# Security Framework For Iot Devices Based on Cryptography Architecture For Mine Workers

**Dr.P.Kannan[1], R.Mouniprabhaa[2], A.Nisha[3], K.Rajalakshmi[4],Ravi.Divya[5]**
[1]Professor, Dept of Electronics and Communication Engineering
[2, 3, 4, 5]Dept of Electronics and Communication Engineering
[1, 2, 3, 4, 5] Panimalar Engineering College, Anna University, Chennai

***Abstract-*** *All living things need clean air to support their best lives, if air quality is not good humans have health issues. People working in mining industries have exposure to air containing dust particles, toxic gases, high temperature and humidity inside the mining environment. This paper presents remote monitoring of mines working people with the IoT technology and IoT device connected with sensor to measure the parameters and alert the workers regarding the environment. The Internet of Things (IoT) technology growth has increased rapidly in recent years and becoming part of different aspects of our lives. IoT devices are heterogeneous which includes sensor, less resource constrained devices. Due to increased usage of IoT devices, if these devices are not secured properly there is a possibility for software, hardware or network attacks and causes issue for confidentiality and privacy. We try to implement powerful and efficient cryptography function in Arduino microcontroller to make it authenticated and to ensure the confidential data transmission.*

***Keywords***- Internet of Things, Cryptography, Air quality, Arduino, Authentication and Confidentiality

## I. INTRODUCTION

Mine workers face different hard situation in mining environment which causes injury and disease. Miners get exposed to harmful toxic gases, dust particles which causes many diseases as time passes. Miners inside the mines inhale air with dust particles and toxic gases which may lead to disease like asthma, black lung which is a form of occupational lung disease group pneumoconiosis and sometimes mining environment will have high temperature which cause heat stress and this in turn cause a health issue, mining environment are often very humid which cause thermal stress in workers. Over exposure to heat and humidity cause body to become fatigue and distressed,this can result in heart stroke. To avoid unwanted accidents all mining industry should follow some basic precautions and rules. Communication is the main factor for any industry to monitor different parameters and take necessary actions accordingly to avoid any types of hazards [5]. The purpose of air quality monitoring is also to provide the information required by scientists to analysis the human body behaviour with respect to the environment. Safety is an important aspect of industry which should be followed strictly without any compromise, in mining industry human directly involve in work hence additional care should be taken in terms of safety because it directly affects human health [4]. Monitoring the air quality remotely is much more efficient by using the modern technology via implementation of both the software and hardware. To reduce the impact on human health due to various dangerous factors present inside the mines it is important to set up effective monitoring system.

The system utilizes the Internet of Things (IOT) service to transmit the sensed data, sending alert mails to the authorized manager and the Arduino microcontroller is used to process the data. Using Internet of Things (IOT) technology data collected by the sensor such as monitoring human conditions like temperature, humidity, pressure, heart rate, CO and $CO_2$ in air and air quality levels for coal working people is send to cloud and it can be viewed from anywhere and also to send alert messages. when we hear Internet of Things (IoT) we get the mechanism of connecting huge number of devices and allows communication between them through internet and this technique minimizes the role of human being’s involvement in such situations. Our task completes this configuration by introducing autonomous modules that are to be placed on an accessible framework with secure data transmission. In security point of view there are many challenges will be faced by IoT. The following are the reasons for security challenge,1) IoT is an extension of 'Internet' through the mobile network, Sensor network and traditional network etc. 2) through this internet every 'thing' is connected and 3) communication take place between all the 'thing' which are connected with each other in the network. New security issues Will be born we should focus on the issues. We should focus on these issues like Privacy, authenticity, integrity of data [2] and many faces Chances of security issues, such as ethical hacking DoS-like attacks and man-on-centre attacks. And Opportunity to use the device by third parties. Here End Device (Node) is a possible entry point and can damage the interconnections. To ensure that no unauthorized user get access to the devices, some form of authentication method must be implemented. IoT devices is getting targeted by many attackers and 70% of the devices can be attacked very easily [8]. To overcome this security issue cryptography algorithm is applied to the IoT devices. There are several algorithms contributed by cryptography engineering which provides security at different levels to the information the cryptography techniques range between classical [7,3] to elliptical curve cryptography [6,3]. Cryptography is categorized into two types they are, Symmetric Key or Secret key Cryptography and Public Key Cryptography or Asymmetric key cryptography. RSA Algorithm is a public key cryptography used for encryption and decryption process.

