University of Sindh Journal of Information and Communication Technology (USJICT)
Volume 5, Issue 4, December 2021
ISSN-E: 2523-1235, ISSN-P: 2521-5582

Website: http://sujo.usindh.edu.pk/index.php/USJICT/

Role of IoT in protecting wearable gadgets

Sana Fatima1, Laviza Falak Naz2
Department of Software Engineering
NED University of Engineering and Technology,Karachi
sanafatima@cloud.neduet.edu.pk1

Abstract: Out of the most entrusted technological revolutions applied for the advancement of living standards and creation of a more convenient operation in the professional world, the Internet of Things (IoT) has been progressing at the highest projected pace. The interconnectivity of gadgets and devices over the internet to produce smarter control, communication, and a swift and easy lifestyle makes it an amazing tech introduction. However, the IoT also brings along a huge flow of privacy and security concerns whilst considering the huge inflow of data breaches and cyberattacks in the network data. The advancements in the security protocols of the data thus bring along a mistrust among the users of IoT networks who might then no longer wish to be a part of this technological revolution. Therefore, it is important to maintain security assurance in the IoT based connection networks of wearable gadgets. This paper discusses the symmetric and asymmetric approaches of encryption over IoT which can help protect the network of smartphones connected to the wearable to assure a safe and smart data commute and avoid access to private data over the same internet connection.

I. INTRODUCTION AND BACKGROUND

There are now numerous features of present day life in the Internet of Things (IoT) and the majority of the areas around the world. IoT presents to us an existence where shrewd items are associated easily into a worldwide organization and where wise articles speak with one another or the outside climate to offer new administrations and progressed measures without human impedance. It was recognized as the following "Mechanical Revolution," which would impact our lives as pioneers, laborers, general society, and clients. IoT has a phenomenal reach. The Internet of Things is a center segment of computerized change that permits organizations to change their method of working [1]. It causes associations to figure and evade administration interferences by checking and perceiving the productivity of their offices. It energizes policymakers in the entirety of their state and public offices to get ready and offer more intelligent, faster, and less fatty projects. The assortment of information from innumerable comparative subjects, just as other information sources inside your undertaking, to settle on more intelligent choices and asset new projects, shape the focal point of the weight delivered by IoT [2]. The procedure from CGI 'little then enormous' helps you in recognizing and meeting your IoT objectives through the measures in question:

- Find out what is conceivable at workshops and move workshops and ponder the interesting difficulties.
- The significance of the innovation is outlined in business-driven use cases. They are provided in a manner that can be determined to satisfy the standards of compelling creation sending [3].
- The information from the first use case will assist with characterizing where possible advantages from other information sources and different instruments can be removed. At that point this can be consolidated and downsized.
- This iterative methodology encourages you to construct a customized way map in light of your staff and cycles [4].

A. Challenges in the world of Wearable IoT gadgets

IoT-empowered wearables are keen instruments that can be utilized as outside connections, embedded in garments, infused into the body, or even inked on the skin. These machines can associate with the web for the preparing, transmission, and getting of data which can be utilized for savvy choices. These wearables have become an inexorably significant part of IoT innovation, developing from brisk assistants to more reasonable and progressed applications [5]. For

registering and systems administration purposes, keen wearables may speak with an assortment of different gadgets, for example, cell phones. As human and creature adaptability guarantees, savvy wearable gadgets are progressively essential so they can catch and communicate information out and about and furthermore acquire Internet data that lets them settle on astute choices.

The progression of wearable advances has been encouraged by improvements in low force cell organizations, diminished electronic gadgets and sensors just as the advantages that savvy wearables may give. We have seen a quick advancement as of late in clever wearable gadgets focused to assorted applications [6]. Any of the wearables intended for different utilizations incorporate savvy watches, wrist groups, eyewear, earphones, earbuds, body ties, foot, and hand-worn apparatuses, and brilliant gems.

