Proceedings of the International Conference on Sustainable Computing and Data Communication Systems (ICSCDS-2023)
IEEE Xplore Part Number: CFP23AZ5-ART; ISBN: 978-1-6654-9199-0

2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS) | 978-1-6654-9199-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSCDS56580.2023.10104878

Blockchain based Lightweight and Secure Aggregation Scheme for Smart Farming

Dr.S. Jegadeesan
Electronics and Communication Engineering
M.Kumarasamy college of Engineering, Karur, India.
jegadeesans@rediff.com

M.Navaneetha
Electronics and Communication Engineering,
M.Kumarasamy College of Engineering, Karur, India.
navaneethamurugesan@gmail.com

P. Poovizhi
Electronics and Communication Engineering,
M.Kumarasamy College of Engineering, Karur, India.
poovizhiparthiban03453@gmail.com

S. Pavithra
Electronics and Communication Engineering
M.Kumarasamy College of Engineering, Karur, India.
spavithra09063@gmail.com

P. Santhiya
Electronics and Communication Engineering,
M.Kumarasamy College of Engineering, Karur, India.
santhiyapalaniappann@gmail.com

Abstract*— Modern farms are just the beginning of India's extensive agricultural sector; nonetheless, misusing agricultural technology reduces crop production. Promoting the use of modern statistics in agriculture can help farmers deal with some challenges. A loss of production occurs when there is a lack of accurate information and communication. These are the topics that our article aims to cover. This Internet of Things (IoT) based software offers a smart tracking platform structure and is designed for an agricultural facility. With the primary goal of reducing water waste throughout the irrigation process, propose a fully intelligent agriculture system based on IoT. Develop a smart agricultural model based on the Internet of Things with the main objective of increasing crop yield by involving various parameters and by using blockchain. This study provides an in-depth understanding to support a contemporary, IoT-enabled blockchain framework to permit a consistent data exchange across many organizations. To provide a consistent record, transmission in the IoT is blockchain-assisted, and this study begin by expanding to the new authentication and key management schemes. Cloud servers use the encrypted transactions to analyze and detect intruders by using a unique deep-learning architecture. A thorough comparison shows the suggested approach offers higher safety and software features. The primary goal of this study is to use a blockchain-based methodology to ensure device safety.

Keywords—Blockchain, Smart farming, and Authentication, Internet of Things, and Cloud server.

I. Introduction

Given the global trend towards new eras and their deployment, the objective of expanding agriculture is crucial. Numerous studies have focused on the issue of agriculture. The accumulated recordings are used to provide information on the many environmental elements. Monitoring not only environmental factors are the most effective way to increase agricultural productivity. More productivity loss is also influenced by several other factors. Automation can thus be used in agriculture to address those issues. Sensor networks statistics acquisition and assignment control for selection assist of clever farming [1].

Due to its self-contained operation, modular-sized hardware platforms, availability, and economical technology, IoT has become a practical tool for computer-aided and self-organized decision-making in agriculture and livestock. Blockchain which can be utilized to increase crop efficiency and prevent loss in production [2]. Precision farming, computerized irrigation planning, crop growth optimization, farmland monitoring, and management of agricultural production methods in crops are some important programs in this area [3]. Several data-gathering epochs will be deployed alongside IoT devices to collect all harvest boom difficulties and information. Implementation of smart village based on IoT for rural development [4].

The info collected is uploaded to cloud servers to alter farmers and interest teams to develop innovative solutions that improve agricultural productivity and quality [5]. Sensor data acquisition and irrigation control in vegetable crops with smartphones and wireless sensor networks for Smart Farm [6]. These difficulties include complicated agricultural issues, yield forecasts, water supply calculations, communications introduce a variety of taxing conditions concerning information sharing, monitoring, and storage and create the complete blockchain atmosphere equally prone to a spread in addition to spoofing, replay, a man in the middle, information poisoning, brute force physical exact devices, and information attacks, realistic attacks are also used [7].

The main objective of the proposed are given as follows,

Achieving automated and self-organized decision-making in agriculture and livestock is now a realistic aim, thanks to the IoT's autonomous operation and modular, scalable, and inexpensive software platform technologies. Precision farming, automated irrigation scheduling, crop growth optimization, farmland monitoring, and improved management of the agricultural production process are a few of the significant uses in this field. A blockchain-based technique used to preserve data is the primary motivator. The initiative aims to implement smart farming through automation and IoT technology. Being in an alert atmosphere is essential for improving the development of productive plants.

