Secure Smart Green House Farming using Blockchain Technology

P.Chinnasamy[a], R. Geetha[b], S. Geetha[c], S.P.Balakannan[d], K.Ramprathap[e], V.Praveena[f]

[a] Department of Information Technology, Sri Shakthi Institute of Engineering and Technology, chinnasamyponnusamy@gmail.com

[b]Assistant Professor, Information Science and Engineering, East Point College of Engineering and Technology, geetha2312@gmail.com

[c] Associate Professor, Information Science and Engineering, CMR Institute of Technology, geetha2016research@gmail.com

[d] Associate Professor, Department of Information Technology, Kalasalingam Academy of Research and Education, balakannansp@gmail.com

[e] Assistant Professor, Department of Management, M.Kumarasamy College of Engineering, msg2ramphd@gmail.com

[f]Assistant Professor, Department of Computer Science and Engineering, Dr.N.G.P Institute of Technology, drvpraveena@gmail.com

Abstract: The evolving agricultural technologies used mostly for remote access and modernization in farming connected via the Internet of Things (IoT) have been grown rapidly. However because of the wide size of all its broadcaster's propagandizing existence, it has some significant concerns with respect to security and privacy. We utilize blockchain to address such security breaches, allowing the development of a decentralized distributed blockchain system that's also exchanged between the IoT cluster heads. This article's major focus is provide smart greenhouse farmlands with a portable blockchain-based infrastructure which offers integrity and confidentiality. Where, green-house IoT sensor nodes are function as a blockchain centrally controlled to optimize the energy consumption by utilizing secure immutable ledgers. Furthermore, we present a significant solution that integrates blockchain technology via IoT devices to offer Smart Greenhouse cultivation with an enhanced secure communication.

Keywords: Internet of Things (IoT), Blockchain, Smart Contract, Smart Green House, Smart Farming.

1. Introduction

The rise of the Internet of Things (IoT) have resulted in significant IoT applications like smart homes, cities, digital industries, healthcare, retail and farming Hussian (2020). With both the growing population, conventional types of agriculture are unable to meet people needs. Smart agriculture based on IoT is becoming an inevitable method of farming techniques. Smart farming by means of the Greenhouse Management System (GMS)[Andreas (2019), Zhao (2020)] could provide monitoring and controlling of farm machinery. The GMS is fixed in order to increase production, efficiency and stop environmental hazards with scientific improvement strategies.Although there are many technological issues which need to be resolved in case of smart farming. For instance, due to the absence of mechanisms to exchange confidential agricultural data in some kind of a secured way, data sharing technology is insufficient [Hong (2020)].

In terms of greenhouse gas emissions and computational cost for IoT applications, existing security approaches may be costly. This current security system is handled by a centralized computer rather than by an IoT device [Ferrag (2020)]. Consequently, Smart Agriculture requires security and confidentiality that is compact, elastic and decentralized. We are implementing Blockchain technology to meet abovementioned IoT challenges (BC). Blockchain is a decentralized peer-to-peer digital asset that tracks transactions, contracts, partnerships, and revenues. Blockchain was originally invented to promote bitcoin, but without an intermediary [Xin (2020)], tomorrow's blockchain technology could be used in a type of transaction. BC is a repository that holds a continuously growing database of information of documents or transactions. It's also decentralized in design, such that there is a replication of a blockchain and transaction data attached to a chain by network participants. Both nodes in the network can verify it if a new transaction is added to the blockchain.Whenever a new transaction is entered into the system, it would be checked by all particles mostly in network. Throughout the chain, a collection of accepted transactions would be packaged, that would be sent to each cluster heads. They can in addition, evaluate the new blocks. A hashes bearing a distinctive feature of the preceding block [Xin (2020)] is used for each of the reports have documented. Therefore, BC seems to have the ability to address the current IoT difficulties, i.e. it is by default decentralized, stable and confidential. In this paper we proposed a BC-based Smart Greenhouse farming solution that supports lightweight and distributed security and confidentiality. Due to low available resources of an overwhelming majority of Sensor nodes, the key concern towards IoT security is enormous size, diversity across multiple networks and lack of integration. The privacy issues of a consumer are triggered by a vast volume of data accumulated and exchanged by IoT devices. A form of security mitigation that measures the risk of revealing information to others, but the expected value of IoT resources in certain circumstances increases the possibility of loss of privacy [Xin (2020)]. The implementation of BC technologies addresses problems including decentralization, confidentiality and protection in IoT through removing a single point of failure, increasing data accessibility and immutability.

