IJCRT.ORG ISSN : 2320-2882
INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Proposal of Lightweight Cryptographic Algorithm for Home Automation

Smt.J.Mounika
Assistant..Professor,
Department of E C E
CBIT
Telangana, India

Begari.Abhishek
Department of E C E
CBIT
Telangana, India

Allampally.Ashish
Department of E C E
CBIT
Telangana, India

Gaddi.Damodhar
Department of E C E
CBIT
Telangana, India

***Abstract*— Lightweight cryptography is a new concept that refers to a method of bettering data security through using less resources and providing higher throughput, conservatism, and low power consumption. Every fraction second, the Internet of Things (IoT), which links billions of devices, collects an enormous amount of data. When the number of devices grows, so does the amount of data generated, and the protection of that data becomes a concern. In IoT architecture, devices are basically smaller and low-powered. Because of their complexity, traditional encryption algorithms are computationally costly and require several rounds to encrypt, effectively wasting the limited resources of IoT devices. A less complex algorithm, on the other hand, can compromise the necessary integrity. There are many lightweight cryptography algorithms available, and we use one of the symmetric encryption algorithms called Advanced Encryption Standard (AES). The speed of this algorithm is six times that of triple DES. Since all around us is automated in today's world, automation is playing an increasingly important role in human life. The term "smart home" encompasses not only the reduction of human effort, but also energy conservation and time management. Home automation enables us to control household appliances such as lights, doors, fans, and air conditioners, which require a large number of energy-constrained devices that constantly interact with one another. The security of this home automation system must not be compromised. This problem of security for automated systems is often solved by using lightweight cryptographic algorithms. For this purpose, a lightweight security algorithm is proposed in our paper that is (AES).**

Keywords— Internet of Things (IoT), Home Automation, LWC, AES, DES.

I. INTRODUCTION

The Internet of Things (IoT) has been around for a few years now. The Internet of Things is now accessible due to improved network capacity, cheaper and more efficient sensing capabilities, and hardware miniaturization. The ability to communicate with non-living objects had become a reality. According to Cisco Systems, the number of computers connecting to the internet in 2008 risen tremendously of people on the planet. By 2012, the population had grown to 1.5 times its original size. This trend is expected to accelerate, with the number of connected devices expected to exceed 50 billion by 2020, resulting in a 1:8 ratio of people to connected devices. It's also predicted that by 2020, everyone on the planet will be communicating with an average of 3000-5000 devices. When all of the objects in the Internet of Things are virtually linked and can communicate with one another, automation becomes extremely feasible.

Someone does not have to think about refuelling a vehicle, washing clothes, driving a car, walking a cat, making coffee, adjusting the temperature, turning off lights, and so on. Despite advances in the Internet of Things, security and privacy concerns remain constant. The key issue that is slowing the adoption of IoT in today's world is stability.

Security is always a stumbling block to any technical innovation in the industry, but it is a major concern. The suspension of Google Glass production may be a good example. If the number of communicating devices grows, it's predicted that the amount of data transmitted over the network will grow dramatically. As of 2012, Google search is capable of searching 4000 Exa-bytes of information (stack of books from the earth to Pluto eighty times).

One of the Internet of Things' applications is the smart home. A smart house is a technology in which all of the devices in the house interact with one another in order to automate the process. It seems orthodox that when we wake up, the space temperature is automatically set, bed coffee is prepared for us in the coffee machine, water is heated/cooled according to the space temperature, your phone creates a daily schedule, turns off the electrical fan and light the moment you leave a space, and so on. As a result, Smart Home creates a user-friendly atmosphere.

Home automation is a system in which physical devices, most of which have little or no resources, interact with one another without the need for human interaction. In this type of communication, data is crucial. As a result, data must be protected from malicious attacks. Cryptography can be used to do this. The earlier encryption algorithm, encryption Standard (DES), has many flaws, including a limited key size and vulnerability to brute force attacks, among others. Furthermore, these algorithms are incapable of delivering high-level, reliable, and exportable protection. A replacement algorithm known as Advanced Encryption Standard closes these gaps (AES).

As engineers, it is our responsibility to provide new technologies to society for the betterment of all, but it is also our concern to find ways to reduce human effort.

Section II consists of the related work done in the field of Secure Home automation system. Section III illustrates the methodology of the proposed system. The actual implementation of proposed system is explained Section IV. Section V consists of results and discussions. Any more modifications which can be done to improve the fidelity and user friendliness of the current prototype have been addressed in section VI.