For some applications, wearable IoT innovation can offer unlimited chances. Be that as it may, when a streamlined IoT gadget is accessible, the genuine intensity of wearable IoT can be reached. Therefore, latest examination papers are associated with the Internet under one of the two structures beneath. Second, wearable IoT can move the information for conceivable, disconnected preparing to the Internet or a worker or cloud [7]. The wearable IoT is held. The subsequent technique is the convenient PC to release any of the calculation. In this way the wearable IoT gadget moves its information to the Internet, which permits the IoT gadget to gather some data to permit the IoT gadget to work. In the event that we fuse IoT frameworks and address a scope of issues encompassing control of information, information sharing practices, security, and assurance, the expansion of wearable IoT can be totally perceived [8].

B. Approaches to enhance IoT connections

Remote frameworks are utilized by all wearable IoT gadgets to advance their detected information to another hub, entryway, or base station. This radio recurrence correspondence requires radiation that could antagonistically influence the strength of the customer on the grounds that the handset receiving wires are so near the body. Radiation dangers might be significantly more prominent among such wearables that are worn on the head and eyes. Because of lightweight and less force utilization plans, the complexity of wearable IoT gadgets is regularly limited [9]. In this way, highlights of insurance on these gadgets might be less solid. The plan of security conventions while keeping up the intricacy of the framework as meager as conceivable is one of the issues of wearable IoT frameworks. When all is said in done, because of awful security and wellbeing, wearables are essential hacking targets.

The on-going sharing of individual data, for example, basic finishes paperwork for wellness, measurements, and positions between the wearable and the IoT center point will make an air for infringement of protection. Normally, wearable IoT gadgets can be immediately found by different hubs in the organization in transmission mode. On the off chance that the pertinent protection strategy isn't upheld, unapproved hubs will take individual information [7]. In such transmission modes, IoT gadgets couldn't have the option to ensure the security of individual information against bargains through incorporated equipment encryption advancements. An IoT broadcasting endorser model where clients' very own data is just common with foreordained hubs, for instance, medical care administrations or client affirmed items [4].

C. Methods to Encrypt data over IoT

This proper encoding cycle or DES is managed by the NIST. To encode and decode documents, DES utilizes a similar encryption key. A similar private key must be utilized to both sender and beneficiary. The unevenly significant calculation, the last is known. DES is less steady than the AES, which is the principle differentiation among DES and AES. DES is credited to the US government's 30-year mission to furnish all administration correspondence with cryptographic securities. The point was both encryption security and normalization. DES is the establishment of encryption; nonetheless, scientists have since been broken [10].

AES utilizes a solitary, variable-length encryption key. Contingent upon the key size, the AES calculation focuses on a solitary square of information. AES follows the USA by utilizing a clinical framework connected to the web. Legal information protection models of HIPAA. AES likewise satisfies FINRA's monetary data protecting necessities. Indeed, even with its center length

decisions, AES is a powerful and exquisite calculation. The more drawn out the key length, the harder it is to break encryption dramatically [11].

This calculation is a type of electronic encryption, with three passes for each square of information. The more drawn out key length offers extra assurance. The NIST, which took the previously mentioned AES, was supplanting the triple DES. Triple DES is presently considered repetitive and as a result of its similarity and adaptability, is as yet utilized for some IoT items. Triple DES is effective at protecting against assaults by beast power. Savage power is an extensive exertion by persistent preliminary and exertion (in spite of scholarly systems). Beast power assaults utilize programmed instruments to figure various varieties before the programmer separates the key [12].

Named after Rivest, Shamir and Adelman, RSA encryption makes use of RSA Data Management as a way to ensure creativity in public-key encryption and also includes radical packages. Encoding RSA allows consumers to send encoded data without expecting a change of code from the collector in advance. The public key provides a unique identity to the data being encrypted and can only be decrypted using a similar function. The method to obtain a key is known to every node of a network to ensure that the system is being performed finely [13].

Over 20 years sooner, Counterpane Labs recommended another square code calculation. Twofish is a choice finalist however has not been picked as the new NIST Advanced Encryption Standard. Twofish utilizations a square chip gadget dependent on a solitary key up to 256 pieces long. On PCs with less limit processors and keen IoT savvy cards, this encoding standard is fruitful. Twofish is utilized in numerous items, for example, VeraCrypt with the expectation of complimentary encryption [14].

