Indonesian Journal of Electrical Engineering and Computer Science
Vol. 18, No. 1, April 2020, pp. 9~15
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v18.i1.pp9-15

Providing enhanced security in IoT based smart weather system

Y. NarasimhaRao[1], P. Surya Chandra[2], V. Revathi[3], N. Suresh Kumar[4]
[1]HOD, Dept of CSE & IT, QIS Engineering College, India
[2,3,4]GITAM Institute of Technology, GITAM (Deemed to be University), India

Article Info

Article history:

Received Jul 19, 2019
Revised sep 22, 2019
Accepted Oct 6, 2019

Keywords:

Arduino
Cloud
Decryption
Encryption
Weather monitoring system
Internet of things

ABSTRACT

Weather reporting system consist multiple devices which are playing dynamic role in producing dynamic environmental parameters such as temperature, humidity, and air pollution. It was a tedious task to bring all the devices together and make them interleaving to produce relevant measurement. Recent trends have proven that the IoT has brought all the devices and peripherals in one place to make more flexible and smart measurement. In the traditional weather monitoring system measurement method is not real time, not continuous and also tedious job to take continuous measurement. But, the IoT has completely changed the measurement scenario and improved the consistency of the measurement. In the present work the environmental parameters such rainfall, temperature, humidity, and density of carbon dioxide in the air are measured with sensors. The Arduino Uno card gathers all information from the devices which are associated with its port pins. The information is sent to cloud server for record and future retrieving. At the same time the data security in cloud been assured with encryption and decryption data while retrieving the information from cloud. This enhances the security, ease of accessing the cloud data from mobile applications, provides wise predictions and minimizes the communication overhead.

Corresponding Author:

Y. Narasimharao,
Department of Computer Science Engineering,
QIS Engineering College, Ongole, India.
Email: narasimha.yamarthi@gmail.com

1. INTRODUCTION

Internet of things (IoT) extends its features beyond its traditional way of device interfacing. It extends its interfacing of network devices with global infrastructures such as electronics equipment, sensors, actuators, and connectivity protocols. The protocols are designed to make establish successful communication between interfacing of devices. The communication comprises of exchanging data values between global infrastructures. The data set consists of several parameters which describe sensory information, controlling information for actuators, synchronous signals [1, 2].

The IoT is associated with other advanced technologies such as cloud computing, security, and Big Data. The accompanying of advanced technologies proved IoT work at high efficiency. The cloud is the base technology used along with IoT in-order to access the sensors and final control elements remotely. In the present work a cloud server is used to store the remotely collected data from each sensor in weather reporting system. As an outcome the resultant system is able to read and maintain sensory data of smart weather system's cloud.

The IoT is defined in different ways in different contexts by number of researchers. Kranenburg defined IoT as, ''a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'Things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the

information network" [3-5]. The recent research proved that billions of devices are interfaced to internet and hence proved the importance of IoT in the current techno world. The recent significant advanced technology made possible of computer and interfacing to take prominent role in the present and future digital world.

In the present work multiple sensors are interfaced to weather monitoring system which is helpful in continuously monitoring the physical parameters such as rainfall, temperature, humidity, and pollution in terms of density of carbon dioxide. In most of the cities; traffic conjunctions, industries, small scale business holders, and daily life activities are becoming clumsy due to bad weather result. These awkward situations can be controlled by monitoring the weather dynamically before users arrive to that particular place or face the situation. Hence a continuous weather monitoring system is required to avoid clumsy times [6]. The continuous measurement involves in several places at different cities and countries produces large data and needs thorough data process. The data creates a large data hull and may cause hazard in system measurement and parameter evaluation. This type of hazard may diminish the performance of the measurement system. The data can be efficiently handled by integrating cloud with the measurement system with the help of internet [7-9]. In this work Arduino Uno is interfaced with sensors to measure parameters and the corresponding data is uploaded into cloud in association with Wi-Fi module.

