International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

Cloud Based Secured and Energy Efficient IoT System

Shukla Ashish Shivbahadur[1], Dr. Ravi K. Sheth[2]

[1]M. TECH Cyber Security Raksha Shakti University

[2]Assistant Professor (IT), Raksha Shakti University

Abstract: ***Industrial Control system is necessary to collect all the relevant information, statistics and data related to the various industrial parameters of sensors. This is aim of providing better technology to serve the Industry for monitoring and analysing the operation. In this new era of technological developments remote control and monitoring via communication techniques like IoT has been widely used in Industries. However, these IoT techniques are generally restricted to simple applications because of their slow communication speeds, distances and data security. In the Present project, a new solution is adopted for the traditional monitoring and controls of Industrial applications through the implementation of Internet of things (IOT) using cloud enabled Energy efficient and high security without the need for much hardware infrastructure in all the coverage areas of the GSM operator and send the data on cloud for analysis.***

Keywords: Internet of Things (IoT), GPRS, GSM, Sensor module, Cloud

1. Introduction

By Gartner reports that they expect over 20 billion IoT units to be installed by 2020. It is a clear sign that new business opportunities are on there. The Internet of Things (IoT) which includes wearables, smart home applications, autonomous vehicles, smart cities, agriculture. It's a speedily growing part of industries. Some people expect that the IoT industry will at some point connect everything to the internet.

However, there's also a increasing concern about security issues and other threats that is big challenge to the IoT industry. There are so many attacks associated with IoT devices. Most of are Cyber based. Hence, it is very challenging task to secure and manage whole IoT Infrastructure. [1] There are some reasons behind it. 1. Vulnerable web interface: Numerous gadgets and devices have a built-in web server that hosts a web application for managing them. Like any web server/application, there might be problem in the source code that may be cause the interface to be vulnerable to a Cyber based attack. 2. Improper Authentication and Authorization Methodology, 3. Insecure Network Services, 4. Absence of transport layer encryption, 5. Privacy Problem, 6. Unreliable cloud interface, 7. Insufficient security features, 8. Improper management of patches and upgrades.

Here some technologies for security of IoT [2]: 1. IoT network Security, 2. IoT authentication, 3. IoT Encryption, 4. IoT PKI, 5. IoT Security Analytics, 6. IoT API Security.

[8] Here, we are focusing the IoT Encryption, which is symmetric key. This is solution for Industrial automation IoT based sensor and cloud network using GSM module. The main Idea of choosing this IoT sensor Network, GSM, and Cloud because in industry we must implement the sensor at very far away from control station specially in Petrochemical Industry. Where all single data is important, and It should be fast transceiver system available for analysis as well as power efficient and Most important secure. To fulfil our need and overcoming limitation where GSM is efficient to transmit the data on cloud for machine learning & data analysis. But we can't use traditional Encryption technics i.e.- AES, DES etc. we must use light weight encryption technics. For energy efficiency because at remote place we can't provide power continuously hence we have to use battery.

2. Literature Review

So many encryption algorithms are available and used in information security. They can be classified into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption, only one key is used to encrypt and decrypt data. DES uses one 64-bits key. Triple DES (3DES) uses three 64-bits keys while AES uses various (128,192,256) bits keys. Blowfish uses various (32-448); default 128bits while RC6 is used various (128,192,256) bits keys [4].

In Asymmetric keys encryption, two numbers of keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (E.g. RSA and ECC). Public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices. Strength of Symmetric key encryption depends on used key size. There are many examples of strong and weak keys of cryptography algorithms like RC2, DES, 3DES, RC6, Blowfish, and AES.RC2 uses one 64-bit key.

The existing Encryption algorithm in figure-4 has some analysis graphs in the below figures [4].