The paper [17] shows an implementation of blockchains node checkpoints in the IoT system which can provide an easier interface for a better hold over the system capabilities. There is a need to protect the nodes during the wireless connection of mobile phones and smart watches to ensure that there is a safe communication among the two useful nodes and other nodes over the same network doesnt have any access to the system. Besides having a secure blockchains, there is an immense need of having a customized encryption every time the data is connected over specific nodes on the network to ease the communication and thence, promote security.

II. METHODOLOGY

Considering the IoT based framework appeared in Figure 1, the accompanying framework comprises of IoT gadgets, for our situation, the gadget is wearable savvy. To speak with one another, the gadgets will require a worker, entryway and client gadget which is Mobile telephone for our situation. The principle parts of IoT gadgets are by and large sensors, actuators and miniature regulators or microcomputer. Here, the entryway goes about as a transmitter between the client and the worker. The passage on which these gadgets are associated is Bluetooth. While, the worker goes about as a safe of the data which is being gathered by the sensors in IoT gadget just as it sends the data over the web. The cell phone will be utilized for controlling the gadget since it gives an interface to the client for observing reason. The correspondence between the two gadgets will be noticed.

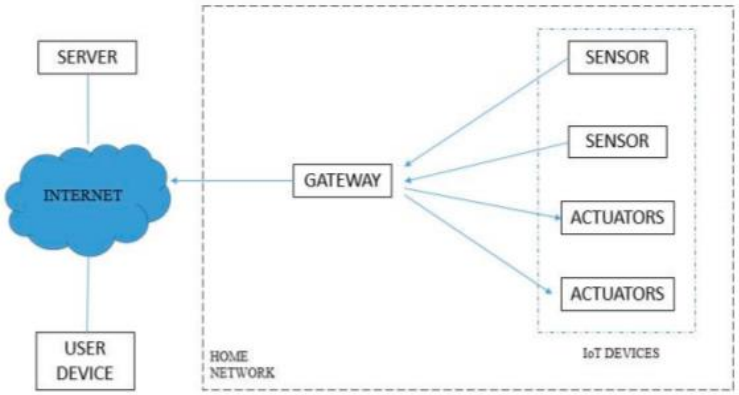

Figure 1 - IoT system configuration

A. PROPOSED TECHNIQUE

The methodology proposed is intended to create an easier data commute over the IoT-based networks. The two nodes of an IoT network should be capable of independently sharing the data without fearing a scarcity between other nodes. Internet data protection was still a concern. This paper aims to provide a safe communication technique with numerous algorithms to robust the network against

security attacks and infringements of data. The methodology suggested is a combinatory algorithm for the transfer of information and message in Symmetric and Asymmetric cryptographic techniques.

1) Symmetric Key Cryptography

The key symmetrical algorithm for encryption of the plains and for decrypting cypher text is the cryptographic algorithm sort used by the same key. The downside of these algorithms is that both parties have access to the secret cryptographic key which results in a key violation.

2) Asymmetric Key Cryptography

This type of encryption uses two keys:

- Public key (generally accesible)
- Private key (User accesible)

The public key is used to encrypt plaintext, whereby the holder decrypts the cypher text with a private password at the receiving end.

B. VIGNERE CIPHER

As the asymmetric cryptographic algorithm is used in the proposed methodology. An updated Vigenere Cipher version of the symmetric algorithm is used in this method.

1) Methodology at Sender's End

Followings steps will be followed at the sender end to secure the process of communication.

1) Fetch key using time stamp
2) Create a key using the obtained timestamp
3) Fetch the data to b encrypted as P
4) Obtain the data P which is to be transmitted.
5) Obtained the cipher text T by applying the method of Vigenere cipher
6) Create a key for the receive to ensure the system can communicate
7) Apply RSA on the receiver and the sender to ensure more security
8) Add the data of RSA and Vigenere cipher to create more encrypted version
9) Data can now be transmitted to M node.

The flow of the Sender's end is elaborated in the Figure 2.