2. RELATED WORK

In recent decade the Wireless Weather Monitoring System (WWMS) has drastically changed the scenario of people's life, with which technology the daily problems like traffic conjunctions, and other hazardous things can be easily manageable with wireless weather report. This may not be possible without Internet of things [10]. These hazardous and clumsy situations are able to manage by simple internet connections and cloud accessing through several readily available APIs.

In weather monitoring system distributed sensor network plays very important role in predicting the climate condition. Wireless distributed sensor network plays very important role in collecting the information [11-13]. The information is processed at microcontroller [14, 15] and further sent to the cloud, with which the user able to take wise decision in their business or in busy traffic on the road. The cloud server "Thingspeak" is used in the present work to place the sensor information.

In this scenario the cloud plays a key role in IoT communication with the client or user. In weather monitoring system management the internet services and infrastructure integrated in the present system are all interfaced with cloud. The cloud provide services like storing the data and retrieving of data from it is in association with internet services and the corresponding infrastructure utilised in the design. Although the cloud is cost effective but it increases the scalability with minimum cost and the usage also more flexible. Basically, the cloud provides two fundamental functionalities, one is data storage and the second one is data processing or computing. In the present work cloud services are considered for data storage only. In most of the cases the cloud infrastructures are shared by users like enterprises, and individual users. Hence the security issues are became one of the serious issues need to be considered in cloud accessing. Hence the cloud services need to be more trust worthy and hence need to be following some security mechanism before uploading the data to cloud inorder to provide more privacy and security [16]. In weather monitoring system the security is required as there is a chance of knowing user's location and the climate condition at their location. If an individual person checking traffic and climate condition on their travelling path through cloud, there is chance of hackers to know the details. Hence this may give a chance to others to do mischief before they arrive to their home or firm. If the third person knows the details such as location, traffic status, and climate condition, it is easy to estimate the travelling time and their current condition. Hence it is very important to provide trust worthy environment for cloud users [17]. Providing data security in cloud is tricky and complex when compared with conventional information system. The data will be at high risk if security is not addressed in the cloud [18, 19].

Before being late it is very important to take security measurement with respective the cloud data. In the present system a preventive model is discussed inorder to provide more security for the data owners. In the present work the data is uploaded to the cloud after encryption phase. The encrypted data will be uploaded to the cloud, and hence the data cannot be decrypted with appropriate decryption key. This will lead hackers into misperception state. The fundamental model of IoT based sensory model and their levels of data processing is shown in Figure 1.

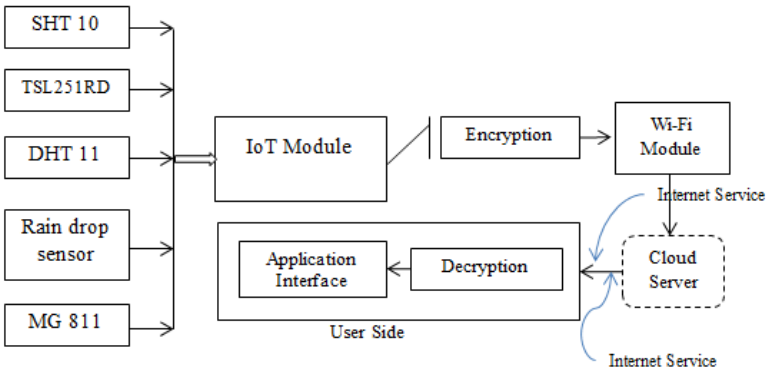

Figure 1. A fundamental model of IoT based system with security

2.1. Circuit Description

In the present model five different sensors are used to measure, they are humidity, object finding, temperature measurement, rain drop sensors, and CO_2 sensors. The SHT 10 is used as humidity sensor and working as, when the humidity changes it affects the conductivity of the substrate present in the sensor and changes the resistance. The change in the resistance modifies the voltage through it and is measured and assessed in-terms of humidity change. The TSL251 used as optical sensor used for detecting objects. The DHT 11 is used as temperature sensor used based on Negative Temperature Co-efficient. It worked based on thermistor working principle. The thermistors are made with semiconductor material. The change in temperature inversely changes the resistance of material. The MG 811 is very good quality of sensing device for CO_2. The working principle of MG 811 is based on electrode reaction in solid electrolyte cell. Two electrode reactions take place when the sensor is exposed to CO_2. It results an proportional electro motive force which changes its value in respective to the gas concentration.