a) CPU Work Load

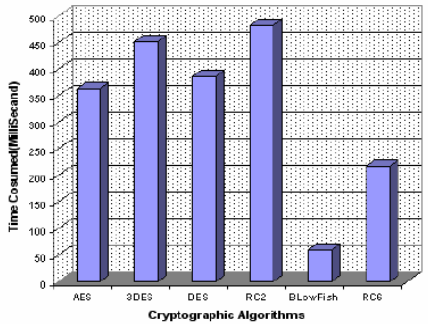


Figure 4: Time consumption for encrypt different Text and Document without data transmission(millisecond) [4]

b) Encryption throughput

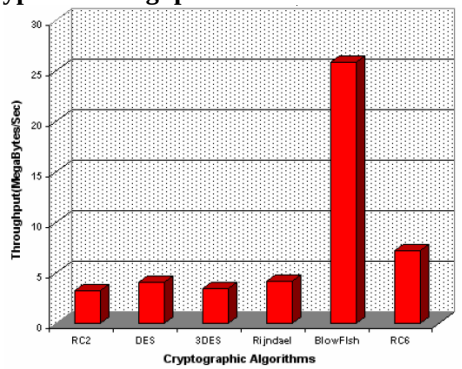


Figure 5: Throughput of each encryption algorithm to encrypt different text data (Megabytes/Second) [4]

c) Power consumption (Micro joule/byte)

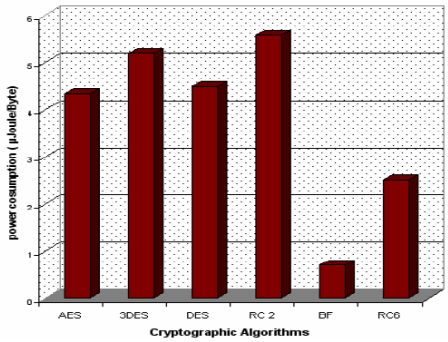


Figure 6: Power consumption for encrypt different Text document Files (micro Joule/Byte) [4]

d) Power consumption (percent of power consumed)

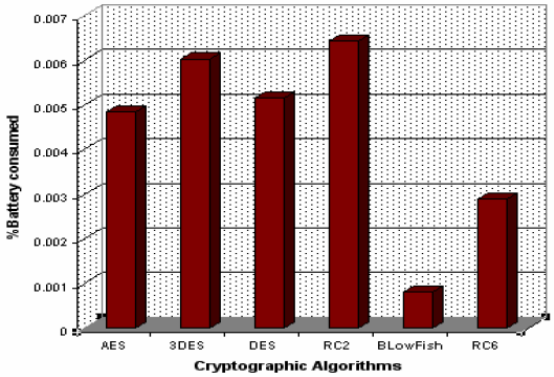


Figure 7: Throughput of each decryption algorithm (Megabyte/Second) for text data without data transmission [4]

Table 1: Comparative execution times for transmission of text data using different encryption algorithms [4]

Text Data					
Data to be transmitted	ad hoc mod(802.11standard)			BBS mod	
	Excellent signals		Poor	Excellent signals	
	WLANs Security Protocol				
	No Encryption(Open System Authentication)	WEP(Shared Key Authentication)	Noise(Poor Signals)	IEEE 802.11i (WPA(TKIP))	No Encryption(Open System Authentication)
	Duration Time in Seconds				
No encryption	10.57	10.76	17.35	17.71	16.1
AES	18.94	18.5	45.93	29.28	25.94
DES	14.38	12.55	21.17	20.72	21.07
RC2	18.82	18.38	61.31	29.29	31.92
3DES	18.05	17.75	30.87	27.47	32.45
BF	10.68	10.93	17.49	19.98	13.93
RC6	10.84	11.13	18.26	20	15.09

In above figures so many encryption techniques listed and their analysis of CPU Work Load, Encryption throughput, Power consumption (Micro joule/byte), Power consumption (percent of power consumed). But it is too high. We should use light weight data encryption technics because our module is in remote place so battery backup should be good it should not drain because of the complex data encryption technique. Here, our main requirement is to encrypt the data which is hardly two digit, hence no need to use complex encryption algorithms.

3. Proposed System

Industrial monitoring and control are a combinedly architectures, mechanisms, and algorithms used in the industry for monitoring and Analysing the activities of industrial processes employed in industry. Though it is good enough to have a smart industrial environment soon, but it will also have to face problem of handling big data as all the devices will communicate with each other and exchange their information over a common platform. This project is focused on Industrial applications that will be continuously monitored through a set of sensors and analyse the data on cloud. The main idea to share the data on cloud to fulfil the two purpose, one to continuous analyse the data it is required cloud platform and also the authority can see and monitor the data online. The proposed architecture is in figure 1:

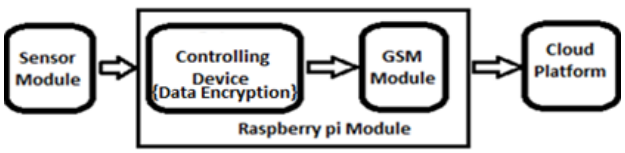


Figure 1: Block Diagram

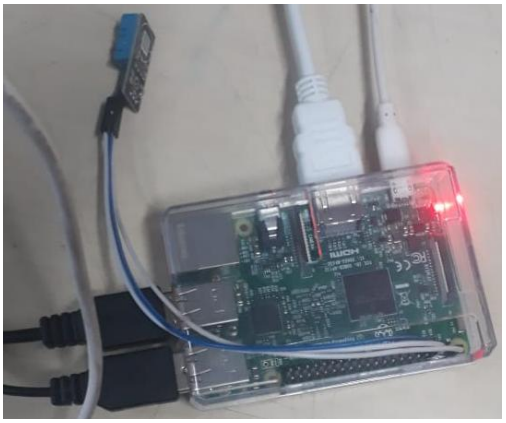


Figure 2

The data from various sensors here temperature sensor and humidity sensor in the sensor module is fed to the controlling device. The controlling device encrypt the data by rail fence algorithm with key = n. This encrypted data is interfaced with a GPRS enabled GSM module to send the data on internet (cloud). On internet cloud service thingspeak is available which is containing its own security authentication by login id and password. An arrangement of data decryption is available which decrypt the data and provide for further analysis.

1) Sensor Module [9]

- Humidity Sensor (DHT11) [10]: DHT11 is +/- 20ppm frequency stability from -55 c to 125 c with.
- Temperature sensor (DS18B20) [10]: 36v low capacitance, low-leakage-current, precision analogy multiplexer. Low on/off leakage currents allow.

2) Raspberry pi 3 B+ Module [3]

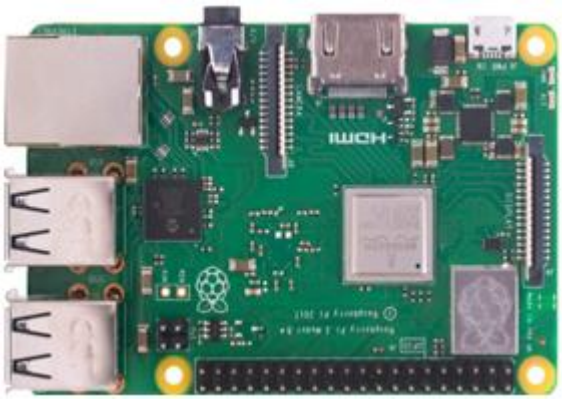


Figure 3: Raspberry pi 3 B+ Board [3]

The new Model B+ has a slightly faster 1.4GHz quad-core Cortex-A53 64-bit Broadcom BCM2873B0 processor that now also features better thermal management to run at sustained speeds for longer without throttling considerably.

The main improvements are to networking. The B+ has dual-band 802.11ac Wi-Fi, which should make it ideal for use on newer 5GHz networks, as well as Bluetooth 4.2. The entire board is now certified as a radio module under FCC rules, which will reduce the cost of conformance testing Raspberry Pi-based products. Gigabit Ethernet is also supported over the USB 2.0 connection and although you won't see the full 1Gbps speed due to USB 2.0 limitations it's still 3x faster than the previous Model B. Power-over-Ethernet support has also been added with separate PoE HAT, improved PXE network and USB mass storage booting.

3) Data Encryption

Our main requirement is to encrypt the data which is hardly two digit, hence no need to use complex encryption algorithms.

The **rail fence cipher[5]** (sometimes called zigzag cipher) is a **transposition cipher** that jumbles up the order of the letters of a message using a basic algorithm.

The rail fence cipher works by writing your message on **alternate lines** across the page, and then reading off each line in turn.

For example, let's consider the **plaintext** "This is a secret message".

Plaintext T H I S I S A S E C R E T M E S S A G E

To encode this message we will first write overtwo lines (the "rails of the fence") as follows:

Rail Fence	T		I		I		A		E		R		T		E		S		G	
Encoding		H		S		S		S		C		E		M		S		A		E

Note that all white spaces have been removed from the plain text.