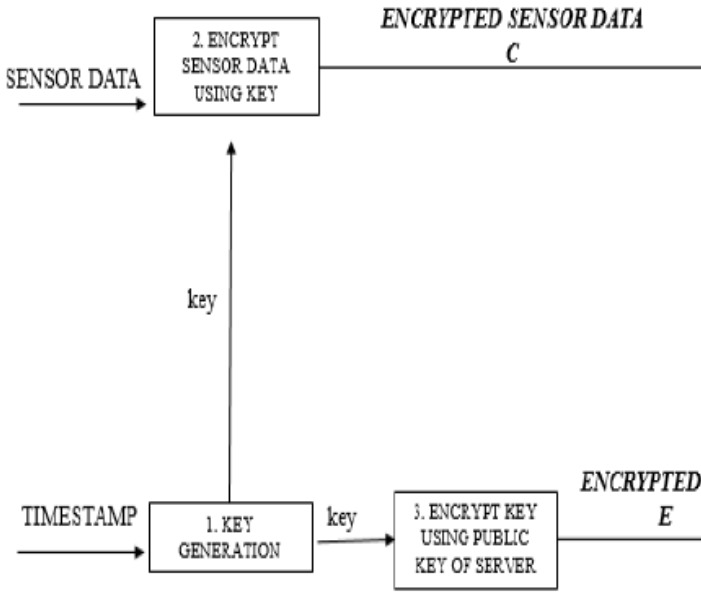

Figure 2 - State machine illustration for Sender's End

2) Methodology at Receiver's End

The following steps will be taken at the receiver's end to ensure the security of the communication.

1) The receive will receive the enhanced encryption version containing cipher text of RSA and Vigenere cipher.
2) Separate the two parts of the term
3) Use the RSA random key to decode the RSA part
4) Use the random key to decode Vigenere part

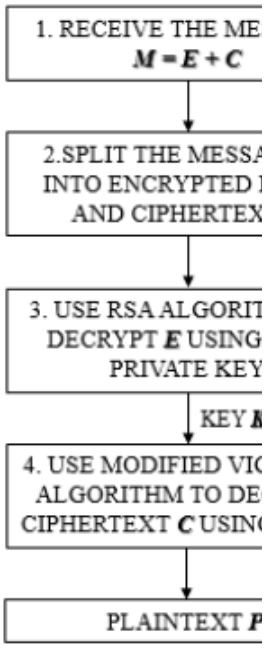

Figure 3 - State machine illustration at Receiver's End

C. THE VIGENERE CIPHER

A French diplomat Blaise de Vigenere designed the Vigenere Cipher in the 16th century. Vigenere Cipher is a type of textual encryption. It uses a basic flexible replacement form. Any cypher that uses more than one substitution alphabet is mostly substitution based on a multiple alphabet. In the Vigenere table or Vigenere table, the encryption of the plain text is achieved.

- The table contains alphabets written in 26 rows of instances each cyclically moved left, equivalent to 26 Caesar Cyphers conceivable, according to the previous alphabet.
- The cypher uses a separate alphabet from one row at multiple points in the encryption process.
- The alphabet used is based on a repetitive keyword at each step.

1) Algebraic Description of Vigenere Cipher

Here is the Arabic demonstration of Vigenere cipher

- Let N be the number of individual characters in the data.
- Assume that the nuber of characters are placed as an array from index 0 to (N-1)
- For a key ***K*** of size ***m***, encryption E using the Vigenere cipher
- Follows steps
  - ***Ci = Ek (Mi) = (Mi + Ki) mod N***
- Find decryption key D using the K:
  - ***Mi = Dk (Mi) = (Ci + Ki) mod N***
- Where M = M1 M2 … Mn is the message of length ***n***
  - C = C1 C2 … Cn is the cipher text
  - K = K1 K2 … Kn is the key obtained by repeating
- [n/m] times, where ***m*** is the length of the key. [15]

2) Limitations or Drawbacks of The Vigenere Cipher

The Vigenere cypher turned out to be much easier to break in recent years with the introduction of the machine. In a couple of seconds most cypher texts can be broken even though they have long keys. This chip has now lost its value, since it is known to be very easy to crack and gives quite much less protection in accordance with the present standards.

D. THE MODIFIED VIGENERE CIPHER

The modified Vigenere algorithm for Encryption is as follows:

1) let P be the data to be encrypted.

