LIGHTWEIGHT CRYPTOGRAPHY FOR SECURITY IN IOT DEVICES

Adisha Waghare
Dept. Of Electronics and Telecommunication
Vidyavardhini's College of Engineering and Technology, Vasai
adisha.180561205@vcet.edu.in

Snehal Singhi
Dept. Of Electronics and Telecommunication
Vidyavardhini's College of Engineering and Technology, Vasai
snehal.180511201@vcet.edu.in

Prerna Tiwari
Dept. Of Electronics and Telecommunication
Vidyavardhini's College of Engineering and Technology, Vasai
prerna.180541201@vcet.edu.in

Ms.Shraddha Gosavi
Assistant Professor
Vidyavardhini's College of Engineering and Technology, Vasai
shraddha.gosavi@vcet.edu.in

Abstract **- Over the last few years there has been vast development in IOT technology.this technology made people life style much easy and intresting through various innovations by finding solution to day to day problems.todays,scenerio of security development is widely more protectable and important in daily life style.In IOT applications,security plays important role because data that has transferred is always become secure if any of the unauthorized access getting in it,they can affected personal injury as well as damage of security development.**

Index Terms – IOT,lightweight,cryptography and Sensor

1. INTRODUCTION

Entire business world is connected to security.The supply and need of the market in the various country has drastically increased over the last few year and it is very important to provide customers with best security.In the future,large amount of lightweight devices going to be connected with each other.It is important to secure entire system in order to ensure to be relied on as truthful.Crptography is well-developed,secure information and communication technique derived from stimulated concept and set-up of rule based calculation called algorithms.Transformation of messages will be in various ways,so that its is hard enough to decipher.these algorithms are used for verification to protect data privacy,web browsing on the internet without any risk,secret communications such as credit card transcations,email etc.Latest estimation in IOT,devices are connected in cloud platform.i.e many of industrial Iot applications.Thus,the insurance of privacy and data protection is struggling at the moment to be solved.

Generally,IOT devices targeted to simple data processing.i.e mobile apps,void control devices,smart TV sets etc.therefore,capcities are often small.Internal system allocated with less amounts of battery,Random access memory(RAM),low rates of data etc.Because of this reason IOT devices are unable to allocate considerable memory and processing energy just for security allocation.that is when introducing lightweight cryptography.This version expects to execute which has less amount of computational complexity giving high robustness against security attacks meanwhile.

The evolution of cloud computing over the years is very uncommon. There are certain things to cloud data for extending cryptography. Cryptography now becomes a huge part of IT department. Various day-to-day activities are carried on it for security purpose. The benefits of cloud computing are being realized by more companies and organizations every day as it is very much secure . Cloud computing gives the clients a virtual computing infrastructure on which they can store data and run many applications. But the main motive of cloud computing is that stored the secure messages of clients. There are many other approaches to extending cryptography to cloud data. Many companies choose this system to encrypt data prior to uploading it to the cloud altogether.

2. MOTIVATION

Necessity is the mother of invention. This led to vast development in the field of technology. Many innovative ideas and inventions had resulted in the advancement of human lifestyle. Things now look much easier than before and this process is going on. When it comes to cryptography there is been development but still there are many complications. without cryptography data will be hacked by anywhere, it is difficult to find the hackers and searching exact location of it. The cryptography can expose critical infrastructure to weak and easy and it is mainly for weak and hidden cryptography. Public main attention to exposed data leads to brand erosion to customers. This new modern environment requires organizations to pay attention to know how cryptography is being implemented and managed throughout the whole enterprises. This motivated us to work on the innovative IOT based cryptography which helps client to find the data easily and don't need to think about data protection.

3. LITERATURE REVIEW

Purposes[1] the primary focus was to examine the importance and uses of lightweight cryptography in security of IOT devices.Now,a days,the majority of humans are increasingly to secure the data on the online platform because it consumed less time and less memory as it is itself named as lightweight cryptography as the peoples data hack easily so the encrypt the message and to overcome this problem,we introduced the lightweight cryptography in IOT devices for assuming it will help the people very much to keep their data secure.thus,this literature reaches were performed using webpages.A lightweight cryptography based on the internet of things(IOT) was presented,which includes ultrasonic sensors,ESP32 micro controller and a LCD screen & a keyboard and a webpage.wireless connection is required for an sensors following that the ESP32 will connect so,after the connection the messages will display on LCD screen automatically.To achieve confidentiality,the data and nodes are encrypted throughly,traditional cryptographic primitives are not directly applicable to I0T devices as it involves very poor resources. Lightweight cryptography should be applied efficient encryption in IOT.lightweight symmetric and asymmetric algorithm should be design for IOT systems.In the future,in IOT data security and authentication is big concerns so number of technique are proposed in which hybrid models of encryption and authentication algorithms are made but this cause increase in the memory requirement on the devices.As a result ,the proposed model is more competitive than alternatives[2].

