ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Emerging Greenhouse Technology

[1] Karthikeyan,
[1] Department Of Computer Science and Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
[1] s.karthikeyan@Galgotiasuniversity.edu.in

Abstract: The rising greenhouse technology in the agriculture dependent on IOT i.e. Internet of Things utilized for automation and remote monitoring has been quickly created. Greenhouse Technology is a technique of giving good environment to the plants. This is fairly used to shield the plants from unfavourable climatic conditions, for example, precipitation, wind, extreme temperature, diseases, insects, excessive radiation and cold. But it despite everything has significant worry about privacy and security, due to the huge size of spreading nature of the network. To beat these security challenges, it use blockchain that permits the production of a disseminated digital ledger of the transactions which is shared between nodes on the IOT network. The fundamental point of paper is to give lightweight blockchain dependent architecture to smart greenhouse farms for providing privacy and security. Here, IOT gadgets in the greenhouses which go about as blockchain oversaw centrally to upgrade energy consumption have an advantage of the private unchanging ledgers. Furthermore, it shows a security structure that mixes the blockchain innovation with the IOT gadgets to give a secure communication stage in the Smart Greenhouse farming.

Keywords: Blockchain Innovation, IOT,Privacy, Security and Smart Greenhouse Farming.

INTRODUCTION

The improvement of IOT i.e. Internet of Things has prompted colossal IOT applications for example, smart city, smart healthcare, smart farming, smart home, industrials internet and smart retails. With the expanding populace, conventional type of farming can't fulfil individuals' requirements. IOT dependent smart farming has become the unavoidable method of agricultural data. Smart farming can give control of farm equipment and remote monitoring through GMS i.e. Greenhouse Monitoring System. GMS is fixed by scientific management strategies to improve the quality, productivity and protect from atmospheric disaster. In any case, there are numerous specialized challenges that should be tended to as far as smart farming. For instance, data sharing foundation is inadequate because of absence of mechanism for sharing delicate agriculture information in privacy ensured way[1].

Moreover, existing detecting foundation permits sporadic observing by means of remote sensing satellite that makes enormous delay to detect the state of soil, effect on production and plant. Existing security strategies could be costly as far as processing overhead and energy consumption for IOT gadgets. This current security system is overseen by focal server and not lean toward IOT gadgets. Consequently, Smart Farming requires scalable, lightweight and distributed privacy and security. To satisfy the above difficulties of IOT, it present the Blockchain innovation. Blockchain is the shared distributed ledger innovation that records agreements, sales, transaction and contracts. Initially blockchain was created to assist crypto-currency, and the present blockchain can be employed in any type of the transaction without a go-between. Blockchain is the database that keeps up a ceaseless rising arrangement of information or transaction records[2].

It is circulated in nature, with the goal that taking part nodes have a duplicate of chain and information records included to the chain. At whatever point another transaction is included to chain, all participants in network will approve it. A lot of endorsed transaction will be packaged in block that will be sent for all the nodes in network. Furtherly, it will approve new blocks. Every one of progressive block comprises a hash conveying an interesting component of the previous block. Subsequently, blockchain can possibly satisfy the current IOT challenges for example it is secure, private and distributed essentially[3]. In this paper, it propose a system to Smart Greenhouse farming dependent on blockchain, which gives lightweight and decentralized privacy and security. Because of low asset capacities of immense larger parts of IOT gadgets, enormous scale, heterogeneity between different gadgets and inaccessibility of institutionalization are the significant worry for the IOT security. A lot of data gathered and shared through the IOT gadgets causes a client's privacy worry. A privacy management technique which figures the danger of revealing information to other people, in any case, in some circumstance, the apparent bit of leeway of IOT services surpasses the danger of privacy loss[4]. Difficulties, for example, anonymity, security

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

and decentralization in IOT are tended to by embracing blockchain innovation, as it disposes of a solitary purpose of disappointment, expanded immutability and data transparency.

SYSTEM MODEL

The framework model comprises of 4 gatherings: cloud storage, Smart Greenhouse, end user and Overlay Network (Fig. 1).

- *Smart Greenhouse:*

It is agriculture domain, which is secured with shade to shield crops from environmental changes, and outfitted with a few IOT sensors (humidity, water level sensors, CO2 sensors, light sensor) and actuators (Fan, sprinkling, heater and LED light). Furtherly, it additionally comprises Local Blockchain (for example Smart Hub) called as private and secure blockchain which is stored and mined by at least one asset able gadgets. The local blockchain is focally overseen by proprietor[5]. The proprietor can include or evacuate gadgets by beginning transaction or erasing its ledgers separately.