II. Literature Survey

The agriculture sector faces significant challenges in feeding the expanding global population. In the future, producing food only through conventional farming will be quite difficult. Using information technology, some academics and business experts are developing smart farming. This takes a look at affords the conceptual version and tool shape for clever farming with network sensor packages if you want to perform the important duties for farmers [8]. The article gives a complete implementation for IoT-enabled agriculture. The creation of a version and device architecture takes into account data analysis, control, and job management, as well as data collection through sensors.

In [9], the article describes an inventive technique for smart farming that involves integrating clever sensor equipment with a clever irrigation system using Wi-Fi communication technology. The equipment specialists in tracking biological characteristics vital to farming operations, such as pH, nutritional level, and soil or water content.

By referring to [10], the study is an illustration of the sophisticated modeling and control techniques employed in modern farming and water supply systems. Our Smart range of factors System effectively sprays the essential vitamins to the needs of the crops after our Smart Sensing System provides results. The approach also can be used to impose pay-per-tool licensing; permitting gadget builders to buy highbrow sets from key vendors at an affordable rate primarily based totally on utilization in place of having to pay excessive license expenses for an infinite variety of IPs.

In [11], our recommended binding-primarily totally based mechanism, IP carriers embed higher finite-kingdom machines into the character IP so that the FSM can be activated through the recommended structures. In the long run, the suggested structures will run during off-peak power hours, connect to sensors to monitor occupancy, trash collection equipment, lighting conditions, and improved irrigation control, and collect their waste.

In this study [12], a gadget is advanced to expose crop fields and control the irrigation machine through the use of sensors (soil moisture, temperature, humidity, and light). A data aggregation method where the intermediate nodes within the network per-process the acquired records and send the computed single-dimensional records to the successor node before the obtained records are immediately transmitted after being received from the predecessor node. Because it combines multidimensional records into single-dimensional records while maintaining excellent operations, records aggregation can reduce record redundancy and communication overhead. Because nodes have limited processing power and bandwidth, record aggregation can help the network last longer. One of the major phases of the IoT is data aggregation. Additionally, under the data set aggregation technique that has developed from a research hot spot, the privacy-legal character of data set aggregation may guarantee the secrecy of sensitive data sets.

This section includes several privacy-preserving datasets aggregation methods that are probably comparable to the use cases for our EBDA software [13].

III. Preliminaries And System Model

A. Blockchain Generation

The block could be sent to all final candidate nodes in the blockchain era method for one to confirm its authenticity. We use the DVAC (designated-verifier anonymous credential) consensus method for this study. The remaining cap potential nodes examine the legitimacy of the block and whether or not its contents have been.

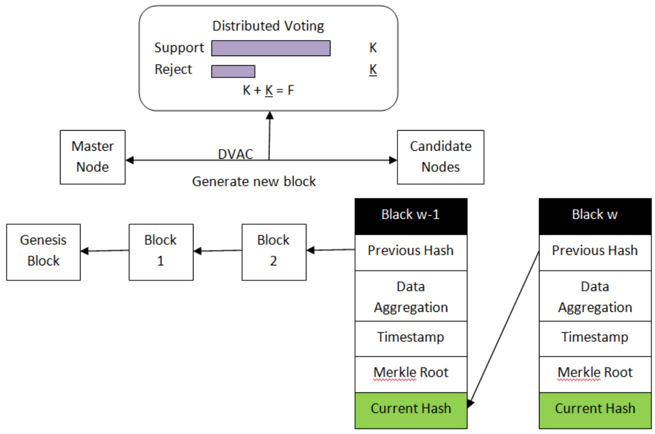

Fig. 1: Generation of blocks

Tampered with. The blockchain generation is shown in Fig. 1, which gives a better idea of the blockchain. The block is considered genuine and can be added to the blockchain after a majority of candidate nodes have reached a consensus. The parameter that sets the applicant nodes' agreement requirement is introduced. The block will be regarded considered legitimate even though the candidate node's very final results satisfy the inequality: The variable extensive type of surviving candidate nodes with opposing views is represented by the approximate form of K, the extensive type of candidate nodes is represented by the approximate form of F, and the threshold, which must be greater than 50%, denotes the extensive type of candidate nodes that are largely aware of the validity of the block and the creation of a blockchain.