Author proposes that the survey with a goal of finding the best suitable solution for IOT security.It is very difficult to find one clear approach which will fit all kinds of application of IOT. So,we all know that the various kinds of devices are connected in IOT networks. Some devices can afford to have a heavyweight and a high security method, but most of the devices are resource constrained. They need a security solution which acts fast and mainly it need to less complex and versatile[3].

Author proposes that the cloud based IOT architecture is a structure which is used for specification of networks physical components its different performance principle and procedures. As the data will secure by the help of cloud server. the cloud server or we can say IOT it has different layers which face many attacks like active and passive

attacks. The main purpose of is that the data is secure by using the SHA256 hash function. Using the SHA256 hash function to encrypt and decrypt the message and also to generate the key such as public key or private key to get an cipher text. The concept and execution of the encrypted or decrypted messages, as well as the cloud server data are discussed[4].

From the above referred papers, it is been understood that the above mentioned approaches have not provided to complete security for the IOT devices.Which can people's easy.So,by considering all the aspects we have design an web page or LCD screen who will display the message after encrypt and decrypt process which will be very helpful for human being to secure the data.

4. PROPOSED APPROACH

The main function of the proposed system is to developed the lightweight cryptography using the IOT devices to secure the data easily.The concept behind the cryptographic application is to find the sender message with decryption process with high security.

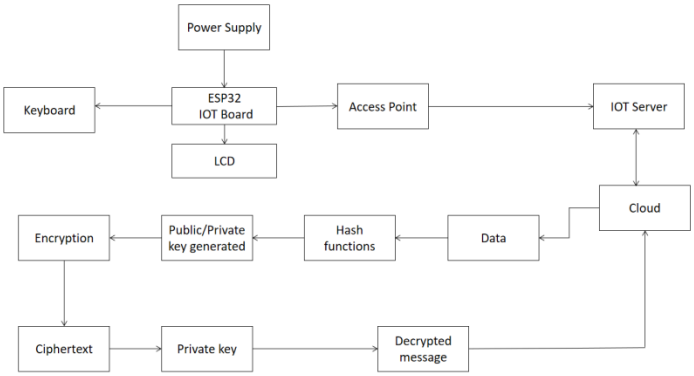


Figure 1:Block diagram of Lightweight cryptography in IOT server.

In the figure 1 ,firstly ESP32 is connected to wifi module and there will be two options available over there i.e. New Registration and Login.And if we click on New Registration or Login we will get 2 options i.e. user phone number and e-mail id.Someone select any of this option than the data will be save in database and we have to enter password.And all this process will be done by API.If there is any new user or if it will click on login then the remaining information i.e. e-mail or password will select the 2 options send or receive the information.And if the user want to store the encrypted message then it have to click on SEND.And it will type the own message and generate a key then the data will get encrypted and store in the database of the user or the process will be through API.And if it want to decrypt message than it have to put a key and for decryption process the user will have to enter the another user information to decrypt the message and than it will display on LCD screen.

5. IMPLEMENTATION

This application consists of various activities for users to secure the data .This all activities are there in the model.

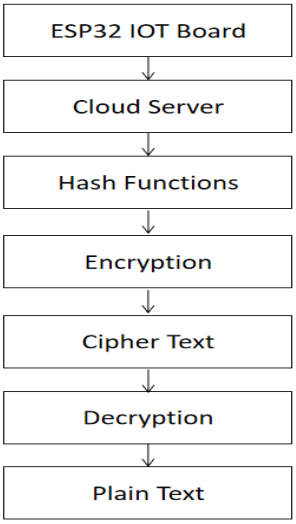


Figure 2: Flow diagram of Encryption and Decryption

In this process of encryption and decryption the cloud server plays a vital role in it to fetch the data from the users and than by to encrypt and decrypt the message in a plaintext by using private/public key and mostly hash function as we are using SHA256 hash function for the small size and efficiency of it will not affected at all.