All the gadgets in the smart greenhouse can speak with others by allowing the consent by providing them the symmetric shared key dependent on algorithm of chaos cryptographic. Local blockchain has the policy header that consists the rundown of all the access control by which proprietor permit to oversee transactions in the smart greenhouse. Miner of every block includes a pointer to the past block and duplicates the policies in previous block header for new transaction[5]. When a block is added and mined, this is considered as genuine transaction. Smart greenhouse likewise contains local stockpiling for storing information.

Smart Greenhouse is an automatic, smaller scale atmosphere controlled atmosphere for ideal plant development. It is done by utilizing acrylic sheet. Screw and clamp is employed to join the acrylic sheet. For developing vegetables in the Smart Greenhouse it has estimated and control various sorts of parameters like humidity, moisture and temperature of soil. In the wake of controlling these sort of the parameter atmosphere is naturally controlled. As a result of the automatic control of the parameter development of plant is fast[6].

Sensor sense parameter and signal provides for controller and the controller control parameter as indicated by necessity. Prerequisite is reliant on the season like summer, monsoon and winter. In winter season, inner temperature high and external temperature low so plant access satisfied atmosphere, In summer season inner temperature low and external temperature high So plant access comfort condition, In monsoon season external temperature is as per climate and inward temperature is as per climate So plant access comfort condition. Likewise, humidity control is extra element which is dealt with for better development of plant[7].

- *Overlay Network:*

Here, overlay network is like bitcoin network where every basic node can be high assets gadgets prepared in greenhouse. In the overlay network, to lessen network overhead and defer each node can frame a bunch known them as cluster, in the meantime cluster can choose its pioneer known as the CH i.e. Cluster Head. Each node has would in general change its pioneer at whatever point it face unnecessary deferrals. The CH of network, deal with overlay blockchain which conveys all multiset transactions which sent by the cloud storage also access transaction.

Furtherly, the CH oversees whether to keep another block or this should discard, relies upon getting transactions. Some time to invent another block transaction increases higher postponement or client needs to oversee more than each gadget in turn[8]. This can be overseen by shared overlay, wherein common miner for example shared storage and CH are chosen. Overlay gadgets in Greenhouse can keep up a table exists the all information of last transaction for example hash of data and block number. The Tor is employed to interface all nodes with the overlay network.

- *Cloud Storage:*

In critical state of crops in greenhouse, clients need a few technical direction from an expert. Gadgets in the greenhouse stores its information in the cloud storage, with the goal that an expert can legitimately get to information of greenhouse from cloud storage and give services concurring circumstance. The information put away in cloud incorporates client's identical blocks with extraordinary block number. For validness, hash data and block number are utilized[9]. When information is put away in the cloud, the block number is encoded by shared key got from chaos dependent cryptographic algorithm. Since the hashes are impact safe, in this way makes ensured for genuine clients can get to information and furthermore chain fresh information to a current ledger.

- *End Users:*

End users allude to proprietor of smart greenhouse. Thus, clients can remotely control also oversee by utilizing the gadgets, for example, computer and smart mobile.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

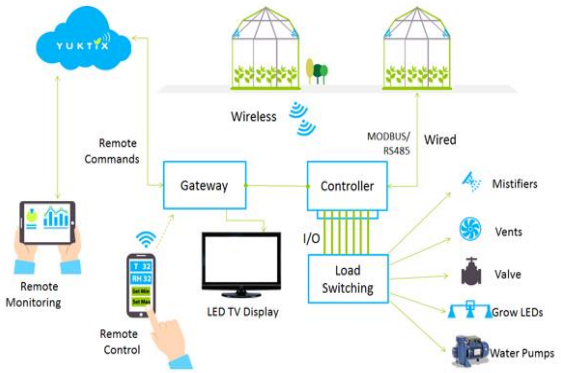

Fig. 1: A Proposed Framework for Blockchain based Smart Greenhouse Farming

SECURITY THREAT

Because of heterogeneous nature of asset compelled IOT gadgets, smart greenhouse farming may be vulnerable against various security attacks. This is important to distinguish different dangers and potential countermeasures so as to plan a compelling arrangement. In the smart greenhouse farming, following threats classifications are distinguished:

1. *Threats on accessibility:*

This risk worries about unapproved endorsing assets. So the principle point of attacker is to keep the lawful client from getting to its information and services.

