Smart Secure with IoT: Agriculture Data based on Farm Monitoring

Vidyashree L*1, Suresha2
1Research Scholar, 2Chairman and Professor
1,2Department of Studies in Computer Science, University of Mysore, Mysore, Karnataka, India
Email: *vid14.1987@gmail.com
DOI: http://doi.org/10.5281/zenodo.3526774

Abstract
The Internet of Things (IoT) is meant for omnipresent property among completely different “things” or entities. Horticulture assumes a major job inside the improvement of the farming nation. In India, about 70% of the population depends on farming and one-third of the nation’s capital comes from farming. Basically according to the present situation the weather condition at a particular agricultural area wasn’t been considered while starting their farming process. To avoid this, we can make a weather bureau which consists of a different sensor that can get different parameters at a particular area and can get a real time report from that data. Securing an agricultural data is also a challenging issue in the agricultural field. So this paper focuses on securing an agriculture data from hackers. Nowadays IoT devices are increasing at the very high rate for all applications. Especially in agriculture field, lack of manpower, farmers all are going for remote control devices. So on going days, we need to ensure the security of the devices and the data about the land and control of the Precious devices. Strangers or competitors may be doing the vulnerable activities if it comes in bigger market, at that time we should be well evolved in security matters. Due to the dearth of security issues in existing, within the paper Extension of AES 128 bit has been planned with extra strategies to provide higher security. We are checking encryption timing difference for both with and without using encryption method. We concluded our algorithm is secure as compare to the existing method because we are using some additional methods to give more security. The proposed algorithm can be efficient, accurate and secure than existing.

Keywords: Agriculture, Authentication, Decryption, Encryption, IoT, Security, Sensor Data Integration

INTRODUCTION
The IoT permits physical objects to visualize, hear, assume and perform tasks by having them “talk” along, to coordinate selections and to share data. Eventually, all aspects relating to people's cyber, physical, social world are going to be interconnected and intelligent within the sensible world [1]. Agricultural IoT is an era of forming agricultural activities using sensing media to present higher services to farmers. Numerous sensor devices are deployed in agriculture land to gather essential data like temperature, humidity, light, dioxide, soil wet, acidity, rain drop, etc. By this kind of observation, it will be very easy for the agricultural survey for instance, the backbone of India economy exclusively depends on agriculture. Around sixty percent of its folks rely on agriculture directly or indirectly and also the seventy percent populations earn money from agriculture [2].

Nowadays, agriculture may become increasingly wide in IoT, the usage of IoT device for agriculture is gradually increased and shipments of IoT Device for
agriculture becoming growing by year to year. AES 256 will be heavy for the embedded devices, to reduce the load extension of AES 128 is used in this system. The main idea of the paper is to focus on securing agricultural data to protect from hackers. So for this, we are developing an algorithm to protect agricultural data from an unauthorized person. Basically, according to the present situation the weather condition at a particular agricultural area wasn’t been considered while starting their farming process. To avoid this, we can make a weather bureau which consists of a different sensor that can get different parameters at a particular area and can get a real time report from that data, which can be captured on the website. By this type of monitoring, it will be very easy for the agricultural survey. The security of the data will be given major role. Previously these data can be maintained in a paper or a document, a huge number of these data is not maintained securely sometimes data can be a loss or steal or destroy. So, on that time the data will be affected by some serious problems. So, in order to avoid all these affect the security can be given for agricultural data. This security can be maintained to protect a loss of information or accessing data from an unauthorized person. This will helps to protect from an unauthorized person accessing a data.

RELATED WORK
Verma O P gave two fundamental choices that separate one cryptography rule from another and its capability to verified information against assaults, its speed and also gave a presentation separation between four of the chief in style cryptography calculations: DES, 3DES, AES and Blowfish [3].

Pitchaiah et al., presented a 128-bit AES secret writing and coding and collaborated exploitation medicine code. The rule consists of three main elements they're a cipher, inverse cipher and key growth. The pointless kind information is reworked by a cipher is thought as cipher text. Cipher and inverse cipher method uses key schedule and it's created by key growth. Cipher and inverse cipher consists of a special variety of rounds [4].