The rain drop sensor board is used to measure the intensity of the rain fall. The rain drop sensing board mainly works based on the principle that the change in the voltage with respect to the change in the resistance. The rain drop sensing board contains some conducting lines which have initially high resistance. When rain drops fall on these lines and increases the conductivity between the lines. It further reduces the resistance and causes drop in the voltage. The drop in the voltage is proportional to the intensity of the rain drops. The experimental work of the current model is represented in Figure 2.

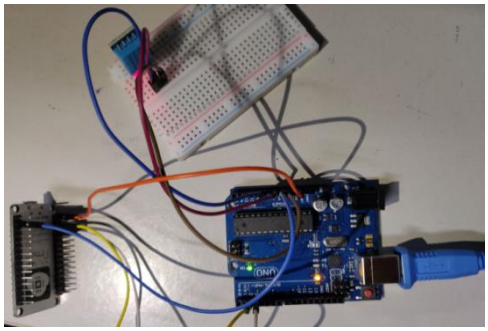

Figure 2. Implementation of present system

3. INTEGRITY OF DATA

This is one of the most important and critical issue in information system. This will provide easy understanding by the users and provides easy interpretation of data. In many cases the data integrity helps to select the cloud services. In the present work this strategy develops an easy method for data retrieve ability [20]. The average accuracy will be improved with proper data integrity [21, 22]. The throughput and accuracy can be further improved by implementing advanced clock synchronization techniques [13, 23]. In the present work all the sensory data is arranged in matrix format for easy understanding, processing, and data retrieving. Each sensor in the design is recognised by particular identification number (ID01 to ID05). The respective sensor outputs obtained at IoT output module are observed on serial monitor as shown

in Figure 3, and simultaneously save at excel sheet for recording, analysis, and future retrieval. The description of the sensor ID numbers and applications is listed in Table 1.

The sensor data (*S*) is taken by IoT module and arranged in 3X2 matrix fashion inorder to apply a security scheme. The matrix values are taken as shown in (1). The sensor values are read into matrix format so it becomes easy for encrypting the data values with specified algorithm. In the matrix only five elements ($ID01_{11}$ to $ID05_{31}$) are representing the actual sensor measured values. The last element $ID06_{32}$ is used for reference value. If the number of sensors increases in the circuit, then the number of elements in the matrix increases and hence the size of the matrix. If any element in the matrix not representing any sensor value except reference value, then the specific element position represented with a NULL value.

```
Current humidity = 62.00%  temperature = 27.00C
Current humidity = 62.00%  temperature = 27.00C
Current humidity = 61.00%  temperature = 27.00C
Current humidity = 60.00%  temperature = 27.00C
Current humidity = 60.00%  temperature = 26.00C
Current humidity = 60.00%  temperature = 26.00C
Current humidity = 60.00%  temperature = 26.00C
Current humidity = 60.00%  temperature = 26.00C
Current humidity = 60.00%  temperature = 26.00C
Current humidity = 61.00%  temperature = 26.00C
Current humidity = 61.00%  temperature = 26.00C
Current humidity = 61.00%  temperature = 26.00C
Current humidity = 61.00%  temperature = 26.00C
Current humidity = 61.00%  temperature = 26.00C
Current humidity = 61.00%  temperature = 26.00C
Current humidity = 61.00%  temperature = 26.00C
Current humidity = 61.00%  temperature = 26.00C
Current humidity = 61.00%  temperature = 26.00C
Current humidity = 61.00%  temperature = 26.00C
Current humidity = 61.00%  temperature = 26.00C
Current humidity = 62.00%  temperature = 26.00C
Current humidity = 62.00%  temperature = 26.00C
Current humidity = 62.00%  temperature = 26.00C
Current humidity = 62.00%  temperature = 26.00C
Current humidity = 61.00%  temperature = 25.00C
```