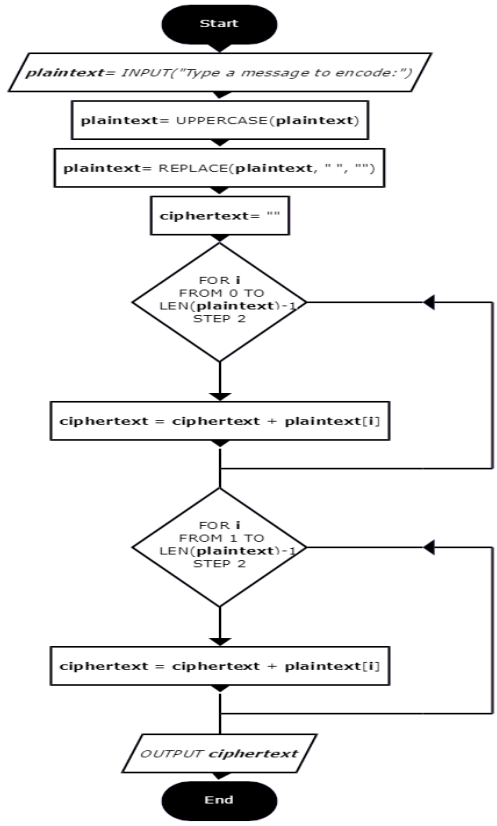
The **ciphertext** is then read off by writing the top row first, followed by the bottom row:

Ciphertext T I I A E R T E S G H S S S C E M S A E

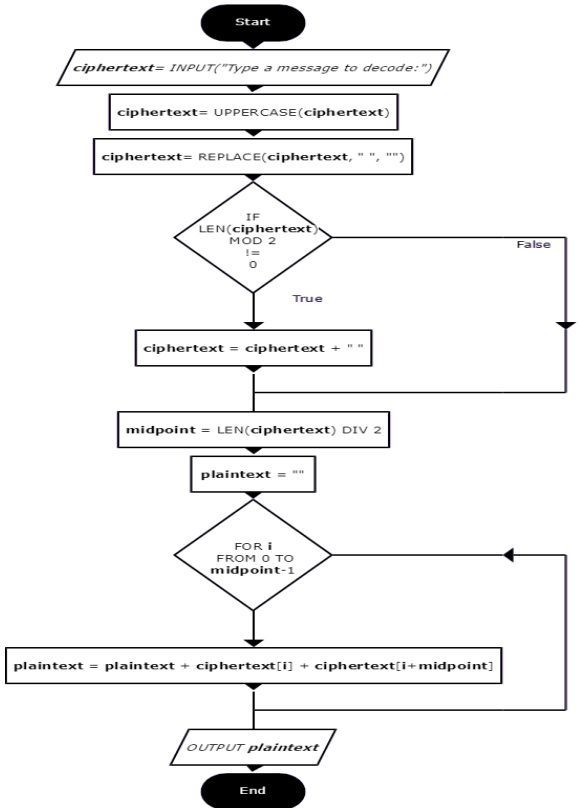
The advantage of this techniques we can vary the depth of encryption as per data sensitivity, but with depth the power consumption increase. Hence, we should be chosen depth carefully.

More complex Rail Fence Ciphers have more "rails". For instance, instead of writing the code over two lines ("rails") you can write over three or four or more lines. The number of lines used in a Rail Fence Cipher is called the **key**.

Data Encryption:



Data Decryption:



4) GSM Module

Here, we are using Inbuilt GSM Module on Raspberry Pi because of we want to transmit our sensor data on internet (Cloud). Hence, only GSM Module can fulfil our purpose with System Resource: 16 Mb+, Network Data Width (kb/s): 64-128+, Coverage Area (meter): 1000+.

5) Cloud

ThingSpeak [6]: The IoT Platform with MATLAB Analytics. ThingSpeakis an IoT analytics platform service that allows we to aggregate, visualize, and analyse live data streams in the cloud. We can send data to ThingSpeak from our devices, create instant visualizations of live data, and send alerts using web services like Twitter and Twilio. With MATLABanalytics inside ThingSpeak, we can write and execute MATLAB code to perform pre-processing, visualizations, and analyses. ThingSpeak helps engineers and scientists to prototype and build IoT systems without setting up servers or developing web software.