Verma Amit et al., presented associate improved AES, which is able to be safer and sensible in performance as compared to existing AES. To encipher the text or image knowledge and to extend the speed, time the info to be encrypted is pipelined. AES is combined with validation and segmentation to form the info safer, key enlargement is completed. The improved version of AES is compared with blowfish, however as compared to the improved AES, results of the blowfish is quick and safer coding algorithmic program [5].

Rajarakshmi P et al., centered on to observe crop-field sensing element using temperature, humidity, soil wet, light-weight and alter the irrigation system. Using wireless transmission, the information from sensors are sent to net server information. The information are encoded in JSON format within the server information. If the wet and temperature of the sphere fall below the brink, the irrigation is machine-driven. Additionally to irrigation, in greenhouses candlepower management can even be machine-driven and all these notifications are sent to farmer’s mobile sporadically. From anyplace the farmers are ready to monitor the sphere conditions. This method are additional helpful in areas wherever water is in inadequacy, that could be a major problem. The system developed is useful and works during a value effective manner. To a bigger extent, it reduces the water consumption and it also needs least maintenance. The facility consumption has been reduced substantially. By using this irrigation system, the crop productivity will increase and also the wastage of crops is substantially reduced [6].
R R Agale et al., provide to induce the data regarding farm related data, proposed an IoT technology for observance soil information. To identify information related to soil and crops is difficult for farmers. IoT technology often utilized in the agricultural environment to gather and store information. Using IoT technology soil observance could be a major conception and small farmers can manage their farm from anyplace within the world [7].

PROPOSED ALGORITHM
To secure agricultural data, the following phases are carried out.

Data Collection on Agriculture
We are assembling a more than one thousands of information from agricultural fields supported some parameters like air quality, humidity, temperature, sound, lighting and smoke. STM32F407VG microcontroller has been employed in this paper to gather agriculture information. It is 32bit ARM cortex M4 microcontroller; it will run clock frequency up to 168 MHz [8, 9]. Micro-controller reads the device information, all sensors connected to the microcontroller's port pins. We are using hardware generated random information for experiment. In Fig. 1, x coordinate shows the agriculture data collection for varied parameters and data may be collected for every parameter individually and y coordinate shows the collected device data.

![Figure 1: Data collection on agriculture based on various parameters.](image)

Proposed Algorithm for Data Security
AES 256 are significant for the embedded devices, to cut back the load extension of AES 128 bit is employed within the paper. AES is that the preponderantly used encoding algorithm for encrypting and decrypting information. In any case, inside the current AES, there are a few downsides like low throughput and takes longer time scramble code. It also has some security issues. These issues are settled inside the proposed augmentation of AES. To convey higher security for the information, the proposed AES has been delineate with three further strategies checksum, segmentation, shuffling of information segments is employed and this system uses both symmetric and asymmetric encrypted with both private and public key method to encrypt the data.

The Fig. 2 shows an encryption and decryption of proposed extension of AES 128. Every data is segmented into number...
of packets and every new packet having its own unique key and header will be created for each packet. Suppose if 10 chunks of data taken, the private and public key of the data to be different and this will be encrypted securely. We cannot easily find which is an original packet or header because every time it keeps on changing. We are applying our proposed extension algorithm on these data in order to check whether it is secured than an existing algorithm.

**Device Side**

![Device Side Diagram](image)

**Server Side**

**Figure 2: Proposed efficient algorithm of AES 128 with extension methods.**

### Transmission of Raw Data to Cloud

After collecting the raw data from various sensors, the next step is to apply the algorithm and transmit raw data to a JSON format. While doing transmission, first it should converted into hexadecimal format and encrypt it. The sensor data is to be securely stored in the cloud. Fig. 2 shows the flow of operation done in the proposed method. The Table 1 and Fig. 3 show the time required for different process while transmitting the raw data to the cloud based on various data length. The encrypted data will be in binary form which cannot be transmitted over internet as an URL query. So, we need to convert into hexadecimal value.

- Take the first nibble (4 bits) from first byte and find the ASCII value from ASCII table.
- Take second nibble (4 bits) from first byte and find the ASCII value from ASCII table.