II. RELATED WORK

According to our research, several systems exist that can power home appliances using Android-based phones and tablets. Each device has its own set of characteristics. The process of developing a model for a home automation system is ongoing. Current systems have a number of flaws, including a lack of an intuitive user interface, a high base cost, and a poor security framework. We have attempted to change the situation. Below are some of the models that have already been designed.

[1] Andrea Zanella defined the model of a comprehensive survey of enabling technologies, protocols, and architecture for an urban Internet of Things. They discussed the various technological solutions and best-practice guidelines used in the Padova Smart City project, which was a proof-of-concept IoT deployment in Padova, Italy, carried out in partnership with the city municipality.

[2] Pavithra.D presented a model for implementing IoT in monitoring and controlling household appliances through the internet (www). This model is both cost-effective and scalable. The model allowed for appliance control through a web server as well as locally without access to the internet.

[3] Ravi Kishore Kodali, Vishal Jain, Suvadeep Bose, and Lakshmi Boppana presented the concept for an IoT project that focuses on developing a smart wireless home protection system that sends warnings to the owner through the Internet in the event of trespassing and, if desired, raises an alarm. The TI- CC3200 Launchpad board is the microcontroller used in the current prototype. This device can send updates and the status of the Wi-Fi-connected microcontroller-managed system can be received by the user on his phone from any distance, regardless of whether his phone is connected to the internet.

[4] According to Statista, there were 14.2 million smart homes in the United States in 2016, with that figure expected to rise to 36.01 million by 2020. With this number steadily that, we can no longer take protection for granted. Attacks on the secrecy and dignity of domestic systems are common. An intruder may take control of a household from afar, allowing them to easily examine the daily activities of the residents. This scenario will easily arise during a physical assault on the user if the attacker is able to open the door remotely or monitor the equipment in a way that causes physical harm to the house's occupants. This is why, in these domotic systems, we must introduce lightweight cryptography algorithms to avoid these attacks.

III. METHODOLOGY

Lightweight cryptography (LWC) is a common subset of cryptography that aims to create a specific, efficient cryptographic mechanism for devices with limited memory and processing power. LWC is a simplified version of traditional cryptography. This branch of cryptography aims to adapt the current computationally intensive operations of traditional cryptography algorithms to these restricted devices by reducing the size of the fundamental parameters, such as key size and block size, at a reasonable pace with minimal memory and energy consumption and few computational cycles, without compromising security.

Some of the algorithms which are commonly used in today's world in IoT are:

DES: The DES algorithm (Data Encryption Standard) is a symmetric-key block cypher developed by an IBM team in the early 1970s and adopted by the National Institute of Standards and Technology (NIST). The algorithm transforms plain text into ciphertext using 48-bit keys after splitting it into 64-bit blocks. Since it is a symmetric-key algorithm, the same key is used to encrypt and decrypt the data. If it were an asymmetrical algorithm, the

encryption and decryption keys would be different. DES is based on Horst Feistel's LUCIFER block cypher, which was created by IBM cryptography researcher Horst Feistel in 1971. DES employs 16 rounds of the Feistel structure, each with a unique key. In November 1976, DES was adopted as the federal encryption standard, and it was reaffirmed in 1983, 1988, and 1999. DES was the data encryption standard in information security for a long time. After a public competition to find a replacement, the Advanced Encryption Standard (AES) succeeded in replacing the DES encryption algorithm as the approved standard in 2002. In May 2005, the NIST officially revoked FIPS 46-3 (the 1999 reaffirmation), while Triple DES (3DES) is still permitted for sensitive government data until 2030.

TDES: Triple DES is a symmetric key-block cypher that uses three copies of the DES cypher. It encrypts with key one (k1), decrypts with key two (k2), and then encrypts with key three (k3) (k3). A two-key version exists, in which k1 and k3 are the same keys.

AES: AES is a symmetric key cryptography that is an iterated block cypher with a fixed block size of 128 bits and a variable key length of 128, 192, or 256 bits. The various transformations operate on the intermediate effects, which are referred to as state. Since the block size is 128 bits, which equals 16 bytes, the state is a rectangular array of bytes with dimensions of 4x4. (In the Rijndael edition, the row size is set at four, but the number of columns is variable.) The number of columns (abbreviated Nb) is the block size divided by 32. The cypher key is often depicted as a four-row rectangular array. The cypher key's number of columns, Nk, is equal to the key length divided by 32. AES uses a fixed number of rounds with a variable number of rounds: A 128-round key has ten rounds. A 192-round key has 12 rounds. There are 14 rounds in a 256-round key. An algorithm begins with a random number, which is used to scramble the key and the data it encrypts using four mathematical operations. The same key that was used to encrypt and decrypt the number must be used to decrypt it. Each round has four operations for encryption: SubBytes, ShiftRows, MixColumns, and AddRoundKey, and decryption uses the opposite of these functions. Below figure shows the structure of AES algorithm.