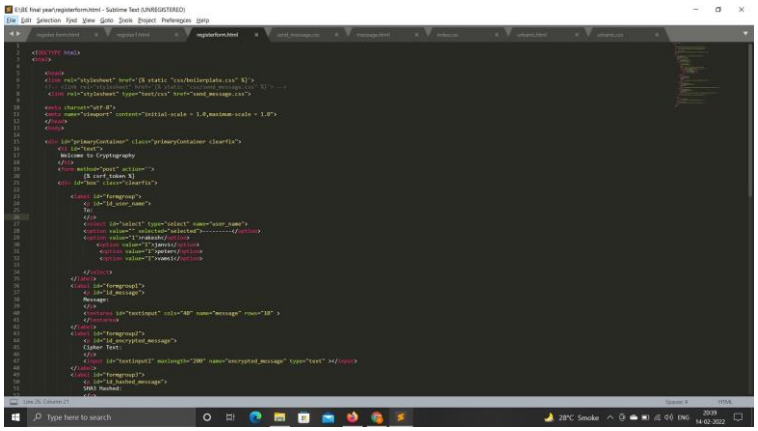
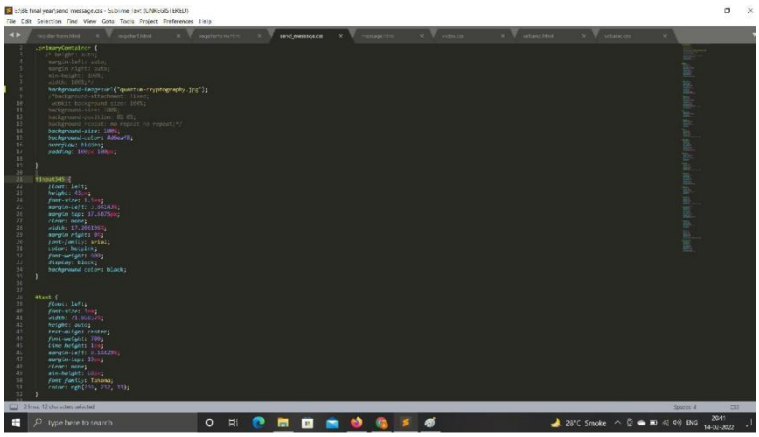


Figure 3:Register code Application



6. RESULT

The desired is to give security to the user by this application.The user should have the keys with them to encrypt/decrypt the message.If they have the keys with them than they can set password which is correct or incorrect password after that user have to login in the application by the E-mail id/phone number and then the user have to type the message and then the hashing function will have the message and then encrypted by the private key is better than the encryption of the whole message because hash are small in size and also efficiency is not affected. And the data will be more secure and there is no type of risk in it.