2. Introduction

Hong (2020) offered both theoretical and practical explanations of food supply chains, insurance schemes, smart agriculture, and payments of various agricultural commodities. After this, they discuss transparent issues in food industry, efficient farming product sharing, and secure smart farming. The demerits of this system was less secure storage and less transaction cost.

Ferrag (2020) addressed some of the major protection and privacy issues that green IoT-based agriculture faces. They also divided the threat models into five dimensions: attacks on authentication, confidentiality, access control, product integrity, and user/product privacy. Finally, they addressed the open protection and privacy issues associated with green IoT-based agriculture.

Patil (2018) presented a novel blockchain based framework for green house farming. The security and privacy of the smart green house was enhanced by using distributed ledger concepts. The energy efficiency and communications of the proposed method was measured and analyzed against the existing methods.

Almeida (2018) gave a brief discussion about to solve enormous problems in backbone of our India (i.e. Agriculture). They summarize their research including all the research problems and open issues on the agriculture filed and supply chain management. In addition to that they discussed security and privacy issues on IoT based blockchain technology.

The effect of blockchain technology on the agriculture and food supply chain is examined by Iskan (2021), which introduces current development strategies and explores the opportunities and benefits of this system while keeping a skeptical approach on the sophistication of certain programs. According to the results, blockchain technique is an effective innovation in the food supply chain, although there are different challenges within producers and frameworks that preclude something from succeeding in smart cities [Vinothini (2021) and Praveena (2021)].

Elham (2020) discussed how the Internet of Things (IoT) and blockchain technology can be used in the poultry industry. To sustain and improve poultry performance, environmental variables such as temperature, moisture, soil, and sunlight are critical. For something like a massive poultry farm, particularly in the traditional manner, inspecting all environmental conditions is critical. IoT and Blockchain have recently was being used to automate the monitoring and management of the plant. It has been demonstrated that it can lower costs and keep the poultry farming excellently.

Farmers benefit from this method of intelligently inspecting the farmland because it provides an integrated watering system through adaptive sensing technology introduced by Havila (2020). Through an Android smartphone, a farmer may receive information about agriculture industry, such as precipitation, weather, and sand moisture levels. These realistic implementations of sensor control module help to accomplish the aim of a precision agriculture management system. They have used the Raspberry PI controller to monitor the entire systems, but they can’t measure the security level of the systems.

Torky (202) introduced a novel techniques to discuss the significant issues in IoT-based predictive farming production. Furthermore, the researchers analysed and information for classification the essential components and weaknesses of different blockchain technology used throughout undertaking different game thread of smart farming, including certain vegetables, agricultural land, as well as the agricultural industry. Eventually, the paper addressed a few of the privacy risks, as well as blockchain-related problems that are impeding that development of blockchain-based personalized agricultural production.

3. System Model

There are 4 sections in our device model: Smart Greenhouse, Edge Network, Data Storage, Customer (Fig. 1).