2) Let N be the number of individual characters in the data

3) Let K be the random key

4) Let R be a randomizing value (R = 1 XOR R = 0))

5) If R = 0;

C[i] = (P[i] + K[i]) mod N

6) If R = 1;

a. Let I.be the Randomizing Index (I = 2 XOR I = 3 XOR I = 5)

b. uses the following steps: -

i. loop over through all characters of the P with i

ii. If I % i = 0 (Remainder is 0);

C(i) = [P(i) - K(i)] mod N

iii. if not, (else condition):

C[i] = (P[i] + K[i]) mod N

Now at a fixed position, concatenate the randomizing factor R and the Randomizing Index I, can be implemented at either at the start or at the end of the encrypted message or cipher text. It is a very important step as these values are essential for the decryption process.

Follow these steps:

- Let V be the received data with R, I and C (Not K)
- Let N be the number of individual characters
- Produce K (Random key)
- Check the value of R

a. if R = 0

use Vigenere decryption

C[i] = (P[i] - K[i]) mod N

b. if R = 1;

the next character indicates the value of I

a. considers I as index.

b. follows these steps:

i. loop over to the data characters of V individually with i.

ii. if I % i = 0 (remainder is 0):

C(i) = [P(i) + K(i)] mod N

iii. else,

C[i] = (P[i] - K[i]) mod N

E. ***RSA ALGORITHM***

RSA was developed by Ron Rivset, Adi Shamir and Leonard Adleman in 1977, as a cryptographically algorithm. The goal was to replace the less efficient framework algorithm of the National Bureau of Standards (NBS). The biggest drawback of RSA is that it uses the digital signatures and the public cryptosystems. Diffie Hellman described the principle of such an algorithm a few years ago, but he could not fully implement it The guiding cause of RSA was the work of Diffie and Hellman.

At the time of paper mail and the age of electronic mail was soon to commence, RSA was initiated.

1) Implementation of RSA Algorithm

Two important ideas were implemented by RSA

a) Public key Encryption

Until development of RSA, public keys were sent to beneficiaries via a "dispatch" from another protected channel prior to contact with the initially coordinated message. RSA excludes this as the keys used to scratch plain contents are open keys on an RSA device. The screwdriver key is then again categorised in order to decipher the chip material by the principal with the right private key. Each has its own (public) encryption and (private) RSA scrap keys. The key is to pre-empt simple allowance or split the private key used to unbundle with the use of a public encryption key.

b) Digital Signatures

Digital signatures are used for validation. The recipient of the message would have to ensure that the sender had sent the message, or if the message had been made by some digital hoodlums. The sender uses the scroll key and only anyone who uses the public encryption key will search the label. The marks cannot be modelled anyway. The

sender of the symbol cannot even refuse to have the letter identified in the future. Subsequently, techniques for electronic transfers and transmissions have been revised, such as shop transmission and billing. In addition to these electronic transmissions and exchanges, the RSA equations are useful for electronic mailing. The security of the RSA calculation is acknowledged to this stage because there are still no known attempts to penetrate the protection of RSA, typically because of the difficulties in listing large numbers n = pq, where p and q are enormous primary numbers. [16]

F. RANDOM KEY GENERATION AND RESULTS

Timestamp is used as a seed in generating the Random Key K. The method of Key generation is a sequential range of values and functions generated through a random function generator. These values are the combination of additive and multiplicative operations. The process of generating key randomly is extremely useful as it reduced the complexities of creating an identifiable key and makes the hybrid combination RSA and Vigenere cipher a better encryption module. While the system has only one timestamp available at the time of key generation, even the developer doesn't know about this value as it can further lead to problem if there is an employee burnout. Additionally, this combination of using a hybrid attachment also reduced the time complexities of the RSA module which individually is a length process and may affect the communication over IoT modules. The smart watches and phones connected remotely needs to have a swift and fast interaction panel to avoid the any delays in the communication and control. It is also important to boost the user experiences.

The operation of this hybrid model was judged on the basis of a time complexity module.

1) First check

We considered the following data to check the algorithm:

- "WE ARE CHECKING THE HYBRID ALGORITHM"
- "THIS IS A RANDOM CHECK USING LINUX C"
- "BEJNndi58Qnei48dwn393ci23nrdi3rxnxf 24ct4xnoc4yr298yrx"

We created the three algorithms for the system in C language using a Linux system. Same system with freed RAM AND no other system functions was ensured to maintain a harmony among the system check. The graoh below illustrates the system the time taken by the three algorithms to complete the encryption of the datasets.