2. *Threats on integrity:*

Unapproved clients can change genuine data so that it can include the bogus data or manipulate information[10].

3. *Threats on confidentiality:*

These are worried about unapproved client can reveal the delicate data.

4. *Threats on authenticity:*

Worried about unauthorised clients access assets and sensitive data.

SECURITY FRAMEWORK

Fig. 2 depicts the security system which comprises of the accompanying layers.

- *Physical Layer:*

Some dangers against access control and authentication are conceivable so attackers can hack gadgets that prepared in the smart greenhouse. Here, each transactions are straightforward to client as the local blockchain is mined in the smart greenhouse. Subsequently attackers can't include new gadgets for smart greenhouse since all gadgets are pre-characterized by the client and a beginning transaction is used formining in local Blockchain [11].

Along these lines, it is incomprehensible for an aggressor to assault on physical layer. In the interim, Smart hub, for example miner centrally procedures the incoming also outgoing transaction. The transaction that is gotten from overlay network is approved by the miner before sending them for devices. Thus, the miner satisfies authorized, authentication and audit transactions just as creating genesis transaction, distributing and updating keys.

- *Communication Layer:*

This layer embraces disseminated overlay blockchain network for providing security from transmitted information and to lessen overhead delay. Here, potential dangers are against the mining attack and dropping attack. To accomplish dropping attack, an assailant must have command over CH. Controlled CH ought to be drop every single received transactions and blocks.

In the proposed architecture, all the nodes in the clusters have position to choose its pioneer. In such condition, all nodes in similar clusters choose new CH. To accomplish mining attack, attacker ought to have authority over the different CHs that sign multisig transaction with the goal that it can mined phony block. In its proposed architecture, all transactions of getting blocks are approved by the CH. In some circumstance, If CH can't recognize a phony block, it can caution all different CHs[12].

- *Database Layer:*

In Blockchain, conveyed ledgers are a sort of the decentralized database that stores records individually. Each record in ledgers comprise one of a kind timestamp and cryptographic. Private Blockchain maintains track transaction and it comprises policy header where dependent on polices deals with the incoming also outgoing transaction.

Each transaction is binded together as immutable ledger in the blockchain. In the meantime, each block consists block header, which convey hash of previous block to manage blockchain immutable and strategy header that is employed for authorizing gadgets and apply policy created by legitimate clients.

- *Interface Layer:*

Attacker may attempts to make distinctive transaction with various IDs. In the proposed architecture permit clients to send self-assertive transaction to overlay

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

network. In the interim, each PKs and IDs are alterable for every transaction. In this manner, accomplished secrecy[12].

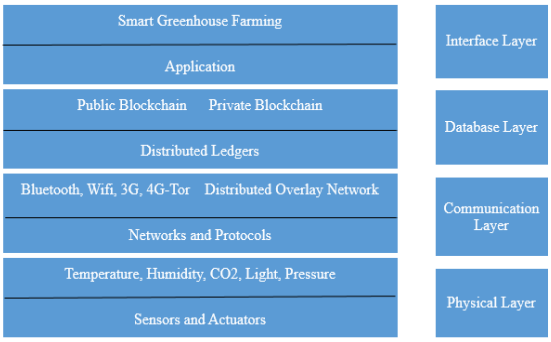

Fig. 2: A Security Framework

CONCLUSION

This paper introduces the advancement of blockchain dependent smart greenhouse farming system to accomplish the IOT privacy and security issues. Because of high energy utilization and preparing overhead existing security arrangements are not fit. A greenhouse gives a controlled situation modified to the vegetation requirements cultivated inside. Customarily, agronomic and micro-climate parameters have been saved in a somewhat manual and conflicting way.To satisfy these challenges, it approach blockchain, that address these difficulties by holding bitcoin blockchain consists permanent ledgers of blocks. It present this thought regarding Smart Greenhouse farming for satisfying a safely observing. It proposed a structure to smart greenhouse farm. Moreover, it additionally propose blockchain dependent security system which empowers the safe information communication in the smart greenhouse farming. This will give a novel highlights, for example, efficient and faster operations, scalability and improved reliability. It makes a typical stage through which all gadgets would have the option to convey safely in a disseminated network.