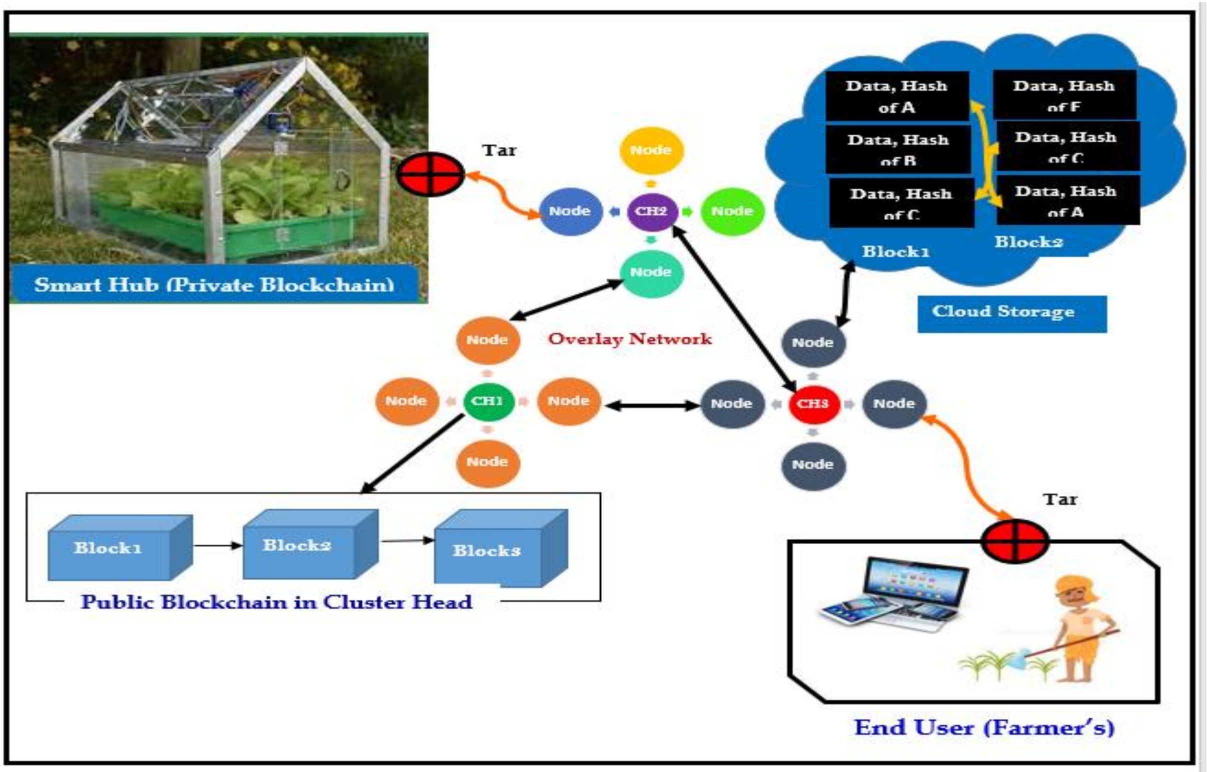

Figure 1. The Architecture of Proposed Method

3.1 Smart Greenhouse (SGH)

It is an agricultural field protected by haze to defend seeds against global threats and fitted with numerous IoT sensors. In addition, it also involves the decentralized blockchain system (i.e. Smart Hub) recognized as a truly secure blockchain, mined and maintained through one or even more devices are capable of resources. The creator centrally controls this local blockchain. By launching the transaction or removing its ledgers, the owner may insert or uninstall the devices. By giving consent, all machines in SGH can interact with others through offering them a symmetrical master secret dependent on the encryption system of chaos [Praveena (2019), Deepalakshmi (2018), Chinnasamy (2021), Padmavathi (2021)]. The Central BC seems to have a frame format presented with a list of all security protocols on which SGH activities can be handled by the owner. Each layer consists a policy header as in blockchain, often a modified policy put in last preceding block that is being used to verify and modify the policies as well as eliminate the PoW overheads [Xiong (2020)]. Each block's miners appends a reference to the preceding block and transfers to a new transaction the policy in the subsequent block header. The result of successful mining is known as legitimate transaction.

3.2 Edge Network

Here the edge network is analogous to the bitcoin system, whereby high-resource machines configured with in farmland could be another crucial nodes. In the edge network, each nodes may create a group named themselves as a community to decrease its communication load and latency, whereas the community can nominate its representative recognized as Cluster Head (CH). Each node, while they experience unreasonable disruptions, also replaced traditional their representative. The system CH manages the overlay blockchain that holds the all multisig tokens sent from the customer for cloud storing and accessing. In addition, depending on obtaining transactions, CH regulates to either hold new blocks or should it reject them. Any time for a fresh block transaction to be invented generates additional latency or users choose to handle upwards of one system at a time. It can be done common miners. Each system seems to have a beginning transaction with in edge blockchain that's also connected towards its cultivation beginning transaction which really progresses to mutual overlap shelling. In Cultivation, overlay systems may preserve a tables where all records from the last transaction resides.

