Original Article

Enhancing Data Security in Fitness Tracker Using HAN Algorithm

Pradeep Sudhakaran[1], M. Preetha[2], V. Sindhu[3]

[1]Department of Computing Technologies, School of Computing, SRM Institute of Science and Technology, Potheri, Kattankulathur, Chengalpattu District, Tamil Nadu, India.

[2]Department of Career Development Center, SRM Institute of Science and Technology, Potheri, Kattankulathur, Chengalpattu District, Tamil Nadu, India.

[3]Assistant Professor, Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu, India.

[1]pradeeps1@srmist.edu.in, [2]preetham1@srmist.edu.in, [3]sindhuv@skcet.ac.in

Abstract

There are some people who are interested in the Internet of things (IoT), which is a cutting-edge technology that people are interested in. People who use the Internet of Things like it because it makes them more aware, sends information reliably, and processes things quickly. People who build things should use small tools that don't have a lot of power. Typical encryption designs are very complicated because they have a lot of different parts. It takes a lot of time to encrypt, which hurts the energy of the devices. Amalgam encryption is a cutting-edge method that can be used in IoT. This type of encryption leads to a lot of surveillance and little data processing. In this work, we have scheduled to use the amalgam encryption approach which has been supervised so as to diminish safety perils and reinforcing encryption's speed and less calculation intricacy in a fitness tracker made for the army people which will track various health aspects of the army personals, encrypt the data using the hybrid algorithm and store it in the cloud which can only be accessed by giving the fingerprint of the registered officers in order to authenticate the user and keep the individual personals data safe. The fundamental idea of the project is to implement an IoT sensor network along with the security aspect of the data being the primary concern.

Keywords: IoT, Surveillance, Hybrid Algorithm, Privateness, Fitness Tracker, Dactylogram.

DOI: 10.47750/pnr.2022.13.S03.075

INTRODUCTION

Wellness is portrayed as the competence to do the day's training without superfluous vulnerability. However, with the rise of machines and changes in how people live, real well-being is seen as a measure of how well the body can work and rest, how strong it is, how well it can fight off lower motor activity illnesses, and how well it can meet deadlock situations. It was released by the US Department of Health and Human Services for people who are at least 3 years old. Advice based on science is given to people who want to move more and improve their health. These rules say that all grown-ups should move more and sit less during the day to improve their mental, enthusiastic, and physical well-being. For major health benefits, adults should do at least 150 to 300 minutes of tolerant-capability, 75 to 150 minutes of high-force oxygen-consuming physical activity, or an equal mix of both spread out over the course of a week. A new study says that episodes of any length add to the medical benefits of the total amount of actual action. This means that the proposal to make the actual action happen in 10-minute chunks has been scrapped.

A fitness tracker can now do more than just keep track of how many steps you've taken. Most of them come with a heart rate monitor, but a few of them also have SpO2 monitors that help you keep track of your blood-oxygen level. In this project, we're going to use IoT sensors to help us reach our goal of making a fitness tracker. Using the IoT devices, a sensor network would be set up. This network would have a main sensor that would record things like heart rate, calories burned in a day, number of steps walked in a day, track the sleep pattern, and other things. All of the data that was recorded would be encrypted inside the tracker using the simple and lightweight HAN algorithm, and then it would be sent to the cloud for long-term storage. People would be able to access the data in the cloud in a way that was safe. To get the data back in its original format, a fingerprint must be made. This fingerprint would include the decryption key for the HAN algorithm, which would be the fingerprint. It would only work if the fingerprint was already in the database, which would be done only for the people who needed it.

For example, the officer who needs to see his own data to figure out how healthy he is, or a senior officer who needs to see it to figure out how well he is. This means that you can get your data from the cloud on any mobile device with a fingerprint reader, such as a phone or tablet. It is the first step in this project for biometrics to be checked. When someone wants to get their health information, this is the key to unlocking and unlocking the person's information. It also serves as a computerized signature, which helps to verify the client. Everybody but a very small number of biometric users now has two stages. In the first step, biometric blueprints are sent to a group of people who are in charge of things. An end user's ID number will be linked to the biometric blueprints.