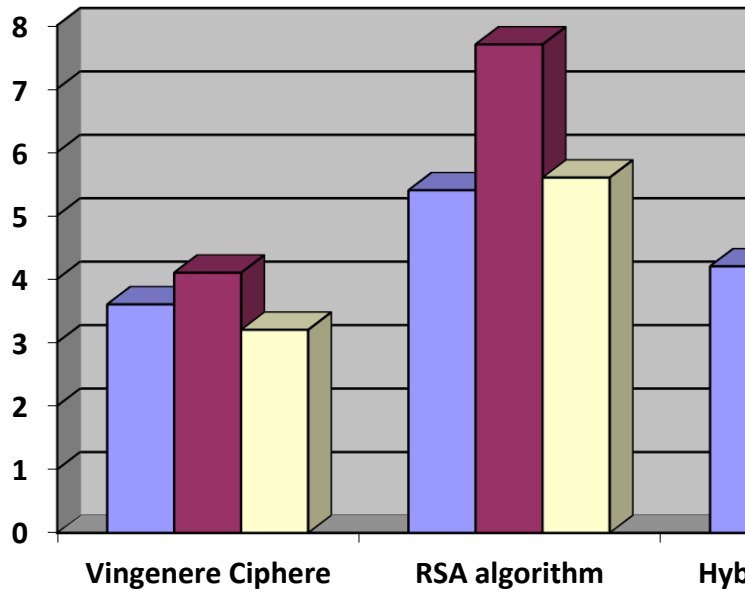

Figure 4 - Time taken to encrypt raw data

2) Second check

The data obtained from a sample data set retrieved from the Kaggle for the InceptionResNet 2 Encryption, was selected. We used the same data as follows to be encrypted:

- "WE ARE CHECKING THE HYBRID ALGORITHM"
- "THIS IS A RANDOM CHECK USING LINUX C"
- "BEJNndi58Qnei48dwn393ci23nrdi3rxnxf 24ct4xnoc4yr298yrx"

The data was encrypted to InceptionResNet 2 using the algorithm described below:

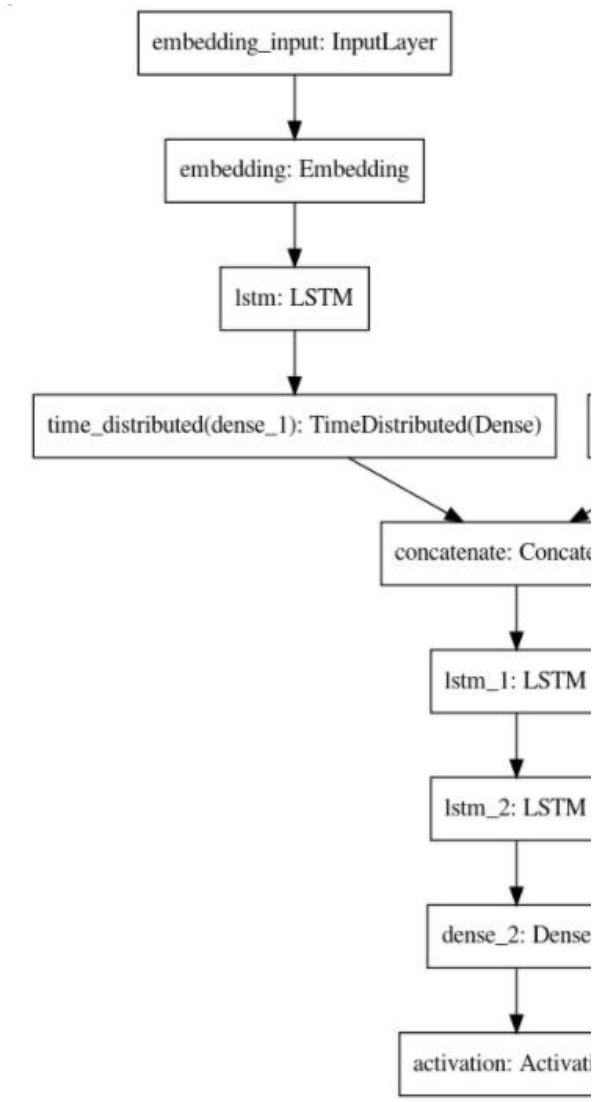

Figure 5 - Flow chart for InceptionResNet 2

This encryption was done to bring data on a similar form. The dataset was run on the Python IDLE program coded for three algorithms using a similar machine (Intel i5-10 Gen, 8 GB RAM, 128 GB SSD). The program ran over to this dataset individually and it was made sure that the program doesn't access any altered version of the dataset to ensure accuracy. The time was calculated systematically for the completion of each process and was converted to graph to illustrate the ease of using the algorithm.

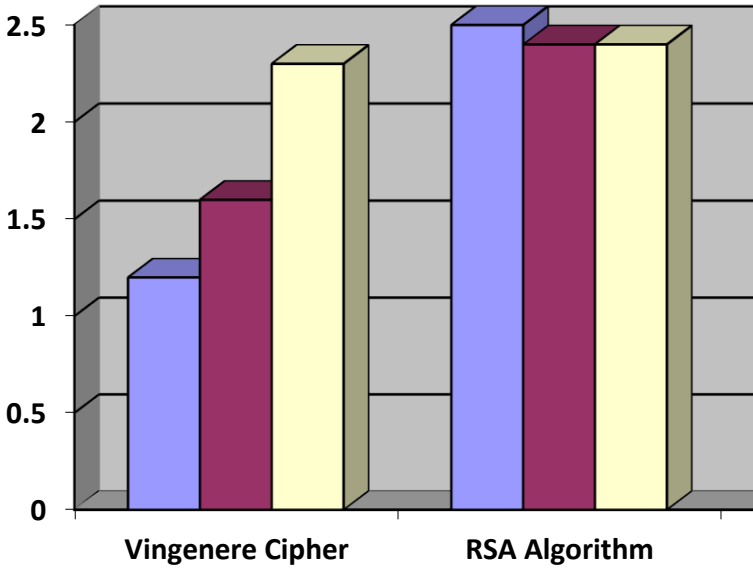

Figure 6 - Time taken to encrypt treated data (through InceptionResNet 2)

3) Accuracy check

We used multiple computer programs to access the running hybrid algorithm to see if they can detect the random key generated in the system. We used three Software for this purpose:

- VeraCrypt
- DiskCyptor
- AxCrypt

The automatic algorithm of these software accessed the hybrid algorithm and used the before and after encryption data to detect the random key generated. The data obtained by the system was converted to graphical forms as follows:

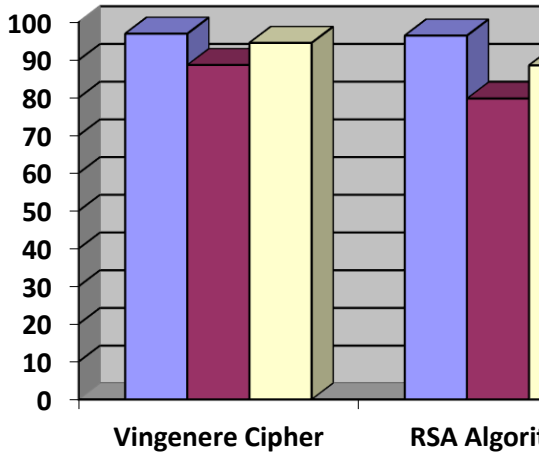

Figure 7 - Accuracy score to predict timestamp at time of Random Key generation

III. CONCLUSION

This paper presents a mechanism for protecting information inside the IoT framework, which was in this circumstance a cell telephone and a smart wearable watch. The methodology proposed involves the combination of symmetric and asymmetric algorithms of cryptography. This special mix of Modified Vigenere and RSA decreases the encryption time compared with the use alone of the RSA algorithm. A significant method to produce hidden keys and messages is random number. Random number. As a random key, the current time stamp as the seed is created for each session of receiving and sending messages. There is therefore no link between the keys. That guarantees more communication protection and puts the device more at risk with safety alerts. The methodology suggested also tackles the issue of session key distribution. In contrast to the standard Vigenere cypher, which provides protection for the entire system, the encrypted text generated is smaller.

