can also be examined to assure stronger security.

VI. REFERENCES

[1] Parthasarathy Panchatcharam, Vivekananda S. "Internet of Things (IOT) in Health and Surveillance, Architectures, Security Analysis and Data Transfer: A Review" International Journal of Software Innovation, Volume: 7, Issue 2, April-June 2019

[2] Qiao Tian, Yun Lin, Xinghao Guo, Jinming Wen, Yi Fang, Jonathan Rodriguez, Shahid Mumtaz, New security mechanism of high reliability IoT communication based on radio frequency fingerprint. IEEE Internet of Things Journal, 6(5), 7980-7987, 2019.

[3] Mohamed Elhoseny, Gustavo Ramirez-Gonzalez, Osama M. Abu-Elnasr, Shihab A. Shawkat, Arunkumar N, Ahmed Farouk "Secure Medical Data Transmission Model for IoT- Based Healthcare Systems" Open Access Journal- Special Section on Information Security Solutions for Telemedicine Applications, DOI: 10.1109, Volume: 6, May 2,2018

[4] Maria Almulhim, Noor Zaman "Proposing Secure and Lightweight Authentication Scheme for IoT Based E-Health Applications" International Conference on Advanced Communication Technology (ICACT), ISBN: 979-11-88428-01-4, February 2018.

[5] Bappaditya Jana, Jayanta Poray, "A Performance analysis on elliptic curve cryptography in network security. 2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE), 1-7, 2016.

[6] R Vijaysanthi, N Radha, M Jaya Shree, V Sindhujaa, Fingerprint authentication using Raspberry Pi based on IoT. 2017 international conference on algorithms, methodology, models and applications in emerging technologies (icammaet), 1-3, 2017.

[7] Yanbing Liu, Yao Kuang, Yunpeng Xiao, Guangxia Xu "SDN-Based Data Transfer Security for Internet of Things" IEEE Internet of Things Journal, DOI: 10.1109/JIOT.20`7.2779180, ISSN: 2327-4662, 2017

[8] Damain Dizal, Bartosz Jachimczyk, Wlodek j. Kulesza, "IoT- Based Information System for Healthcare Application: Design Methodology Approach" www.mpdi.com/journal/applsci, Appl. Sci. 2017,7,596; doi: 10.3390/app7060596

[9] Fernet Library https://cryptography.io/en/latest/fernet.html Acc: 01 December 2020.

[10] Yadav S, Singh AK. A biometric traits-based authentication system for Indian voting system. International Journal of Computer Applications. 2013 Jan 1;65(15).

[11] Nanavati S, Nanavati R, inventors; FusionArc Inc, assignee. Identity verification method using a central biometric authority. United States patent application US 11/761,734. 2007 Oct 4.