PROPOSED METHOD

Internet of Things (IoT) developers can utilise "amalgam" to encrypt data. The amalgam encryption method is used in the Internet of Things (IOT) to protect messages, slow down information sharing, and prevent hacking. This paper examines HAN, a type of encryption. In terms of encryption and decryption, the proposed approach has unique qualities, such as how fast it is to produce keys and how it might improve web security in a variety of ways, such as employing a computerized signature. Misbehavior: Equipment and gizmos are processed as if they were depicted in the flowchart.

Steps of the cryptography are in this manner:

- The shopper or the enlisted official has an open key that's made by the relative encryption.
- At this minute all the wellbeing data which are fundamental to be scrambled will be coordinated to the unbalanced calculation by the open key or the unique finger impression.
- Later, the wellbeing data is scrambled by unbalanced encryption strategy and will be coordinated to the cloud/database.
- The database will store all the different fingerprints which is able be enrolled, and the information can as it were be gotten to when the person gives his unique finger impression once more and it is display within the database.
- Operators cannot hypothesize the key word of gadget as the key required to decode the information is the unique mark which is onliest for each individual.
- The receiver uses the open key and the scrambled material to try to decipher information from the sender. Here, we'll offer a new amalgam computation that ensures access and increases the speed of key creation, encryption, and decryption, among other things.

A. Creating a Key

Two 4 × 4 lattices, known as remain and key, are used to abdicate the key for encryption by using AES key fructification. H is an open key that may be exported in XOR activity. We will select a space from the state cross section and a key from the key system and an open key of H.

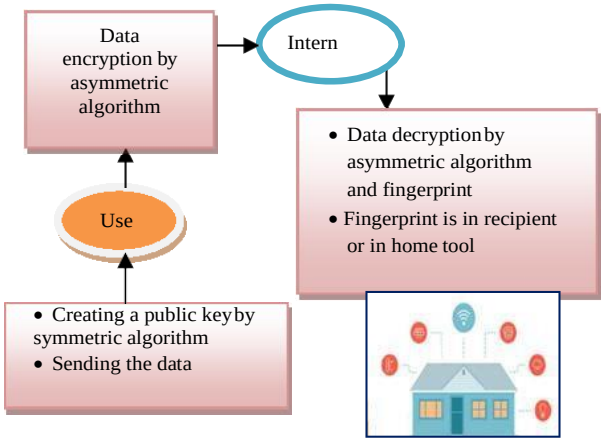


Fig. 1: Usage in IOT - HAN

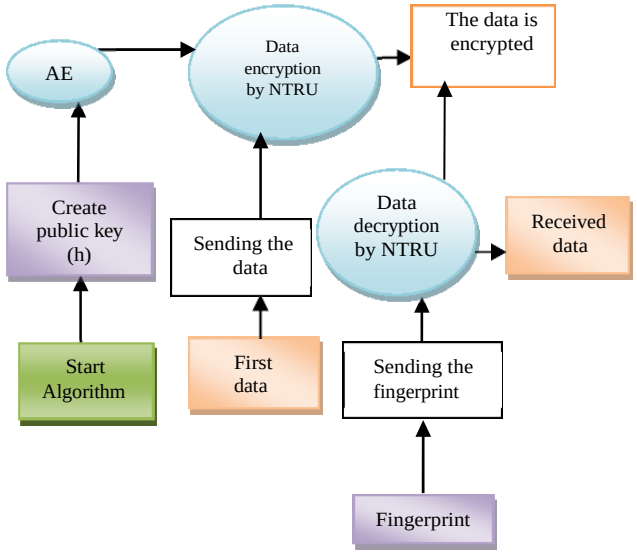


Fig. 2: Steps for sending public key in HAN

The AEC approach is used to decide this phase of the HAN approach. The hexadecimal value of the letter h is represented by the shaped key of h. At this moment, the open key 'b' is generated. When sending separated information from the tracker to the cloud/database, the goal is to ensure that each unique finger impression is fairly seen by the cloud/database and that each open key is fairly observed by both the tracker and the cloud/database. As a result, the encryption approach must have a strong reconnaissance component. It suggests that the jumbled information generated by the exporter will be delivered to a cloud/database that is both mysterious and secure in nature. As a result, NTRU deviating encryption