## II. PROPOSED SYSTEM

The proposed system id to implement an air quality monitoring system by using the advanced IoT techniques. With the aid of Arduino microcontroller network, the air sensing data over a large coverage area is collected and transmitted to the IoT cloud in time. All the functions of this system are implemented on Arduino microcontroller. The system detects the carbon monoxide CO with the help of MQ6 sensor presence of methane is also measured with the help of MQ3 sensor. Humidity sensor is used to measure amount of water present in the surrounding air and gives electrical signal as output. This water content in the air is an important component in the well-being of mankind. For example, Human body releases sweat when it starts to heat up, it evaporates from skin make to feel cool. Air with high moist present in air cannot evaporate sweat which make to feel hot,hence it leads to excessive sweating, increased respiration. Increased sweating leads to loss of water and chemicals which are essential for normal functioning of the body. Air monitoring can greatly help us understand air pollution and find a way to solve the problem of air pollution partially. Temperature sensor is used to measure temperature in the surroundings. Pulse sensor is used to measure the heart rate of person.

These data are collected by Arduino microcontroller and transmitted to the cloud storage. To get the data from the cloud, the receiver must be an authorized person. The administrator should verify the user. Administrator encrypts token by RSA(Rivest Shamir Adleman) and user should be able return the same token to the administrator this is done securely by using RSA. And the data which is transmitted will also be encrypted and stored in encrypted form in the cloud by performing this, passive attackers targeting communication channels to extract data cannot identify the data.

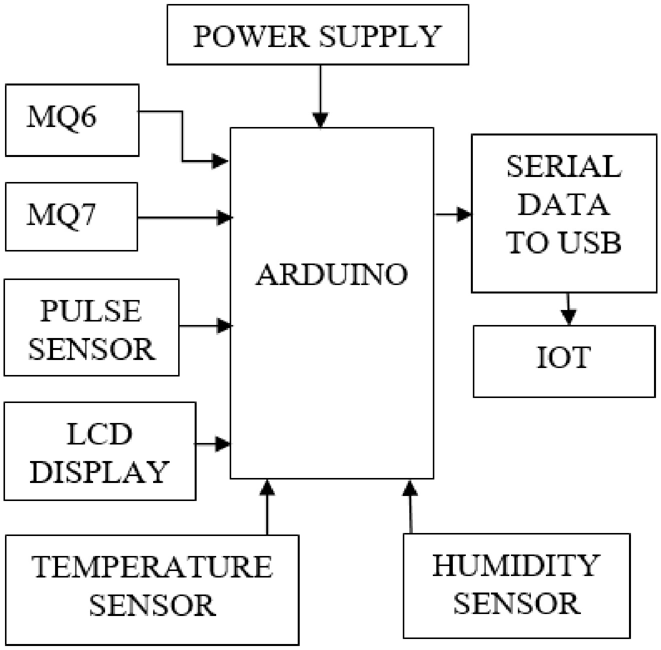


Fig.1 Proposed block diagram

## III. CRYPTOGRAPHY

Cryptography is a method used for protecting information and communications using codes. Cryptography types are, Symmetric Key Cryptography, a single key shared between sender and receiver and same key is used to encrypt and decrypt the message. Asymmetric key cryptography, different pair of keys is used to encrypt and decrypt the information in the system. A public key is used for encryption and for decryption private key is used. Public key and Private Key are different. Symmetric Key Systems use same key to encrypt and decrypt the information since it uses same key it is faster and simpler, but key exchange should be taken in secure manner.

Cryptography provides privacy: When transmitting data, one does not want the knowledge to understand the contents of the transmitted message. The same is true for stored data, which must be protected against unauthorized access, for example by hackers. Validation: This property is equivalent to a signature. The message sent by sender will have cipher text of the original data along with a proof which is the indication that the message is sent by certain authorized party and not from unauthorized persons.

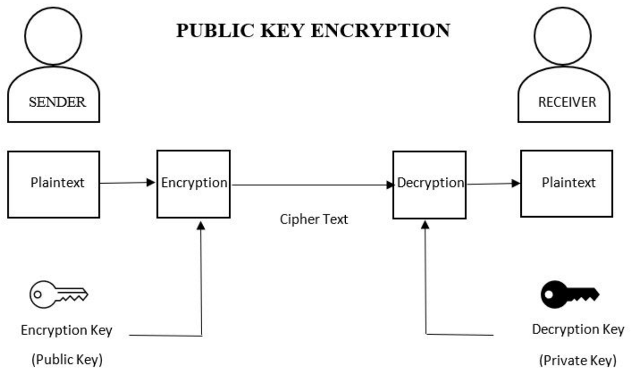


Fig.2 Public key cryptography

### A. RSA Algorithm

RSA algorithm is asymmetric cryptography algorithm. Asymmetric algorithm works with private and public keys which are different keys. The RSA algorithm uses prime numbers and the selected prime numbers are processed by exponentiation and modular arithmetic.