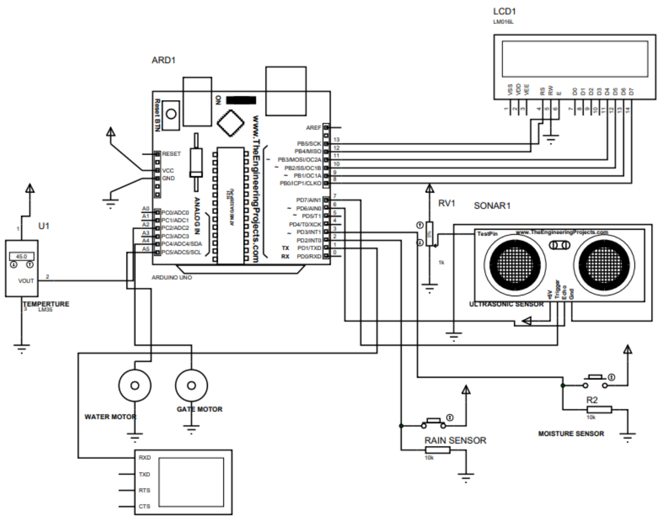

Fig 2: Circuit Diagram

B. System Model:

As illustrated in Fig. 2, this study has investigated a blockchain-based smart network device with sensors, a fog server, trusted authority, and authorized users.

The authority depending on the methods of manipulation is included in the cloud layer. Since trusted authority is completely dependent, it is crucial to the device as a whole. Public keys and parameters are distributed to each entity in the engine via She will disconnect the connection once her preferred chores are completed. The central controller can read, evaluate, store, and output the aggregated data gathered from the hosts due to its capacity to utilize the fog host dynamically in real time. Please keep in mind that the control center reads out the data for each minute region, which means that the data for each area may be per-processed with the resource of utilizing the appropriate location server to allow the tracking center to expose the strength intake at a particular time.

Our answer leverages the Distributed Voting Authorization Certificate (DVAC) on the web page stage to steady the safety and integrity of facts on the web page stage. Each site server announces its computer ownership and network credentials to different site servers during the machine activation process. Each web website online server votes on the threshold servers primarily based it gets from the entities it gets the records from actually, that's very nice. It's worth noting that you can only Vote once on each edge server and that each server has the best voting system.

The candidate node gathers transaction records from the complete web page layer whilst it’s far selected because the candidate node due to the fact the conserving node has closed, transmits the block to all possible ones following integrating the transaction data inside it. Exclusive neighboring nodes approve and vote on the block. A block in the blockchain becomes irreversible if the majority of candidate nodes concur that it is legitimate.

IV. Proposed System

The main source of grain and readily available resources, agriculture is regarded as the "foundation of survival" of the human species [14]. Agriculture plays a crucial role in the development of an agrarian nation. The finest approach to displaying environmental aspects is not the best way to embellish agricultural produce. Numerous other factors also play a role in the increased level of productivity loss [15]. Automation can thus be used in agriculture to address those problems.

This device has sensors for temperature, rain, humidity, and ultrasonic waves. Water level, temperature, and soil moisture content are measured using moisture sensors, temperature sensors, and ultrasonic sensors, respectively, as mentioned in Fig 3. For the farmer to have good access to the measured parameters from any place, they are uploaded to the Internet of Things.

A. Ultrasonic Sensor (HC-SR04): An ultrasonic sensor is a piece of technology that uses ultrasonic sound waves to detect the distance to a target item and then turns the sound that is reflected into an electrical signal.

B. Temperature Sensor (DH11): To record, monitor, or communicate temperature changes, a temperature sensor is an electronic device that monitors the temperature of its surroundings and turns the input data into electronic data.

C. Rain Sensor: A switching device that is triggered by rainfall is known as a rain sensor or rain switch.

D. Moisture Sensor: The volumetric content of water in the soil is measured using a variety of sensors, one of which is the soil moisture sensor. Drying, sample weighing, and elimination of the straight gravimeter dimension of soil moisture are required. These sensors use other soil laws, such as the dielectric constant, electrical resistance, neutron interaction, and replacement of the moisture content, to indirectly estimate the volumetric water content.