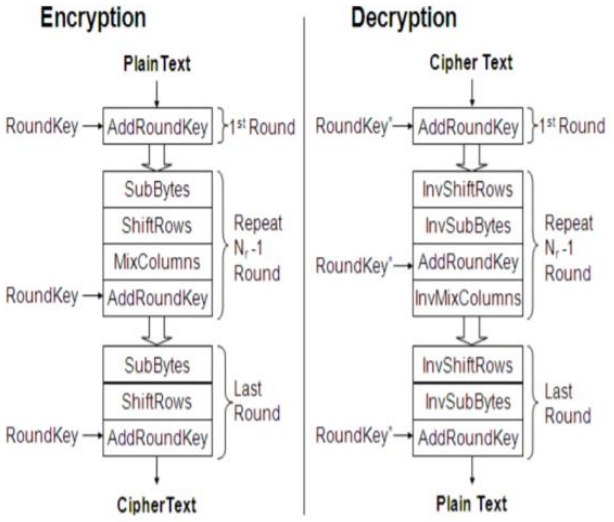

Fig.1 Flow chart of AES Algorithm

Among all lightweight cryptography algorithms we choose AES to secure constrained devices in Home Automation. Because AES Encryption is more mathematically efficient and elegant cryptographic algorithm. Till the date there is no evidence that this algorithm is hacked.

IV. IMPLEMENTATION

A. Implementation of Home Automation in Tinkercad:

As we have discussed the algorithms we are using for this work, we are now discussing the implementation of the algorithms and how these algorithms are used in implementing this problem statement. First, we will implement normal Home Automation system using Tinkercad. First connect the circuit as shown in the below figure:

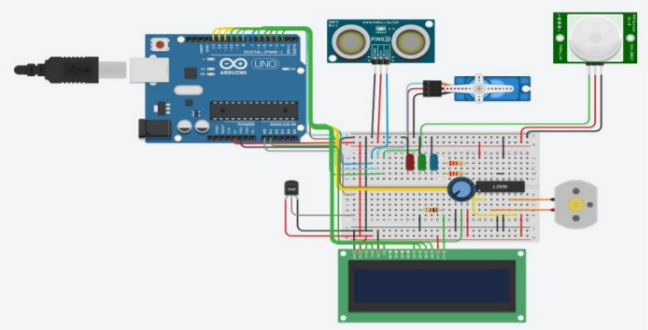

Fig.2 Home Automation using Tinkercad software

Step 1: Connecting the circuit: To connect any circuit in Tinkercad first select all the required components from the list of components. From above circuit we can observe that Arduino is the heart of our project we connect all required output pins for certain applications .

Step 2: Programming the Arduino: Here code is written in c

B. Implementation of AES for Home Automation:

As a next step of our implementation here we consider the hardware components such as Arduino Uno, PIR sensor, LED, jumpers ,a Pc/laptop Connect the circuit as shown below:

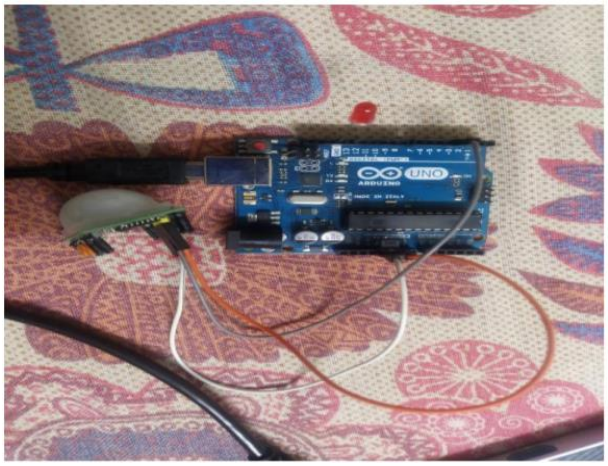

Fig.3 Basic Home automation

Next step is major part of our project as already discussed we implement security to our home automation system using lightweight cryptography among all the algorithms we choose AES as most secure and mathematical efficient compared to all other algorithms.