Figure 3. Observed serial monitor readings on arduino

Table 1 list of Sensors used and Their Respective IDs

Sensor tag ID	Name of the Sensor	Description
ID01	SHT 10	Temperature
ID02	DHT 11	Humidity
ID03	TSL251	Object detection
ID04	Contact sensor	Rain drop sensor
ID05	MG 811	CO_2 sensor

$$S = \begin{pmatrix} ID01_{11} & ID02_{12} \\ ID03_{21} & ID04_{22} \\ ID05_{31} & ID06_{32} \end{pmatrix} \quad (1)$$

4. DATA SECURITY

The data values of matrix are stored into the cloud with security which is highly essential for confidentiality. In the present work Homomorphic encryption technique is used for sensor data encryption. In this work the climate conditions are measured with sensors and uploaded onto cloud with secure homomorphic encryption technique. Here homomorphic encryption technique is used because that is most capable of carrying mathematical computations evolved on data readings. A very complex strategy is implemented to implement encryption with the help of cipher matrix. Although homomorphic encryption is not much suitable for cloud security, but it is most suitable for simple mathematical calculations occurred on data of IoT. The homomorphic encryption avoids all overheads occur in the communication between cloud and consumer. Hence a light weight homomorphic mechanism is suitable and is used in the present work [24, 25]. A unique encryption key is applied on all data elements of the matrix for simplicity.

In the second method an asymmetric encryption is done to enhance the security of the data and more commutative encryption is applied to the data. The private key is used for both encryption and decryption. The asymmetric encryption can be implemented by dividing sensory data into individual chunks.

Encryption:

The sensor values stored in matric format are multiplied with a 3X3 key matrix. If for suppose the key matrix '*K'* is given as in (2) as,

$$K = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \quad (2)$$

Now encrypt the sensor reading by taking individual column of the S and multiply with key matrix as shown in (3),
Where, S^1 is the sensor data obtain from first column of '*S*' matrix. Similarly continue the same multiplication operation with S^2 which is a second column of the *'S'* matrix to obtain ($K.S^2$). Combine KS^1 *and* KS^2 into ingle 3X2 matrix. Now calculate cipher-code by applying mod26 individually both on KS^1 *and* KS^2.

$$K.S^1 = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} ID01_{11} \\ ID03_{21} \\ ID05_{31} \end{pmatrix} = \begin{pmatrix} k_{11} * ID01_{11} + k_{12} * ID03_{21} + k_{13} * ID05_{31} \\ k_{21} * ID01_{11} + k_{22} * ID03_{21} + k_{23} * ID05_{31} \\ k_{31} * ID01_{11} + k_{32} * ID03_{21} + k_{33} * ID05_{31} \end{pmatrix} \quad (3)$$

Decryption:

The cypher-code converted back into respective actual values by evaluating mod26 of inverse of key matrix. The inverse of key matrix is equivalent to,

$$K^{-1} = d^{-1} X adj(K)$$

Now multiply each column of cypher code with each column of inverse key matrix and apply mod 26 on the resultant product matrix to obtain original values. Where d^{-1} is the inverse of determent matrix for key matrix.

5. RESULTS

The sensor values acquired from different sensors interfaced with the IoT module are shown in Table 2. The sensor readings are further scaled to display in user understandable format. The rain drop sensor produce the readings inversely proportional to rain drop fall on the board surface. When there is no drop on the sensor board, that is at dry state it produce approximately an output equivalent to 1024. As the drops increases the reading fall down as shown in Table 2 column 4. In the present work the readings are further transformed into simple values by applying simple scaling factor. For example when the reading is 985 it is transformed into 1000-985=39. Then 39 is converted into fractions like 39/255=0.153. Similarly reading 700 is transformed into a fraction equivalent to 1.17. So that it became easy to compare these values to the standard readings.