is beneficial in increasing the level of surveillance. When the transmitted data from the tracker is scrambled, it should not be susceptible to interception by a third party.

B. Encryption

Let's pretend that data is being transferred from the tracker to the cloud or database. This information is stored in a multinomial referred to as 'n'. Following the creation of a multinomial 'n,' the tracker selects a fingerprint as a multi nominal, such as 'a,' from a database of acquired fingerprints that is identical to the sender's fingerprint, such as Kr.

It should be highlighted that we can obtain the data by the use of several nominal r. As a result, it should not be disclosed to the sender.

$$E = Qr \times b + n \quad (1)$$

Equation 1 is data that will be transmitted to the cloud/database as an encrypted message.

C. Decryption

During encryption, the client makes an attempt to open the text using their unique mark or to scramble the information in some other way. The NTRU computation will be used half-way through the HAN calculation process for message unscrambling. The recipient has both secret keys: g and gp, one of which is used to structure the helter-skelter encryption and the other which is used to distinguish their distinctive mark. True, gp is spoken with a multinomial of g, therefore it is reasonable to assume that it will be g * gp = 1, and the cloud/information base recipient increases the information with respect to the unique mark that is given beneath with the boundary c, as shown below:

$$c = g \times E(2)$$

$$c = g \times (Qr \times b + n)(3)$$

$$c = g \times Qr \times b + g \times n(4)$$

It is necessary to choose coefficients of the polynomial equation that are somewhere between -q/2 and p/2 in order to determine the appropriate boundary. As a result, when K = 3, it drastically drops in size and has no effect on the cycle, allowing us to cut the associated link completely.

$$Qr \times b = 0(5)$$

$$c = g \times n\ (6)$$

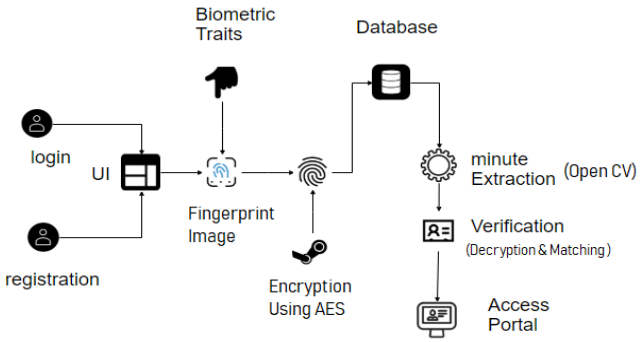
The boundary d will be determined in the following stage. Simply copy and paste the private key f from the tracker's initial message into the body of the message.

$$c = d = g \times n\ (7)$$

$$D = (gpxd)/y^2\ (8)$$

When we employ Decryption Data, we can be confident that the information will reach the intended recipient safely and without disruption.

D. Digital-Signature



The following is a diagram of the project's architecture. The Fingerprint Scanner is used to perform biometric authentication on the user's hands. At the time of registration, biometric features are encrypted to prevent unauthorized access. While the template is being saved in the database, you can use it. Using the unique id granted to it, that template is retrieved at the moment of login, and the template is then decrypted on the user's computer.

Only when the minute extraction has been reviewed and found to be in compliance with the template can the user gain access to the portal; otherwise, access is prohibited.