language here there are two ways to write one way is directly writing code based to required output and the second way is by implementing coding blocks this method is very useful and easy to understand the probability of errors in code is very less compared to other method. This method is briefly explained in above software description of Tinkercad.

i. Description of Basic Home Automation:

Here first we connect Arduino uno Vcc and Gnd pins on the bread board later in the implementation of home automation here we use 3 sensors they are ultrasonic sensor, PIR 55 sensor, Temperature sensor. The function of ultrasonic sensor is used for obstacle detection in our project, PIR sensor is used to sense the motion of any object at a distance of 10m, temperature sensor is used to detect the temperature of the environment. Here current status of the project will be displayed on LCD now we connect the circuit as shown above after connections we write the code accordingly. The above circuit is said to be home automation for below reasons: 1. The servo motor which is connected in the circuit is similar to our main door in home when an obstacle is detected near to ultrasonic sensor the door opens and later when obstacle is far automatically the door closes. 2. When the moving object is entered into home as we have PIR sensor it detects the motion then LED's blink accordingly. 3. Let's consider an example when the room temperature is more than 14 the dc motor which is connected in the circuit is activated here, we can understand as an application of home automation when temperature rises automatically the fan starts rotation is seen in this instance.

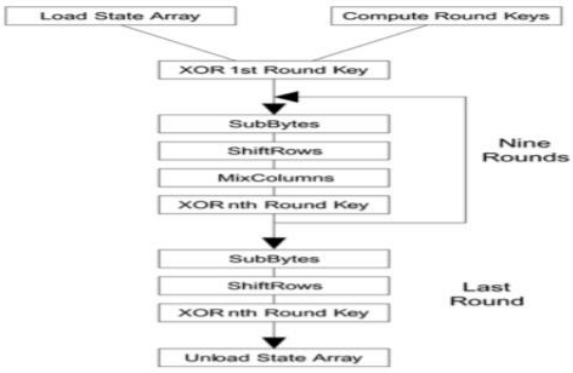

Fig.4 Summary of AES algorithm

Each round of algorithm consists of four steps they are, SubBytes, ShiftRows, MixColumns, AddRound Key.

Here using all these steps, we implement a c code in Arduino software in order to write this code first need to add aes.lib and base64 libraries in Arduino . Here plain text is written in code itself and we can observe the cipher text and encryption decryption entire process in serial monitor of Arduino. As per circuit shown above, we can also observe the time period of motion detected by PIR sensor. By all these operations entire home automation system is secured using AES algorithm.

IV. RESULTS AND DISCUSSION

A. Basic Home Automation using Tinkercad execution results:

1) If someone approaches the door within 40cm, the door will open and remain open for 2 seconds. Here we have ultrasonic sensor for distance measurement and a servo motor to open the door. 2) If the room senses movements, the light (LED) will turn on automatically. PIR was used to track movement in this case. 3) It will sense the room temperature and, if it is greater than 20 (degree Celsius), it will activate the fan; otherwise, it will remain turned off. *On the LCD, the current state will be shown.

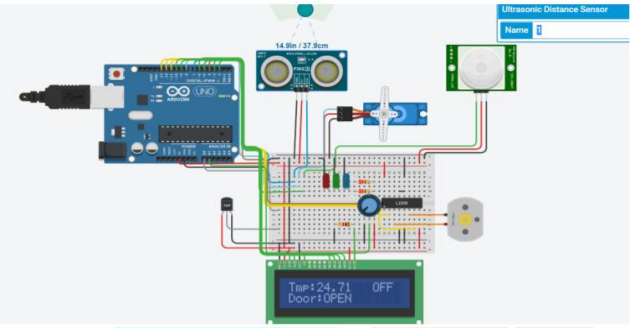

Fig.5 Working of Home automation with sensors

B. AES algorithm implementation for Home automation results:

Only one sensor is taken for building home automation which could be easy to understand.

Fig.6 serial monitor output for AES implementation

Fig.5 is the screenshot of the serial terminator of Arduino software. Here the plain text let us say "SECURE HOME AUTOMATION " is written in code itself according to AES algorithm during encryption the plain text is converted to cipher text it means the unreadable text format and during decryption the cipher text is converted to actual plain text which is sent and time taken for this process is clearly seen the serial terminator this entire process can be observed in above fig.5 along with the encryption we have also connected the home automation circuit using PIR sensor whenever the motion detected the LED blinks and in the serial monitor its is shows at what time motion detected and end of motion is clearly shown in above figure 5.