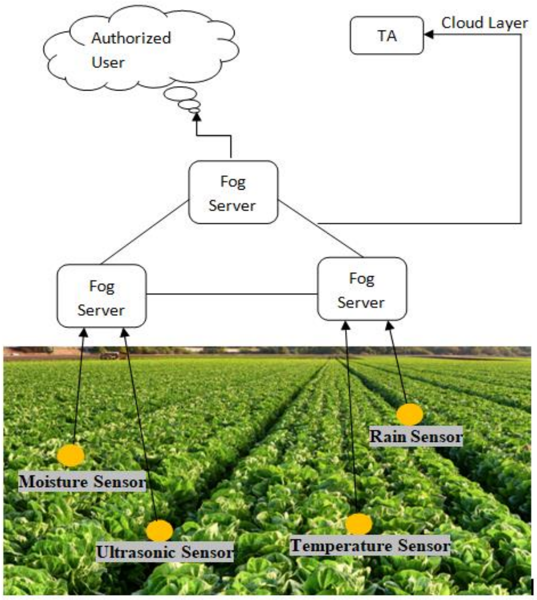

Fig 3: Block diagram

A. Module about Deep Learning:

The part provides a deep learning model to detect intruders in the enabled environment. Deep getting-to-know fashions outperform conventional statistical or gadget-getting-to-know strategies while managing large quantities of data. Numerous research papers and publications [1–11] have described and verified this phenomenon. Consequently, deep learning is preferable to conventional statistical or machine learning approaches. To improve on enabled, this study offers a revolutionary deep learning architecture. The contractive sparse automatic encoder (CSAE), closed recurrent unit network, multilateral perceptron, and SoftMax classifier have been incorporated into this method and are shown below:

A. *Contractive Sparse Auto Encoder Layer:* The autoencoder () is an unsupervised learning technique that consists of two parts: a decoder and an encoder. As can be observed, the encoder transforms the input into a concealed illustration using a settled transformation matrix with highly nonlinear.

$$YT = F(Ł_1 DT + \beta_1) \quad (1)$$

Where $Ł_1$-weight between the input denoting the difference and the decoder uses the variable to recreate the output.

$$cDT = F'(Ł_2 \mathrm{DT} + \beta_2) \quad (2)$$

Component In which the significance of the veiled presentations *YT*, by lowering the following cost function while becoming familiar with the conditions of *AE*, the primary goal of *AE* is to reduce the reconstruction error for a given training set.

$$\{Ł_1, Ł_2, \beta_1, \beta_2\} = \underset{Ł_1, Ł_2, \beta_1, \beta_2}{\operatorname{argmin}} \{ \mathscr{L}_{\mathrm{AE}}(Ł, \beta)$$

$$= \underset{Ł_1, Ł_2, \beta_1, \beta_2}{\operatorname{argmin}} \{ \quad \frac{1}{2\mathrm{N}} \sum_{\mathrm{T}=1}^{\mathrm{N}} \mathcal{L}(D_{\mathrm{T}}, \hat{}D_T) + \frac{\lambda}{2} \sum_{r=1}^{2} \| D_{\mathrm{T}} \| 2_{\mathrm{F}} \; (3)$$

The training pattern and its reconstruction result are each represented by D_T. The total number of training samples, *LDT,* and *cDT* is *N*. Displays the loss function. This can be lessened by square error or cross-entropy. λ Refers to the phrase for normalization that helps to generalize the model. The *SAE* function is set to and is generated by summing a deficiency term of penalties for such *AE* gradient descent.

$$\mathscr{L}_{\mathrm{SAE}}(\hat{}Ł_1, \hat{}Ł_2, \beta_1, \beta_2) = \mathscr{L}_{\mathrm{AE}}(Ł, \beta) + \eta \sum_{J=1}^{\mathrm{M}} KL(\varrho \| \hat{}\varrho^J) \quad (4)$$

Algorithm 1 evidence of authority for checking and including blocks1:

1: State: *CS € IDs* Set of orders,

2: $D_i = (Ki, F_i)$ A_i local node blockchain F_i is a block DAG A_i and the pointer F_i

3: indicates Bloc documents

4: parent and b front node

5: who signs and totals block b; orders

6: Next, the network will receive a separate block.