IV. FUTURE WORK

Through the integration of several elements into the updated Vigenere cipher, the proposed scheme may be further improved. This will improve the cypher text's stability. To further improve the random K-key can be used for the encryption of each communication session, asymmetrical algorithms like Elliptical Curve Cryptography (ECC) etc. Hashing strategy should be used to ensure and improve the credibility of the texts.

V. REFERENCES

[1] Dian, F. J., Vahidnia, R., & Rahmati, A. (2020). Wearables and the Internet of Things (IoT), Applications, Opportunities, and Challenges: A Survey. *IEEE Access*, *8*, 69200-69211

[2] Haghi, M., Thurow, K., & Stoll, R. (2017). Wearable devices in medical internet of things: scientific research and commercially available devices. *Healthcare informatics research*, *23*(1), 4-15

[3] Jara, A. J. (2014, October). Wearable internet: Powering personal devices with the internet of things capabilities. In *2014 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)* (pp. 7-7). IEEE Computer Society

[4] Grønli, T. M., Biørn-Hansen, A., & Majchrzak, T. A. (2019, January). Software development for mobile computing, the internet of things and wearable devices: Inspecting the past to understand the future. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

[5] Santamaria, A. F., Raimondo, P., De Rango, F., & Serianni, A. (2016, September). A two stages fuzzy logic approach for the Internet of Things (IoT) wearable devices. In *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)* (pp. 1-6). IEEE.

[6] Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015). Privacy and security on the internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems*, *1*(2), 99-109.

[7] Castillejo, P., Martínez, J. F., López, L., & Rubio, G. (2013). Internet of things approaches for managing smart services provided by wearable devices. *International Journal of Distributed Sensor Networks*, *9*(2), 190813.

[8] Thierer, A. D. (2015). The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation. *Adam Thierer, The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, *21*.

[9] Tahir, H., Tahir, R., & McDonald-Maier, K. (2018). On the security of consumer wearable devices in the Internet of Things. *PloS one*, *13*(4), e0195487.

[10] Amorado, R. V., Sison, A. M., & Medina, R. P. (2019, March). Enhanced Data Encryption Standard (DES) Algorithm based on Filtering and Striding Techniques. In *Proceedings of the 2019 2nd International Conference on Information Science and Systems* (pp. 252-256).

[11] Daemen, J., & Rijmen, V. (2020). *The Design of Rijndael: The Advanced Encryption Standard (AES)*. Springer Nature.

[12] Vuppala, A., Roshan, R. S., Nawaz, S., & Ravindra, J. V. R. (2020). An Efficient Optimization and Secured Triple Data Encryption Standard Using Enhanced Key Scheduling Algorithm. *Procedia Computer Science*, *171*, 1054-1063.

[13] Liu, Y., Tang, S., Liu, R., Zhang, L., & Ma, Z. (2018). Secure and robust digital image watermarking scheme using logistic and RSA encryption. *Expert Systems with Applications*, *97*, 95-105.

[14] Gulsezim, D., Zhansaya, S., Razaque, A., Ramina, Y., Amsaad, F., Almiani, M., ... & Oun, A. (2019, October). Two Factor Authentication using Twofish Encryption and Visual Cryptography Algorithms for Secure Data Communication. In *2019 Sixth International Conference on Internet of Things: Systems, Management, and Security (IOTSMS)* (pp. 405-411). IEEE.

[15]Michelle S Henriques, Prof. Nagaraj K. Vernakar, "Using Symmetric and Asymmetric Cryptography to secure communication between devices in IoT", presented at the International Conference on IoT and Applications, Nagapattinam, India, 19-20 May, 2017, 10.1109/ICIOTA.2017.8073643

[16] Evegny Milanov*," The RSA Algorithm"*, June,2009

[17] Singh, C., & Chauhan, D. IoT–Blockchains Integration-Based Applications Challenges and Opportunities. In Mobile Radio Communications and 5G Networks (pp. 87-116). Springer, Singapore.