RSA is a set of two algorithms:

- Key Generation: A key generation algorithm.
- RSA Function Evaluation: A function FF, that takes as input a point xx and a key kk and produces either an encrypted result or plaintext, depending on the input and the key.

### B. Key generation

Step 1: A and B which are prime numbers; A = 61, B = 41

Step 2: Calculation of N and$\phi(N)$
N = (A × B)= (61 ×41) = 2501
$\phi(N)$= (A-1) × (B-1) = (60 ×40) = 2400

Step 3: ENCRYPT (e) - public key calculation
ENCRYPT = gcd(e, $\phi(N)$)= 1
ENCRYPT = 19

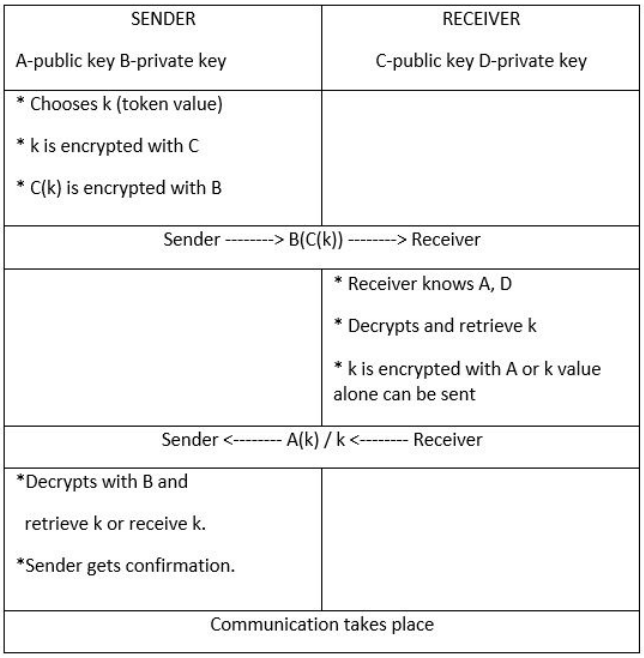
Step 4: DECRYPT(d) - private key calculation
DECRYPT =(h×$\phi(N)$+ 1 ) / e,
for some positive number h.
DECRYPT = ( 3× 2400 + 1 ) / 19 = 379
for the chosen prime numbers, the key values are,
public key {ENCRYPT(e), n} = {19, 2501}
private key {DECRYPT(d), n} = {379, 2501}

### C. RSA function evaluation

1. ENCRYPTION
Data (t) = 50
C (cipher text) = (data)$^{e}$ mod n
C (cipher text) = (50)$^{19}$ mod 2501
C = 2451
2451 is the cipher text of 50.
2. DECRYPTION
Cipher text (c) = 2451
T = (cipher text)$^{d}$mod n
T = (2451)$^{379}$ mod 2501
T = 50
50 data is retrieved from cipher text 2451 by decryption.
Alphabet from words are converted into ASCII values and then the ASCII array of values is encrypted, and the cipher values is decrypted to get the original word.

### D. RSA for authentication

TABLE 1
Authentication done by RSA



| SENDER<br>A-public key B-private key | RECEIVER<br>C-public key D-private key |
|---|---|
| * Chooses k (token value)<br>* k is encrypted with C<br>* C(k) is encrypted with B | |
| Sender --------> B(C(k)) --------> Receiver | |
| | * Receiver knows A, D<br>* Decrypts and retrieve k<br>* k is encrypted with A or k value alone can be sent |
| Sender <-------- A(k) / k <-------- Receiver | |
| *Decrypts with B and<br>retrieve k or receive k.<br>*Sender gets confirmation. | |
| Communication takes place | |

## IV. CONCLUSION

The air quality monitoring design along with sensors to measure temperature, humidity, pulse of workers proposes a superior solution to air complexity, health and environment monitoring for mine workers, this design increase accuracy of sensed value, reduce monitoring cost, more systematic and complete data monitoring is done. If any sensor value exceeds the threshold value the workers are alerted using this system and monitoring person also get alert about the critical environment situation. In this data is securely processed based on RSA cryptography technique, data is encrypted by transmitter and decrypted by receiver. All the sensors and communication device are packed in a compact size to make it portable. This system also allows us to integrate other modules with microcontroller for further enhancement of the system.