7: time length, each block requires time to inspect before being presented

8: *PROPOSE () k*

9: *while True*

10: step ← *CT / duration, CT → clock time*

11: *if k €* $CS1Astepmod|CS1| ==$ *k then*

12: $b.parent \leftarrow 1b(Ci), 1b \rightarrow lastblock$

13: $b.CS \leftarrow F_i$

14: $b.step \leftarrow step$

15: $D \leftarrow (A_i \cup b, F_i \cup b.parent)$

16: $disseminate\ (i\ )D$

$sleep\ (duration)$
$endif$
$endwhile$
$endfunction$
$functionSCORE(A\_i, F\_j)$

return $UNIT256 - MAX * height(A_i, F_i) - step - num(A_i, F_i)$

end function
function $DELIVER\ (A_i, F_i)$

if$Score(A_i, F_j) > Score(A_i, F_i)$then

$Score(A_i, F_i) \leftarrow Score(A_i, F_j)$
$endif$
$endfunction$
$functionISDECIDED(b)k$

$V \leftarrow \{b_i.UAV|b_i \in A_i \wedge b_i.step \geq b.step\}$

$Return(|V| * 2 > |CS1|)$

$endfunction$

B. Software and Hardware requirements

The microcontroller is programmed using the Arduino IDE. Before being implemented in a real-time application, the module is simulated using the Proteus program.

Arduino Uno is used as a microcontroller, LCD to Display values, Ultrasonic Sensor, Moisture Sensor, Temperature Sensor, Rain Sensor, and Motor.

V. Performance Analysis

In this part, we usually assess how well our EBDA theme performs in terms of safety, computational overhead, and therefore news coverage overhead. We frequently start by comparing the EBDA plan to the conventional system, which is not yet combined with blockchain technology. While the blockchain partially enables the three-tiered smart grid system, the old scheme gives the statistics aggregated scheme. EBDA provides less vulnerable capacity and attack resistance than a traditional system. Simply put, EBDA is vulnerable to the same assault, but it is far less likely to be attacked across different staging environments. The water motor turns on when the temperature is high and the water level is high but the moisture level is low. The rain motor turns on when the level of rainwater is higher and opens to drain the extra water from the field, enhancing crop health and yield. There is no need to turn on the motor when the outside temperature is low, the water temperature is high, the moisture level is low, and the water motor is in good functioning order. Likewise, when the outside temperature is low and the rain motor is no longer open. Temperature can be low, water stage can be excessive, and more; however, the moisture stage will be low, so the water motor is in good condition and running. The rain is low, and the rain motor will no longer be open. Temperatures can be low and water stages excessive; however, moisture stages will be low, so the water motor is in good condition and running. The rain is low, and the rain motor will no longer be open.

VI. Security Analysis

In this part, we examine the EBDA scheme's overall general protection performance. We estimate the likelihood that the attacker will launch the injection attack using solid records in the side layer.

Security features of different methods

Security Features	**Schemes**				
	[11]	**[12]**	**[13]**	**[14]**	**Ours**
Mutual authentication	✓	✓	✓	✓	✓
Anonymity	✓	×	✓	✓	✓
Untrace ability	✓	✓	×	✓	✓
Message modification attack	✓	✓	✓	✓	✓
Session key agreement	×	✓	×	×	✓
Replay attack	✓	✓	✓	✓	✓

Table 1: Security Features

Through every theoretical evaluation and simulation, we compare the EBDA system against the conventional approach. Our intention with the advent of blockchain is to enhance the general safety overall performance of the aspect layer, so we most effectively want to consider the assault case at the resistance to threshold layer. Wireless Sensor Network for Precise Agriculture Monitoring. The nearby hold node is identified as an ability contender component with precise block ownership. Basic Guidelines for Deploying Wireless Sensor Networks in Agriculture. We account for three attack methods and estimate the typical location risk of an effective attack for each plan. The same requirements apply to each scheme: (1) The assault to objectives is confined to the web page server and management center; (2) To release a hit forgery facts injection assault, additionally referred to as a community assault, the attacker desires to have to manage over as a minimum the fog servers; and (3) All aggression strategies are independent.