REFERENCES

[1] K. Paustian, J. Lehmann, S. Ogle, D. Reay, G. P. Robertson, and P. Smith, "Climate-smart soils," *Nature*. 2016.

[2] S. Kuppusamy, P. Thavamani, M. Megharaj, K. Venkateswarlu, and R. Naidu, "Agronomic and remedial benefits and risks of applying biochar to soil: Current knowledge and future research directions," *Environment International*. 2016.

[3] T. O. Wiedmann *et al.*, "Application of hybrid life cycle approaches to emerging energy technologies - The case of wind power in the UK," *Environ. Sci. Technol.*, 2011.

[4] I. Arto and E. Dietzenbacher, "Drivers of the growth in global greenhouse gas emissions," *Environ. Sci. Technol.*, 2014.

[5] Y. Cao and A. Pawłowski, "Life cycle assessment of two emerging sewage sludge-to-energy systems: Evaluating energy and greenhouse gas emissions implications," *Bioresour. Technol.*, 2013.

[6] T. Tong and M. Elimelech, "The Global Rise of Zero Liquid Discharge for Wastewater Management: Drivers, Technologies, and Future Directions," *Environmental Science and Technology*. 2016.

[7] A. S. Patil, B. A. Tama, Y. Park, and K. H. Rhee, "A framework for blockchain based secure smart green house farming," in *Lecture Notes in Electrical Engineering*, 2018.

[8] D. Gielen, F. Boshell, D. Saygin, M. D. Bazilian, N. Wagner, and R. Gorini, "The role of renewable energy in the global energy transformation," *Energy Strateg. Rev.*, 2019.

[9] M. Finkenrath, "Carbon Dioxide Capture from Power Generation - Status of Cost and Performance," *Chem. Eng. Technol.*, 2012.

[10] E. F. Einsiedel, A. D. Boyd, J. Medlock, and P. Ashworth, "Assessing socio-technical mindsets: Public deliberations on carbon capture and storage in the context of energy sources and climate change," *Energy Policy*, 2013.

[11] C. Chen *et al.*, "Challenges in biogas production from anaerobic membrane bioreactors," *Renew. Energy*, 2016.

[12] V. Prabu and N. Mallick, "Coalbed methane with CO2 sequestration: An emerging clean coal technology in India," *Renewable and Sustainable Energy Reviews*. 2015.

[13] Prachi Dewal, Gagandeep Singh Narula and Vishal Jain, "Detection and Prevention of Black Hole Attacks in Cluster based Wireless Sensor Networks", 10th INDIACom; INDIACom-2016, 3rd 2016 International Conference on "Computing for Sustainable Global Development", 16th – 18th March, 2016 having

ISBN No. 978-9-3805-4421-2, page no. 3399 to 3403.

[14] Prachi Dewal, Gagandeep Singh Narula, Anupam Baliyan and Vishal Jain, "Security Attacks in Wireless Sensor Networks: A Survey", CSI-2015; 50th Golden Jubilee Annual Convention on "Digital Life", held on 02nd to 05th December, 2015 at New Delhi, published by the Springer under ICT Based Innovations, Advances in Intelligent Systems and Computing having ISBN 978-981-10-6602-3.

[15] Ishleen Kaur, Gagandeep Singh Narula and Vishal Jain, "Identification and Analysis of Software Quality Estimators for Prediction of Fault Prone Modules", INDIACom-2017, 4th 2017 International Conference on "Computing for Sustainable Global Development".

[16] RS Venkatesh, PK Reejeesh, S Balamurugan, S Charanyaa, "Further More Investigations on Evolution of Approaches for Cloud Security", International Journal of Innovative Research in Computer and Communication Engineering , Vol. 3, Issue 1, January 2015

[17] K Deepika, N Naveen Prasad, S Balamurugan, S Charanyaa, "Survey on Security on Cloud Computing by Trusted Computer Strategy", International Journal of Innovative Research in Computer and Communication Engineering, 2015

[18] P Durga, S Jeevitha, A Poomalai, M Sowmiya, S Balamurugan, "Aspect Oriented Strategy to model the Examination Management Systems", International Journal of Innovative Research in Science, Engineering and Technology , Vol. 4, Issue 2, February 2015