The standard readings are encrypted with key represented with (2) and the resultant code is obtained by passing the values into (2). An alphabet code is utilized as key for encryption. The encrypted is uploaded to the cloud. In this manner the sensor data is protected from the attackers. At the receiver end encoded data is retrieved and decrypted with inverse of the key.

Table 2. Parameter Reading Taken at Different Timings During a Day

Temp (ID01)	Humidity (ID02)	Object Detection (ID03)	Rain drop sensor (ID04)	CO2 Emission (ID05)
28	50	1	985	250
29	52	1	965	375
30	53	1	900	400
27	55	1	850	500
25	56	1	800	550
24	58	1	700	600

6. CONCLUSION

The cloud is a favourable technology in the recent IoT technology. The main objective of the organizes and individual persons is reduce the data storage cost and also infrastructure service cost. In the present system a cloud is used in the place of traditional database management system. Using cloud the cost of using database management system is reduced and avoided the management of complex databases. The cloud provides a service for storing the data and retrieving by the consumer. There is no local database connected in the work; here a global database located globally and connected through internet is accessible through anywhere from the world. The cloud allows the consumer to access the data via individual devices

like palmtops, desktops, or mobile phones. This increases the scalability and prediction. In the present work a homomorphic encryption technique is used to provide enhanced security in communication between cloud and consumer. The homomorphic technique is proposed to use in the present work, because the limitations due to communication overheads are minimized. The light weight homomorphic strategies further reduces the demerits of the present security schemes.

REFERENCES

[1] Pallavi Sethi et al., "Internet of Things: Architectures, Protocols, and Applications," *Journal of Electrical and Computer Engineering*, vol. 2017, Article ID 9324035, 25 pages, 2017.

[2] S.Renuka et al., "Statistical Accuracy of Authentication with Biometrics", *International Journal of Engineering and Advanced Technology*, vol 8, issue 4, April 2019, pp1040-1043.

[3] Nallapaneni Manoj Kumar et al., "*Internet of Things (IoT): An Opportunity for Energy-Food-Water Nexus*", 2018 International Conference on Power Energy, Environment and Intelligent Control (PEEIC), 13-14 April 2018.

[4] Nallapaneni Manoj Kumar et al., "*Internet of Things (IoT) in Photovoltaic Systems*", 2018 National Power Engineering Conference (NPEC), 9-10 March 2018.

[5] Kranenburg, R.V., 2008. "The Internet of Things: A Critique of Ambient Technology and the All-Seeing Network of RFID", *Institute of Network Cultures*.

[6] P. Jagannadha Rao et al., "Detection of Rain Fall and Wind Direction using Wireless Mobile Multi Node Energy Efficient Sensor Network", *International Journal of Applied Information Systems (IJAIS)*, Vol 3 No.9, Feb 2012.

[7] Paria Jokar et al., "A survey on security issues in smart grids", Security and communication networks", *Security Comm. Networks* (2012).

[8] Andreas P. Plageras et al., "Efficient IoT-based Sensor BIG Data Collection-Processing and Analysis in Smart Buildings", *Future Generation Computer Systems* (2017).

[9] Nallapaneni ManojKumar et al., "*The Internet of Things: Insights into the building blocks, component interactions, and architecture layers*", Procedia Computer Science, Volume 132, 2018, Pages 109-117.

[10] V Sridevi et al., "Automated Gesture Based Wireless Wheelchair Control by Means of Accelerometer", *International Journal of Engineering and Advanced Technology (IJEAT)*, Vol 9 issue 1, 2019.

[11] N. Suresh Kumar et al. / *(IJCSE) International Journal on Computer Science and Engineering*, "Intelligent Network Design of intelligent multinode Sensor networking", *IJCSE* vol2 (3), 2010, pp. 468-472.