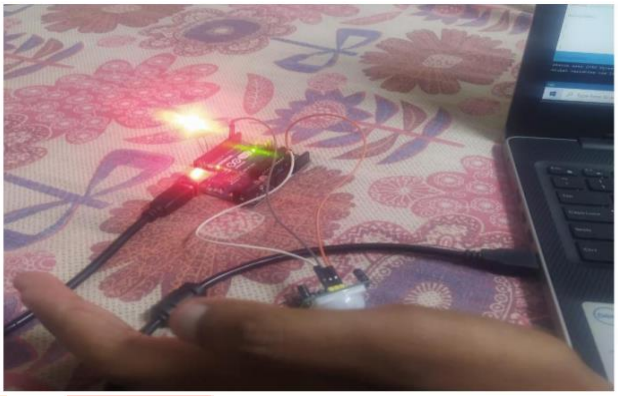

Fig.7 Home Automation using hardware components.

In the above image fig 6 the home automation using one sensor is implemented and whenever the motion detected the LED blinks this process only starts after encryption of plain text which is sent from Arduino to sensor entire output for above connected circuit is shown in serial monitor of Arduino.

C. Output Analysis:

From the fig.5 time taken after sending plain text to encrypt is 1.573 seconds/1573 milli seconds , time taken to generate cipher text is 0.48 seconds/ 48 milli seconds. Time taken to decrypt the original plain text is 0.45 seconds/ 45 milli seconds. The time required for sensor to activate is 1 minute 6.675 seconds and first motion is detected 33 seconds and motion ended at 42 seconds. Below Table 1 describes the time taken for various modules to respond. Modules include PIR sensor time and AES overall run time.

S. No	Module	Time Taken (Seconds)
1	Encrypt Time	1.573
2	Cipher text Time	0.48
3	Decrypt Time	0.45
4	Sensor Response Time	minute 6.675 seconds
5	Overall AES Runtime	1 minute 45 seconds

Table 1 Response Time

V. CONCLUSION AND FUTURE SCOPE

A. Conclusion:

The work is successfully implemented and verified. It is developed by integrating features of all the hardware and software components used. Mathematical efficient and easy computational lightweight cryptography algorithm such as AES is chosen as it is implemented in both software and hardware. Here PIR sensor , Ultrasonic sensor and Temperature sensor are used to build simple automation. AES algorithm for home automation is implemented using less resources and the runtime of AES algorithm in home automation is noted as 1 minute 45 seconds. Thus, the developed system is efficient and secure smart home that is convenient to solve security problems which will help to reduce or stop the break-ins.

B. Future Scope:

The system can further improved by developing cloud-based home automation where the user can control his house from anywhere if any unknown person wants to control home becomes tough task as AES is encrypted at transmitter and decrypted at receiver . The present system has application such as in Wireless communication, transmission of secured data is a big concern which consumes more memory in resource constrained devices. To overcome this drawback, key whitening can be implemented in the encryption side. This system can be further extended in the field of Retailing sector to reduce cybercrimes.

REFERENCES

[1] Gouthame P, Dr.M. Manikandan, “Secured Real time Smart room Automation using AES Algorithm”, in International Journal of Engineering and Techniques, Issue 4, Volume 6,2020.

[2] Neal R. Wagner , “The Laws of Cryptography with Java code”,”2003”.

[3] R.Kousalya and Dr.G.A.Sathish Kumar , “A Survey of Light-Weight Cryptographic Algorithm for Information Security and Hardware Efficiency in Resource Constrained Devices”, in International Conference on Vision Towards Emerging Trends in Communication and Networking,2019.

[4] Sattar B.Sadkhan and Akbal O. Salman , “A Survey on Lightweight-Cryptography Status and Future Challenges” , in International Conference on Advances in Sustainable Engineering and Applications (ICASEA), Wasit University, Kut, Iraq,2018.

[5] Isha Bhardwaj, Ajay Kumar, Manu Bansal, "A Review on Light-weight Cryptography Algorithms for Data Security and Authentication in IoTs", International Conference on “Signal Processing, Computing and Control” ISPCC- 2k17; IEEE Conference, September, 2017.

[6] Susha Surendran (NYIT, Abu Dhabi, UAE), Amira Nassef (NYIT, Abu Dhabi, UAE), Babak D. Beheshti (NYIT, Old Westbury, New York), “A Survey of Cryptographic Algorithms for IoT Devices”, in IEEE Long Island Systems, Applications and Technology Conference (LISAT),2018.