Suppose for example, consider 5 bytes of data shown below: Encrypted data= 0x38 0xf9 0x9a 0x1e 0xb5 converted as, Hexadecimal= 0x33 0x38 0x66 0x39 0x39 0x61 0x31 0x65 0x62 0x35

### Table 1: Timing for raw data transmission to cloud for various data length.

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Process</th>
<th>Time(us) for 16 byte</th>
<th>Time(us) for 48 byte</th>
<th>Time(us) for 96 byte</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Encryption</td>
<td>75</td>
<td>180</td>
<td>330</td>
</tr>
<tr>
<td>2</td>
<td>Encrypted data to Hex</td>
<td>90</td>
<td>200</td>
<td>260</td>
</tr>
<tr>
<td>3</td>
<td>Hex to Encrypted data</td>
<td>100</td>
<td>280</td>
<td>550</td>
</tr>
<tr>
<td>4</td>
<td>Decryption</td>
<td>110</td>
<td>350</td>
<td>900</td>
</tr>
</tbody>
</table>
Sensor Data Collection from Cloud and Formatting the Data

The sensor data is securely stored in the cloud. Device collecting the sensor data from the cloud and later that data gets framed into JSON format at the encryption side in the device system. The data gets encrypted using the proposed extension of AES 128 cryptography method and at the decryption side all the steps are done in the reverse order. By using the JSON parser raw data will be generated at decryption side in the server system.

Data framing and data parsing is simple sequencing of collected sensor data into string and parsing is retaining the data from the string. Data framing done at encryption side and data parsing done at decryption side of the proposed system.

Suppose for example, Humidity=75 temperature=38, framed data {“Humidity”:75, “temperature”:38}

The Table 2 and Fig. 4 show with and without encryption and decryption timing between data framing and data parsing for various data length, i.e., 16,32,48 and 64 bytes. Data framing can be done at encryption side and data parsing done at decryption side. In the Table 2, encryption and decryption timing for all data length without using encryption is always zero because we are not applying any encryption method. But the encryption and decryption timing varies for each byte as shown in the Table 2 and Fig. 4.

Table 2: Timing between data framing and parsing of data with and without using encryption at various data length.

<table>
<thead>
<tr>
<th>Data Length</th>
<th>Encryption Timing</th>
<th>Data Framing</th>
<th>Data Parsing</th>
<th>Decryption Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>With Encryption 16 Byte</td>
<td>140</td>
<td>100</td>
<td>130</td>
<td>220</td>
</tr>
<tr>
<td>Without Encryption 16 Byte</td>
<td>0</td>
<td>100</td>
<td>130</td>
<td>0</td>
</tr>
<tr>
<td>With Encryption 32 Byte</td>
<td>150</td>
<td>210</td>
<td>280</td>
<td>230</td>
</tr>
<tr>
<td>Without Encryption 32 Byte</td>
<td>0</td>
<td>210</td>
<td>280</td>
<td>0</td>
</tr>
<tr>
<td>With Encryption 48 Byte</td>
<td>190</td>
<td>330</td>
<td>470</td>
<td>320</td>
</tr>
<tr>
<td>Without Encryption 48 Byte</td>
<td>0</td>
<td>330</td>
<td>470</td>
<td>0</td>
</tr>
<tr>
<td>With Encryption 64 Byte</td>
<td>260</td>
<td>440</td>
<td>660</td>
<td>420</td>
</tr>
<tr>
<td>Without Encryption 64 Byte</td>
<td>0</td>
<td>440</td>
<td>660</td>
<td>0</td>
</tr>
</tbody>
</table>
CONCLUSION

In this paper, partner expansion of AES 128 piece has been proposed to pass on higher security, some additional methodologies checksum, division and rearranging are used in the calculation and this framework utilizes both symmetric and hilter kilter with both private and open key technique to encode the data. Our result shows that the proposed system has a very optimal latency for controlling the system as well as high packet delivery rates and accuracy for mitigating the data. In order to perform of these things proposed algorithm targeted on mitigating the complexity of securing agricultural information. By the experimental results proposed method is more secure because we are using the additional methods in the proposed extension of AES 128 algorithm with security level incorporated using JSON format and encrypted, later adding CRC check sum. In segmentation breaking the packets into chunks of many in a random fashion and transmitting the packet with random number generation. So any interfering cannot decode the data. In this paper, encryption and decryption time for both with and without using proposed method can be calculated, while storing the data at cloud level and along with data shows the encryption, decryption and packet framing process time taken by the controller for various length of data. In the future development of this work, we will concentrate on the improvement of algorithm speed and decryption time reduction.

REFERENCES