[12] Nashwa El-Bendary, Mohamed Mostafa M. Fouad, Rabie A. Ramadan, Soumya Banerjee and Aboul Ella Hassanien, "Smart Environmental Monitoring Using Wireless Sensor Networks", K15146_C025.indd, 2013.

[13] N. Suresh Kumar et al., "Digital frequency meter using DMA Terminal Count Stop method", *International Journal of Engineering and Technology (IJET)*, vol2 (2), 2010, 34-37.

[14] Jie Yuan et al., "A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion", *Special Section on Security and Trusted Computing for Industrial Internet of Things, IEEE Access*, 2018.

[15] N. Suresh Kumar et. al., "Virtual Software to Design and Interface peripherals with different Microprocessors", *International Journal of Engineering Science and Technology*, Vol. 2(5), 2010, 1143-1146.

[16] Nallapaneni ManojKumar et al., "*Blockchain technology for security issues and challenges in IoT*", Procedia Computer Science 132 (2018) 1815-1823.

[17] R. Latif, H. Abbas, S. Assar, and Q. Ali, "Cloud computing risk assessment: a systematic literature review," in *Future Information Technology*, pp. 285-295, Springer, Berlin, Germany, 2014.

[18] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. "*Achieving secure, scalable and fine-grained data access control in cloud computing*", in: IN-FOCOM, 2010 Proceedings IEEE, 2010.p.1-9.

[19] S.Renuka et al., "Multiple Optimization Services in Cloud Computing for Customers", *International Journal of Recent Technology and Engineering*, Vol 8 No 1, May 2019 pp 3376-3381.

[20] K.B.Priya Iyer et al., "*Analysis of data security in cloud computing*", International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB16), IEEE 2016.

[21] N. Suresh Kumar et al., "A New Method to Enhance Performance of Digital Frequency Measurement and Minimize the Clock Skew" in *IEEE Sensor Journal*, vol 11(6) 2011.

[22] S.Renuka et al., "A Survey on Cloud Data Security", *International Journal of Computer Sciences and Engineering*, Vol.7, Issue.4, 2019, pp.88-95.

[23] N. Suresh Kumar et al., "Multi-dimensional parametric assessment with IoT in acquaintance of digital pipeline", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 9, No. 6, December 2019, pp. 4649-4656.

[24] Abdulatif Alabdulatif et al., "Privacy-preserving cloud-based billing with lightweight homomorphic encryption for sensor-enabled smart grid infrastructure", *IET Wireless Sensor Systems*, july 2017.

[25] Claude Castelluccia, "Efficient and Provably Secure Aggregation of Encrypted Data in Wireless Sensor Networks", *ACM Transactions on Sensor Networks*, Vol. 5, No. 3, Article 20, Publication date: May 2009.

BIOGRAPHIES OF AUTHORS

Dr.Y.Narasimha Rao has received B.E from Jawaharlal Nehru Technological University (Hyderabad, India) and M.Tech from Acharya Nagarjuna University (Guntur, India) and has completed his Ph.D from Andhra University(Visakhapatnam, India). He is dedicated to teaching field from the last 15 years and currently working as Head of CSE&IT in QIS College of Engineering and Technology(Autonomous), Ongole, Andhra Pradesh, India

P. Surya Chandra has more than 11 years of teaching experience and has handled several subjects for IT students. During his experience he has published numerous research papers in various International journals.

vankayalapati Revathi has more than four years of teaching experience and has handled several subjects for IT students. During her experience she has published numerous research papers in various International journals.

Dr. N. Suresh Kumar research of interest is parallel processing, Natural Language Processing, Reconfigurable Computing Systems, Information Communication Technology, and Computerized Process Control Measurement. He is currently working as Assistant professor in GITAM University, Visakhapatnam, India. During his 16 years of experience he has occupied different positions in academic and administration. He has published research papers in various refereed National and International Conferences and journals. The author has also worked as reviewer for some of the conference papers and also working as editorial board member in various reputed journals.