Steps are:

1. An image hash of the user's fingerprint is made first, and then a unique ID for that person is generated using the image hash of the fingerprint.
2. This hash will be utilised as a key in the second stage of the HAN algorithm, which will be completed in the third stage. 3.
3. The final step involves putting this hash code in the cloud/database, as previously mentioned.
4. In step four, when an individual attempts to access (login) to the data using his or her unique ID and by scanning their finger print again, a hash code for that individual will be generated, and the server will retrieve the registered fingerprint hash code from the cloud/database using the user's unique id.
5. . The server will now compare these hash codes, both the one that was stored in the database at the time of registration and the one that is generated everytime the user attempts to log into the system.
6. The encrypted data will be decrypted at the user's end, and the user will be granted access if both codes are within a particular threshold.

In order to register, the user must supply a unique ID, which serves as his or her username, and with this username,

biometric traits are deemed to be the system's password, which is stored in a database. This is referred to as a biometric characteristic in this context, and fingerprint scanning is one such characteristic. A hash code is generated from a biometric attribute, such as a fingerprint trait, on the user's end at the time of registration and the hash code is then saved in the database. The hash code for the fingerprint image may be obtained right here.

When compared to a normal string user id or password, it has a greater number of lines. When a user attempts to log into the system, he or she must provide a username and fingerprint as a password. With the help of the username, the hash code of the image fingerprint is fetched from the database and it is decrypted at the user side, resulting in a squeezed text of a specific number of lines (similar to the number of lines in the Normal Fingerprint Image String) being obtained, which is compared and if similarities are identified, the user is authenticated and is granted.

We'll be using picture hashing instead of cryptographic hashes (such as md5, sha-1, and so on) due to the fact that some of the images in my needle or bundle heaps may have been marginally modified, including possible JPEG artefacts. We'll be using picture hashing instead of cryptographic hashes (such as md5, sha-1, and so on). As a result, we should rely on our perceptual hashing calculation, which is capable of dealing with minor variations in the input images. Overall, the flow of this code block is nearly comparable to the one that came before it:

- We stack the picture from disk (whereas guaranteeing it's not None)
- Convert the picture to grayscale
- And compute the picture hash

$$E = (n \times g)/y^2 \quad (9)$$

$$D = ((\ b/2*gp*En) \times b)/2 \quad (10)$$

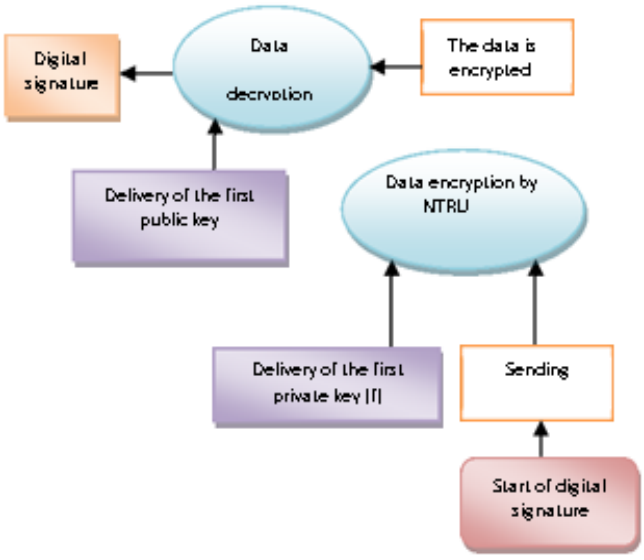


Fig. 3: Digital signature steps

RESULT

HAN calculation has been recreated by MATLAB programming, so it is contrasted and two calculations of AES and RSA to check rapid of the calculation in encryption measure.

The outcomes are given in Table I.