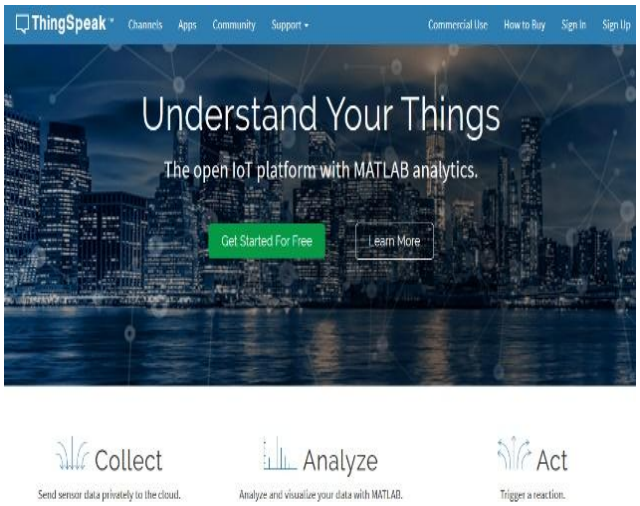


Figure 8[6]

Here, Some top 10 cloud services for IoT [7]

1) AMAZON WEB SERVICES IOT PLATFORM
2) MICROSOFT
3) AZURE IOT HUB
4) IBM WATSON IOT PLATFORM
5) GOOGLE CLOUD PLATFORM
6) ORACLE
7) SALESFORCE
8) BOSCH
9) CISCO IOT CLOUD CONNECT
10) GENERAL ELECTRICS PREDIXSAP

6) Coding step for project implementation

Step 1: Import required library i.e.- urllib.request, threading, json, random, sys, Adafruit_DHT.

Step 2: Encryption: Create the matrix to cipher, Plain text key = rows, length(text) = columns, filling the rail matrix, to distinguish filled, Check the direction of flow, reverse the direction, filled the top or bottom rail, fill the corresponding alphabet, find the next row using, direction flag.

Step 3: Decryption: Define decryptRailFence(cipher, key), create the matrix to cipher, plain text key = rows, length(text) = columns, filling the rail matrix to distinguish filled spaces from blank ones, This function receives cipher-

text and key and returns the original text after decryption def decryptRailFence(cipher, key); create the matrix to cipher plain text key = rows, length(text) = columns, filling the rail matrix to distinguish filled spaces from blank ones.

Step 4: Define a function that will post on thingspeak cloud server every 15 Seconds,
URL='https://api.thingspeak.com/update?api_key=UC74O2MB1WPBE1GM&field1=0'.

Discussion Limitation

The presented model is environment and application limited, it is trade-off between security and battery life of application because if we are using high security algorithm then the battery life is sort and if we are not using proper security algorithm then it unsecure application. Hence, we must balance both as per importance of data and location of site of industry.

4. Conclusion

This proposed energy efficient secure model will help the industry, which is at remote place like petrochemical, cement, fertilizer etc. to monitor and analyse with the help of sensor data for future decision related to maintenance. This is initial model of Energy efficient IoT based Secure Data Transfer on Cloud which is not universal solution of secure IoT based industrial automation, but It is child model of it. Hence, to extend it we can think more secure and more power efficient encryption algorithm.

References

[1] https://blog.learningtree.com/10-internet-of-things-security-vulnerabilities/ [Last access on 15 March 2019]
[2] https://www.techradar.com/ [Last access on 25 February 2019]
[3] https://www.raspberrypi.org/products/ [Last access on 25 April 2019]
[4] Shadi R. Masadeh, ShadiAljawarneh, NedalTurab - A Comparison of Data Encryption Algorithms with the Proposed Algorithm: Wireless Security
[5] https://www.101computing.net/the-rail-fence-cipher/ [Last access on 29 March 2019]
[6] https://thingspeak.com/ [Last access on 20 February 2019]
[7] https://www.devteam.space/blog/10-best-internet-of-things-iot-cloud-platforms/ [Last access on 11 March 2019]
[8] Dr. S.W Mohod, Rohit S. Deshmukh - Internet of Things for Industrial Monitoring and Control Applications.
[9] Geetesh Chaudhari, Sudarshan Jadhav, Sandeep Batule- Industrial Automation using Sensing based Applications for Internet of Things.
[10] https://components101.com/ [Last access on 26 April 2019]