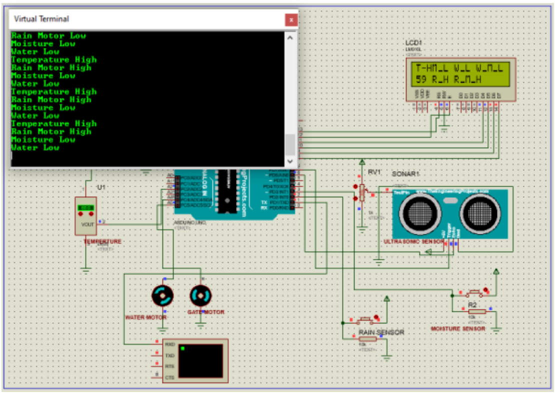

Fig 4: When rain motor runs

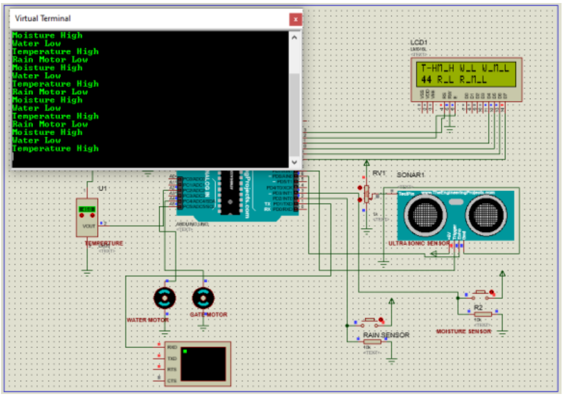

Fig 5: When the motor is in the off condition

VII. Conclusion and Future Scope

Fully intelligent farming technology is mainly based on IoT and blockchain, which can be very beneficial for farmers, and a lack of information is not always good for farming. Threshold values for climatic situations can be completely related to the environmental situations of this individual region at all times. This technology can inform the farmer or authorized users whether there is a need for irrigation or not and related parameters. Continuous community connectivity is required. By using fog servers and cloud servers, which additionally consist of blockchain technology, we ensure the secure transfer of aggregated data. The results can be packaged into transactions and saved within the blocks of the blockchain.

In the future, we will be able to monitor fields in real time using camera modules to prevent both humans and animals from stealing and damaging crops.

References

[1] SinungSuakanto, Ventje J. L. Engel, Maclaurin Hutagalung, Dina Angela, "Sensor networks data acquisition and task management for decision support of smart agriculture," in 2016 International Conference on Information Technology Systems and Innovation (ICITSI) Bandung – Bali, pp. 24–27, Oct. 2016.

[2] Edge Blockchain Assisted Lightweight Privacy-Preserving Data Aggregation for Smart Grid Weifeng Lu, Zhihao Ren, Jia Xu , Member, IEEE, and Siguang Chen, Member, IEEE

[3] NarayutPutjaika, SasimaneePhusae, Anupong Chen-Im, PhondPhunchongharn, and KhajonpongAkkarajitSakul, "A control system in intelligent agriculture by using Arduino technology," in Fifth ICT International Student Project Conference (ICT-ISPC), 2016.

[4] Subramani, J. et al. (2021) "Lightweight batch authentication and Privacy-Preserving Scheme for the online education system," Computers & Electrical Engineering, 96, p. 107532. Available at: https://doi.org/10.1016/j.compeleceng.2021.107532.

[5] Rajalakshmi P and S. Devi Mahalakshmi, IOT Based Crop-Field Monitoring and Irrigation Automation.

[6] Subramani, J. et al. (2021) "Lightweight batch authentication and Privacy-Preserving Scheme for the online education system," Computers & Electrical Engineering, 96, p. 107532. Available at: https://doi.org/10.1016/j.compeleceng.2021.107532.

[7] Subramani, J. et al. (2021) "EPPAS: Energy-efficient privacy-preserving and physically secure mutual authentication scheme for secure communication in Smart Grid Systems," International Journal of Communication Systems, 34(8). Available at: https://doi.org/10.1002/dac.4788.

[8] Jegadeesan, S. *et al.* (2020) "EPAW: Efficient privacy-preserving anonymous mutual authentication scheme for wireless body area networks (WBANS)," IEEE Access, 8, pp. 48576–48586. Available at: https://doi.org/10.1109/access.2020.2977968.

[9] S Niranchana, E Dinesh, "Optimized" 2013 International Conference on Information Communication and Embedded Systems (ICICE) IEEE.

[10] Nandagopal C and Ramesh, S.M. (2020) "An efficient data gathering technique using optimal minimum coverage spanning tree algorithm in WSN," Journal of Circuits, Systems, and Computers, 29(14), p. 2050225. https://doi.org/10.1142/s0218126620502254.

[11] Dinesh E, (2013) "E-farming using cloud computing," International Journal of Cloud Computing and Services Science (IJ-CLOSER), 2(5). Available at: https://doi.org/10.11591/closer.v2i5.5192.

[12] Nandagopal C. (2020) "An effective data filtering scheme based on the context in VANETs," 2020.