TABLE AUX I

Approach	Time period for achieving the whole approach per unit
HAN	0.321081
AES	2.718182
RSA	2.350752

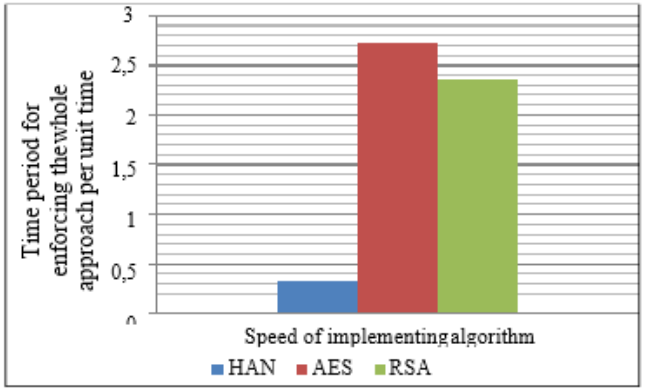


Fig. 4 two different encryption approaches

A computerized mark is raised to scrutinize the security advancement in this calculation, lastly, the quickness of the computerized verification has been contrasted and two different calculations that did not used computerized verification. The outcomes show that the speed of the proposed calculation even with a computerized mark is higher than the two others, and that is the reason calculation is useful.

TABLE AUX II: APPLICATION TIME OF DIGITAL STAMP IN SUGGESTED APPROACH

Approach	Total time algorithm implementation (sec)
HAN by digital stamp	0.58
AES without digital stamp	2.718182
RSA without digital stamp	2.350752

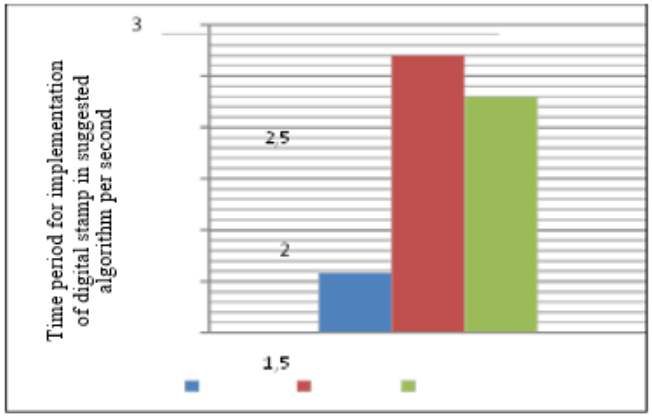


Fig. 5: Different two approaches omitting digital stamp

Closure

In this section, we discussed the Internet of Things, including its presentation and application, statistics, tactics, and security systems, as well as the encryption calculation for the Internet of Things, on which scientists have previously focussed. Additionally, we looked into the recommended technique for mixture encryption calculation, which is used in the Internet of Things. We presented a potential technique for improving the Internet of Things through the use of mixture encryption calculations. To develop the Internet of Things, the HAN calculation is a proposed technique, which is a combination of AES proportional encryption calculation and NTRU lopsided encryption calculation for IoT advancement. This calculation has to be done quickly in order to generate a key, perform encryption and unscrambling, and provide sufficient monitoring in the Internet of Things. The security of this calculation is due to the use of a multinomial in the encryption and decoding processes, as well as the use of an advanced mark to produce the correct text. Because of the low level of financial complexity, this calculation only consumes a little amount of memory. This computation makes it possible to use encryption in the Internet of Things with a low number of attacks and revised surveillance.

REFERENCES

Muhammad Usman, Irfan Ahmed, M. Imran Aslam, Shujaat Khan and Usman Ali Shah, "A Lightweight Encryption Algorithm for Secure Internet of Things", IJACSA, 2017

R. Davice, "The Internet of Things Opportunities and challenge", European, p.p.1-8, 2015.

G. Price, "The Internet of Things 2015", State of THE Market: Internet of Things 2015, Verison wireless company p. p1-24, 2015.

Deris Stiawan, Mohd. Yazid Idris, Reza Firsandaya Malik, Siti Nurmaini, Rahmat Budiarto," Anomaly Detection and Monitoring in Internet of Things Communication", ICITEE,2016

Y. Challal, E. Natalizio, S. Sen, and A. Maria Vegni "Internet of Things security and privacy: Design methods and optimization", Add Hoc Network, vol.32, Science Direct, p.p1-2, 2015.