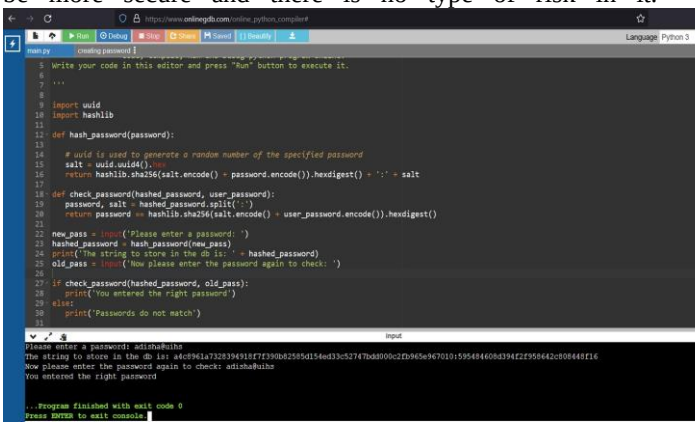


Figure 4:Correct password

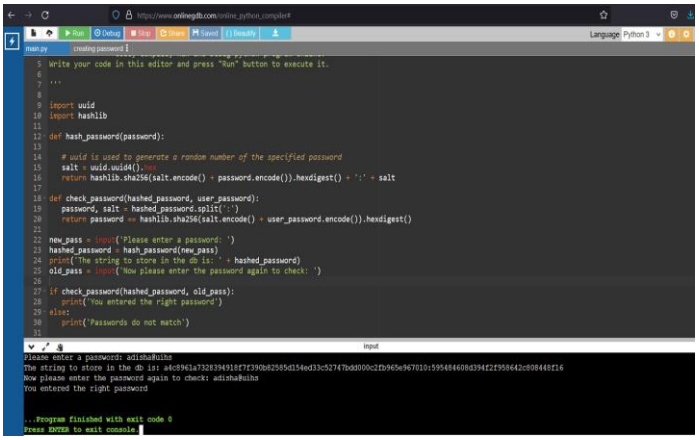


Figure 5:Incorrect password

Figure 6 : Login Page

Figure 7 :Register Login Page

6.CONCLUSION

Internet of Things has been rapidly finding a path through our modern-day life and is aiming to improve the quality of life by connecting us with many smart devices,technologies,and applications.Due to the drastic growth in the number of IoT device in various domains mainly in communication purpose, IoT security is one of the main concerns. For resource-constrained IoT devices,lightweight cryptography is an effective way to secure communication by transforming the data.Conclusively, this paper wraps up with data for hardware/software for a particular application.

The concept of lightweight cryptography was introduced to overcome the challenge.Lightweight cryptographic function are still emerging to deliver precise privacy and data protection via accurate encryption and decryption models for the benefits of users.In this paper we discussed about the different architectures,security,privacy issues and lightweight solutions that can be taken to solve them.

7. FUTURE SCOPE

This application is mostly automated,the final part of clients privacy of various algorithms.This can be replaced by AES algorithm by giving best security.Now it's tough to implement considering manipulation of data system.But when its application get launched on a large scale it can be achieved.Lightweight cryptography have excellent main security challenges have reduced the size of implementation while keeping the decreasing range as good as possible.In the close future interested in the details performance of lightweight cryptography.And by searching bestest security it would be very helpful for users.This will help the user to secure data with a lightweight.

7.ACKNOWLEDGMENT

It is indeed a moment of great pleasure and immense satisfaction for us to express our thanks and sense of gratitude to all who lead helping hand.We express our thanks to our project guide Ms. Shraddha Gosavi ,(Assistant Professor VCET).We are also immensely grateful to Dr. Vikas Gupta and other staff members of Dept. of EXTC, VCET for their guidance and support.

VII. REFERENCES

[1] D. H. Bui, D. Puschini, S. Bacles-Min, E. Beigne, and X. T. Tran, "AES Datapath Optimization Strategies for Low-Power Low- Energy Multisecurity-Level Internet-of-Things Applications," IEEE Trans. Very Large Scale Integr. Syst., vol. 25, no. 12, pp. 3281– 3290, 2017. [19] D. H. Bui, D.

[2] G. Bansod, N. Raval, and N. Pisharoty, ''Implementation of a new lightweight encryption design for embedded security,'' IEEE Trans. Inf.Forensics Security, vol. 10, no. 1, pp. 142–151, Jan. 2015.

[3] M. Lu, A. Fan, J. Xu, and W. Shan, "A Compact, Lightweight and Low-Cost 8-Bit Datapath AES Circuit for IoT Applications in 28nm CMOS," 2018 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng., pp. 1464–1469, 2018.

[4] L. Zhu, Y. Wang, and R. Li, "Efficient differential fault analysis attacks to AES decryption for low cost sensors in IoTs," Proc. -IEEE Int. Symp. Circuits Syst., vol. 2016–July, no. 61173036, pp. 554–557, 2016.

[5] Zhi-Kai Zhang , Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, "IoT Security: Ongoing Challenges and Research Opportunities", IEEE, 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp 2163-2871, 2014.

[6] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," 2014 Int.Conf. Electron. Commun. Comput. Eng. ICECCE 2014, pp. 83–93, 2014.

[7] O. P. Pinol, S. Raza, J. Eriksson, and T. Voigt, "BSD-based elliptic curve cryptography for the open Internet of Things," 2015 7th Int.Conf. New Technol. Mobil. Secur. - Proc. NTMS 2015 Conf. Work., 2015.[5] I. Chatzig.

[8]W. Diehl, F. Farahmand, P. Yalla, J. P. Kaps, and K. Gaj, "Comparison of hardware and software implementations of selected lightweight block ciphers," 2017 27th Int. Conf. F. Program. Log. Appl. FPL 2017, 2017.

[9]R. Sharma and S. Pansare, "Analysis of symmetric key cryptographic algorithms," Int. Res. J. Eng. Technol., vol. 4, no. 2, pp. 1628–1630, 2017.

[10]Y. Weize and S. Kose, "A Lightweight Masked AES Implementation for Securing IoT Against CPA Attacks," IEEE Trans. Circuits Syst. I Regul. Pap., vol. 64, no. 11, pp. 2934–2944, 2017.