3.3 Data Storage

In sensitive greenhouse crop yield, customers need to have some professional assistance from an expert. Greenhouse systems store its data in the cloud, such that a specialist could access greenhouse information directly through data storage and offer the service based on the case. The information stored in the cloud contains similar blocks of separate block numbers for users. Block numbers and hash details should be used for verification. When data is uploaded to the cloud [Praveena (2019), Deepalakshmi (2018), Chinnasamy (2021), Padmavathi (2021)] the mutual keys generated from chaos-based encryption algorithms is secured by key amount. Although hashing remain accident, it means that true customers can view details and connect new data to an established blockchain as well.

3.4 End Users

Users can freely access and monitor embedded sensors smart phones, computers, etc.

4. Threat Model

Smart greenhouse cultivation may be susceptible to a variety of security threats owing to the interdependent existence of resource limited IoT devices. In order to develop and implement an effective solution, it is important to recognize different challenges and risks prevention methods. The aforementioned security categories are identified in smart greenhouses:

(1) **Availability threats:** This vulnerability involves unauthorized resource endorsements. Thus, the attacker's primary goal is to prohibit the legitimate users from gaining access your resources and applications.

(2) **Risks to integrity:** unauthorized users may alter the actual data in a way that incorrect information may be added or data may be manipulated.

(3) **Risks to confidentiality:** confidential information may be leaked by unauthorized users.

(4) **Authentication threat:** access to services and sensitive material is obtained by unauthorized parties

5. Security of the Proposed Method

The protection structure that comprises the following fabrics is shown in Figure 2.

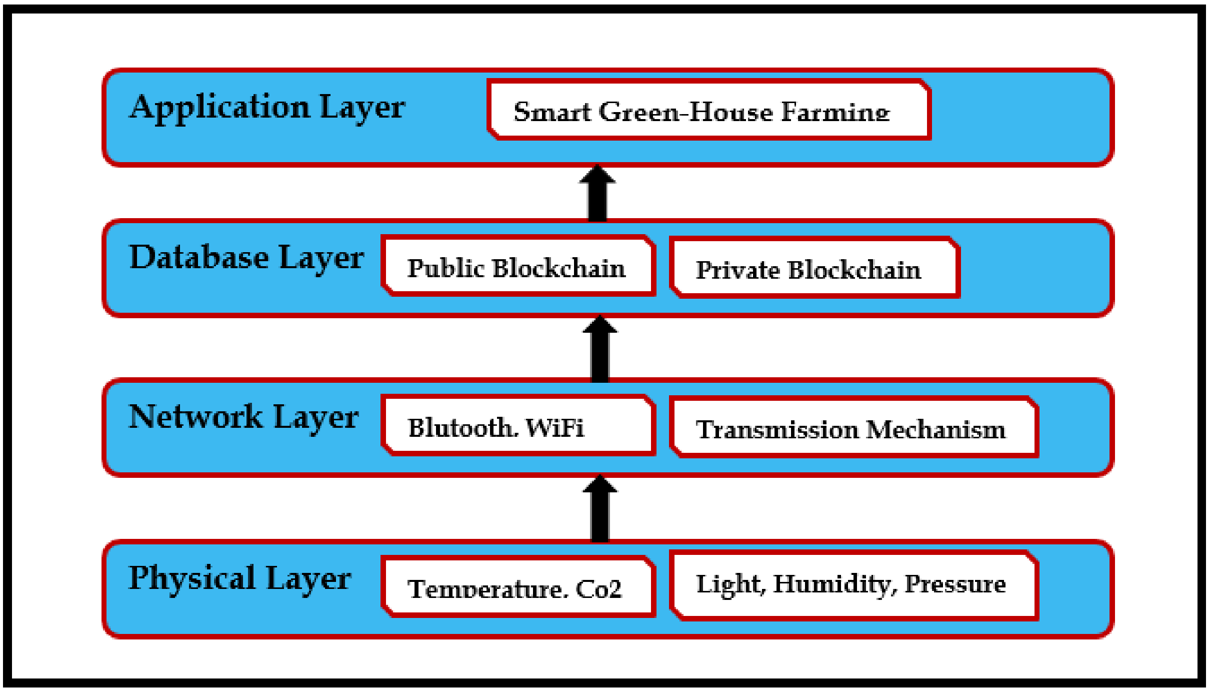

Figure 2. Security Structure of Proposed Method

5.1 Physical Layer

Within this component, several authorization and access control risks are conceivable such that the adversaries may penetrate the SGH configured machines. In this, as local BC is mined in SGH, all transactions are flexible for users. Therefore, adversaries are unable to introduce additional machines to SGH like all machines are pre-defined by consumer, and specific BC mines the exchange of goods. It is, therefore, difficult for an intruder to penetrate the physical layer. This miner authorizes a transaction obtained from the edge network before transmitting it to the computers. However, Miner thus fulfils, verification and validation of all the transactions and generates genesis transactions, updates and distributes keys.