## REFERENCES

[1] "Richard A.Mollin An Introduction to Cryptography": 2nd edition. Chapman and Hall/CRC, ISBN-10: 1584886181, 2006 pp 37-39.

[2] Hui Suoa, JiafuWana,CaifengZoua, JianqiLiua ."Security in the Internet of Things: A Review".2012 International Conference on Computer Science and Electronics Engineering.

[3] Qasem Abu Al-Haija, Mashhoor Al Tarayrah, Hasan Al-Qadeeb and Abdulmohsen Al-Lwaimi.,"A Tiny RSA Cryptosystem Based on Arduino Microcontroller Useful for Small Scale Networks", Al-Ahsa 31982, P.O.Box 380.

[4] M. A. Fekih et al., "Participatory Air Quality and Urban Heat Islands Monitoring System," in IEEE Transactions on Instrumentation and Measurement, vol. 70, pp. 1-14, 2021,Art no. 9503914.

[5] Sachin M. Ledange, S.S. Mathurkar. "Robot based Wireless Monitoring and Safety System for Underground Coal Mines using ZigBee". SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE) – Volume 3 Issue 10 – October 2016.

[6] Qasem Abu Al-Haija and A. Al-Badawi. Cost-Effective "Design for Binary Edwards Elliptic Curves Crypto processor Over GF (2N) Using Parallel Multipliers & Architectures". International Journal of Information & Computer Security (IJICS), Inderscience, V.5 (3) 2013.

[7] Q. Abu Al-Haija, et. Al. "Hardware and Software Simulation for Classical Cryptosystem". 4th International Conference on Emerging Niagara Falls, Canada, 21-24, Oct-2013.

[8] Mirza Abdur Razzaq, Muhammad Ali Qureshi, Sajid Habib Gill, Saleem Ullah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study". (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017.

[9] K.M.Ng, M.A.HaziqMohdSuhaimi, A.Ahmad and N.A.Razak, "Remote Air Quality Monitoring System by Using MyRIO-LabVIEW" 2018 9th IEEE Control and System Graduate Research Colloquium (ICSGRC), Shah Alam, Malaysia, 2018, pp. 105-109.

[10] S.Ali, T.Glass, B.Parr, J.Potgieter and F.Alam, "Low-Cost Sensor With IoT LoRaWAN Connectivity and Machine Learning-Based Calibration for Air Pollution Monitoring" in IEEE Transactions on Instrumentation and Measurement, vol. 70, pp. 1-11, 2021, Art no. 5500511.

[11] S. Esfahani, P. Rollins, J. P. Specht, M. Cole and J. W. Gardner, "Smart City Battery Operated IoT Based Indoor Air Quality Monitoring System", 2020 IEEE SENSORS, Rotterdam, Netherlands, 2020, pp. 1-4.

[12] L. Zhao, W. Wu and S. Li, "Design and Implementation of an IoT-Based Indoor Air Quality Detector With Multiple Communication Interfaces",in IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9621-9632, Dec. 2019.

[13] J. Huang et al., "A Crowdsource-Based Sensing System for Monitoring Fine-Grained Air Quality in Urban Environments", in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3240-3247, April 2019.

[14] B. Wang, W. Kong, H. Guan and N. N. Xiong, "Air Quality Forecasting Based on Gated Recurrent Long Short Term Memory Model in Internet of Things", in IEEE Access, vol. 7, pp. 69524-69534, 2019.

[15] S. Sridhar, Dr. S. Smys, "Intelligent Security Framework for IoT Devices Cryptography based End -To- End security Architecture", International Conference on Inventive Systems and Control (ICISC-2017) .

[16] Mohammed El-hajj, Maroun Chamoun, Ahmad Fadlallah, Ahmed Serhrouchni,"Analysis of Cryptographic Algorithms on IoT Hardware platforms", 2018 2nd Cyber Security in Networking Conference (CSNet).

[17] Echo P. Zhang, Junbin Fang∗ , Delta C.C. Li, Michael W.H. Ching, T.W. Chim, Lucas C.K. Hui, S.M. Yiu, "A Simple and Efficient Way to Combine Microcontrollers with RSA Cryptography", Proceedings of the World Congress on Engineering and Computer Science 2013 Vol I WCECS 2013, 23-25 October, 2013, San Francisco, USA.

[18] Rodrigo Roman a, Jianying Zhou a, Javier Lopez b, "On the features and challenges of security and privacy in distributed internet of things", Computer Networks 57 (2013) 2266-2279.