Ch. Qiang, G. Quan, B. Yu, L. Yang, "Research on Security Issues of the Internet of Things", International Journal of Future Generation Communication and Networking (IJFGCN), vol.6, NO.6, IEEE, pp 1-10, 2013.

R. Weber, "Internet of Things New security and privacy challenges", Computer and Low Security Review, vol.26, issue1, Science Direct, p.p. 23-30, 2010.

Brinzel Rodrigues, Rushikesh Pawar, Pranay Patil, Ankit Gour," Encryption and Decryption of Biometric Traits", IOSR-JCE,2019

F. Olivier, G. Carlos, N. Florent "New Security Architecture for IoT Network", Procedia Computer Science, vol.52, Science Direct, p.p1028- 1033, 2015.

M. Xin, H. China "A Mixed Encryption Algorithm Used in Internet of Things Security Transmission System", International Conference on Cyber-Enabled Disributed Computing and Knowledge Discovery, Xian, IEEE, p.p.62-65, 2015.

Mohammed El-hajj, Maroun Chamoun, Ahmad Fadlallah, Ahmed Serhrouchni," Analysis of Authentication Techniques in Internet of Things (IoT)", CSNet,2017

A. F. Skarmeta, J. L. Hernandez, M. V. Moreno" A decentralized approach for Security and Privacy challenges in the Internet of Things", IEEE Word Forum on Internet of Things (WF-IOT), Seoul, IEEE, p.p.67-72, 2014.

N. Hong, Z. Xuefeng, "A Security Framework for internet of thingsbased on SM2 cipher algorithm", Fifth International Conference on Computer Science and Network Technology, Shiyang, Hubia, China, IEEE, p.p13-16, 2013.

R. Arbia, Ya. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah. "A systemic approach for IoT security." In 2013¬ IEEE International Conference on Distributed Computing in Sensor Systems, p.p. 351-355. IEEE, 2013.

L. Yuan Zeng, "A Security Framework for Internet of Things Based on 4G communication,-2nd International Conference On computer Science And Network Technology, Chanchun, China, IEEE, p.p1715-1718, 2012.

S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, "Proposed embeded seurity framework for internet of things", 2nd International Conference on Information Theory and Aerospace & Elentronic Systems Technology, Chennai, IEEE, p.p.1-5, 2011.

K. Nur Prasetyo ST, Y. Purwanto, and D. Darlis. "An implementation of data encryption for Internet of Things using blowfish algorithm on FPGA."In Information and Communication Technology (ICoICT), 2014 2nd International Conference, Bandung, p.p. 75-79. IEEE, 2014.

SB. Vinayaga, M. Ramnath, M. Prasanth, and V. Sundaram. "Encryption and hash based security in Internet of Things." In Signal Processing, Communication and Networking (ICSCN), 2015 3rd International Conference, Chennai, p.p. 1-6. IEEE, 2015.

P. Xu, Li. Min, and He. Yu-Jie. "A hybrid encryption algorithm in the application of equipment information management based on Internet of things." In 3rd International Conference on Multimedia Technology (ICMT-13). Atlantis Press, 2013.

Amirhossein Safi, "Improving the Security of Internet of Things Using Encryption Algorithms", IJCIE,2017

R. Wuling, and Zh. Miao. "A hybrid encryption algorithm based on DES and RSA in Bluetooth communication." In Modeling, Simulation and Visualization Methods (WMSVM), 2010 Second International Conference on Sanya, p.p. 221-225. IEEE, 2010.

R. Jha, A. Kumar saini, "A Comparative Analysis & Enhancement of NTRU Algorithm for Network Security and Performance Improvement", International Conference on Communication Systems and Network Technologies, Katra, Jammu, IEEE, p.p.80-84, 2011.

Ibrahim, S. (2022). Commutativity of high-order linear time-varying systems. Advances in Differential Equations and Control Processes, 27, 73-83.