5.2 Communication Layer

To provide protection against all the data transmitted and to minimize downtime latency, this element implements a decentralized overlay BC framework. Where, the declining attack as well as the mining attacks are potentially threatened. An adversary should include power over the CH to accomplish the declining assault. Both acquired blocks and transactions will be dropped by the regulated CH. Both entities in groups have the opportunity to elect the representative throughout the suggested architecture. In these cases, all participants in same group choose the newest CH. The intruder ought to have authority over numerous CHs which signed the multisig contract in terms of achieving the mining intrusion such that they might steal false blocks. In this proposed architecture all the transactions are authorized and validated by CH. If CH does not recognize a false block in certain case, this could warn almost all CHs.

5.3 Database Layer

Distributed ledger technology in Blockchain are really a kind of decentralized repository that stores records one after the other. The cryptographically secure signatures and a timeframe are included in each records in the transactions. Personal BC controls the transaction and includes the smart contract wherein the inbound and outbound network transaction is handled depending on policies. As something of an immutable ledger throughout the blockchain, each transaction is linked around each other. Similarly, each block contains the data block who carries the preceding block's hashes to maintain the blockchain persistent as well as the policy header that is being used to authorize machines and enforce the valid user-generated policy.

5.4 Interface Layer

With different IDs, the intruder can attempt to create different transactions. Enabling customers to upload conditional transactions to an edge network throughout the proposed system. Both IDs and PKs at each transaction, whereas, are subject to change by this property we can enhance the confidentiality.

5. Conclusion

This article describes the implementation of a smart-green house agricultural system that relies on BC to resolve the issues of IoT protection and privacy. Current protection technologies really aren't appropriate due to increased energy utilization and overhead storage. We discuss the BC, that solves this issues by keeping the Bitcoin BC includes permanent block ledgers to meet this issues. In order to accomplish a secure controlling, we have developed a Smart Greenhouse Farm system. In addition, we often proposed a blockchain-based protection system that allows smart greenhouse cultivation to secure communication protocol. It also has unique characteristics like enhanced reliability, better and more accurate and flexible activities. It provides a shared framework from which all devices in such a decentralized system that can perform communication in a secure manner.

References

1. Sabir Hussain Awan, Sheeraz Ahmed, Asif Nawaz, Sozan Sulaiman Maghdid, Khalid Zaman, M.Yousaf Ali Khan, Zeeshan Najam and Sohail Imran (2020), “BlockChain with IoT, an Emergent Routing Scheme for Smart Agriculture” International Journal of Advanced Computer Science and Applications(IJACSA), 11(4), 2020. http://dx.doi.org/10.14569/IJACSA.2020.0110457.
2. Andreas Kamilaris, Agusti Fonts, Francesc X. Prenafeta-Bold (2019), The rise of blockchain technology in agriculture and food supply chains, Trends in Food Science & Technology, Volume 91, 2019,pp 640-652.
3. Hong Zhao, Dongyi Kong (2020), The Design and Realization of Intelligent Greenhouse Control System Based on Cloud Integration, Journal of Physics: Conference Series, Vol. 1646, 2020.
4. Xin C, Zhang T, Tsai S-B, Zhai Y-M, Wang J (2020), An Empirical Study on Greenhouse Gas Emission Calculations Under Different Municipal Solid Waste Management Strategies. *Applied Sciences*. 2020; 10(5):1673.
5. Xiong Hang, Dalhaus Tobias, Wang Puqing, Huang Jiajin (2020),Blockchain Technology for Agriculture: Applications and Rationale, Frontiers in Blockchain, Vol. 3, 2020, pp. 1-7, doi:10.3389/fbloc.2020.00007

6. M. A. Ferrag, L. Shu, X. Yang, A. Derhab and L. Maglaras (2020), "Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges," in *IEEE Access*, vol. 8, pp. 32031-32053, 2020, doi: 10.1109/ACCESS.2020.2973178.
7. Patil A.S., Tama B.A., Park Y., Rhee KH. (2018) A Framework for Blockchain Based Secure Smart Green House Farming. In: Park J., Loia V., Yi G., Sung Y. (eds) Advances in Computer Science and Ubiquitous Computing. CUTE 2017, CSA 2017. Lecture Notes in Electrical Engineering, vol 474. Springer, Singapore. https://doi.org/10.1007/978-981-10-7605-3_185
8. Bermeo-Almeida O., Cardenas-Rodriguez M., Samaniego-Cobo T., Ferruzola-Gómez E., Cabezas-Cabezas R., Bazán-Vera W. (2018) Blockchain in Agriculture: A Systematic Literature Review. In: Valencia-García R., Alcaraz-Mármol G., Del Cioppo-Morstadt J., Vera-Lucio N., Bucaram-Leverone M. (eds) Technologies and Innovation. CITI 2018. Communications in Computer and Information Science, vol 883. Springer, Cham. https://doi.org/10.1007/978-3-030-00940-3_4
9. Toptancı, Ali İskan (2021), Adoption of Blockchain Technology in the Agricultural Sector and Food Supply Chain, ZBW - Leibniz Information Centre for Economics, Kiel, Hamburg
10. M. N. Elham *et al*. (2020), "A Preliminary Study on Poultry Farm Environmental Monitoring using Internet of Things and Blockchain Technology," *2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, Malaysia, 2020, pp. 273-276, doi: 10.1109/ISCAIE47305.2020.9108820.
11. A.Jemima Havila Catherine, Dr.P.Ezhilarasi (2020), Smart Farming using Blockchain Technology, International Research Journal of Engineering and Technology (IRJET), Vol.7, No.10, pp.302-305, 2020.
12. Mohamed Torky, Aboul Ella Hassanein (2020), Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges, Computers and Electronics in Agriculture, Vol. 178, 2020, 105476, https://doi.org/10.1016/j.compag.2020.105476.
13. P.Chinnasamy, P.Deepalakshmi, V. Praveena, K.Rajakumari, P.Hamsagayathri, (2019) “Blockchain Technology: A Step Towards Sustainable Development” International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-9 Issue-2S2.
14. Xiong H, Dalhaus T, Wang P and Huang J (2020) Blockchain Technology for Agriculture:Applications and Rationale. Front. Blockchain 3:7. doi: 10.3389/fbloc.2020.00007.
15. P. Chinnasamy and P. Deepalakshmi (2018), "Design of Secure Storage for Health-care Cloud using Hybrid Cryptography," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 2018, pp. 1717-1720, doi: 10.1109/ICICCT.2018.8473107.
16. Chinnasamy, P., Deepalakshmi, P (2021). HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud. J Ambient Intell Human Comput (2021). https://doi.org/10.1007/s12652-021-02942-2
17. Chinnasamy P., Padmavathi S., Swathy R., Rakesh S. (2021) Efficient Data Security Using Hybrid Cryptography on Cloud Computing. In: Ranganathan G., Chen J., Rocha Á. (eds) Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems, vol 145. Springer, Singapore. https://doi.org/10.1007/978-981-15-7345-3_46.
18. Chinnasamy P., Vinothini C., Arun Kumar S., Allwyn Sundarraj A., Annlin Jeba S.V., Praveena V. (2021) Blockchain Technology in Smart-Cities. In: Panda S.K., Jena A.K., Swain S.K., Satapathy S.C. (eds) Blockchain Technology: Applications and Challenges. Intelligent Systems Reference Library, vol 203. Springer, Cham. https://doi.org/10.1007/978-3-030-69395-4_11.
19. C Vinothini and B Ben Sujitha Chinnasamy P, B Vinodhini, V Praveena, Blockchain based Access Control and Data Sharing Systems for Smart Devices, Journal of Physics:Conference Series, Vol.1767, No.1, pp-1-8, 2021.