An approach using Trust Management with Next-Generation IoT Networks for Healthcare, Agriculture and Sustainable Development Goals

D.O.I - 10.51201/Jusst12653

http://doi.org/10.51201/Jusst12653

Shubham Joshi
Research Scholar, Mewar University, Chittorgarh

Dr. Meghna Dubey
Professor, Mewar University, Chittorgarh

Dr. Durgesh Kumar Mishra
Professor, Sri Aurobindo Institute of Technology, Indore

Abstract: *The Internet of Things (IoT) is one of the most promising scientific fields of the last decade. The number of devices developed that support Internet things makes the application of internet things more interesting. The field of use includes the insurance sector, intelligent monitoring Environment, Smart City, sector-health care, Intelligent City, and also many other applications enabled for smart devices.The vision of the introduction of the internet, forming a network called IoT, where various information technology devices are connected, security and trust are most important for the user, because this network presumably used a large amount of data.However, trust is a significant obstacle that can hinder the growth of the IoT and even slow down the significant compression of many applications.This paper presents an approach using trust management (TM) with next-generation IoT networks for healthcare, agriculture, and sustainable development goals. Implementation of IoT conveys various problems of security and confidentiality. The use of IoT to ensure confidentiality, integrity, authentication, authorization, trust, secrecy, and management challenges are addressed. The paper uses decentralized blockchain technology to solve security and privacy issues in applications with the support of the IoT.Ethereum virtual machine is used to implement theBlockchain distributed networkand healthcare insurance claims are taken as anexample to test the proposed solution. Also, it is provided that the lessons and opinions discussed are primarily about the purpose of the trust, which can be reproduced in the future on the internet.The results show that distributed blockchain technology provides trust management and can improve the existing security and privacy of the IoT in the health and agriculture sectors, which is helpful for next-generation IoT networks.*

Keywords: Internet of Things, Trust Management, IoT networks for healthcare and agriculture, Blockchain, Ethereum.

1. INTRODUCTION

Internet of Things (IoT) is a new model that was developed to connect millions of intelligent communications nodes to the Internet [1]. Some nodes are sensors and actuators that can process data from receiving and other equipment without human intervention [2].The development of the internet has things exerting significant influence in several areas including smart city [3], smart healthcare[4], intelligent transport[5], air-link [6], data mining [7], manufacturing [8], and environmental monitoring [9-13].This is the highest level of heterogeneity associated with the systems of Internet things, estimated to increase the existing security threats to the Internet, which are used to allow people to interact with machines[14].Conventional privacy solutions and security settings do not meet the requirements of users due to their limited computing power.

In IoT different independent devices interact with each other to perform different tasks. These devices are so dense environment sustainably discovers other devices.Such discoveries are called semantic discoveries, which

create various problems related to information trust[15]. Various ways to achieve semantic interoperability include using a broker-based architecture.The broker architecture is complex and weak to handle discovery between objects. [16] Trust management in IoT environments is provided by various methods[17], [18] that user experience, sensor data irregularity, reliability, and availability as trust matrices.Its network environment is characterized by a special new challenge from the point of view of the IoT. The most important thing, in addition to its features, apart from confidentiality and security is trust.That is, if the aggregated information from different devices is malicious and not reliable enough, then the trust of the application layer and the network layer is fully ensured.The most important question that arises knows how the generated IoT data is converted into useful information to ensure a secure and reliable connection.

Sector healthcare is one of the most important sectors where the patient's condition is controlled using various smart things placed in the patient's body.Collecting data on patient health based on the architecture of the IoT network is already described in work[19]. The sector is gradually expanding globally. The traditional department of insurance is a centralized system in which all these operations are not known to each other.In the system of health insurance, patients are already registered with each insurance company, and this corresponds to all insurance companies.Some problems arise when a patient receives treatment at a hospital and requires an insurance policy, such as the type of treatment, financial claims, settlement, and trust.In recent years, the development of IoT devices has allowed us to collect, process, store, and analyze patient information in real-time. The benefits of using the IoT to provide medical care are faster treatment, lower costs, and easier diagnosis.

The next generation of smart agriculture based on IoT is expected to support advances in agricultural practices and technologies to support sustainable farmers and resources. It is economically viable, is reliable, socially stable, and works well. This approach is aimed at maintaining the quality of soils, reducing erosion and degradation of soils, as well as maintaining water resources.Also, especially in smart agriculture, if any of the sensors become malicious, it will affect decisions that directly hinder production [20]. Some existing approaches use a trust to solve the problem of identifying malicious nodes, but the field of intelligent agriculture is completely ignored.This paper presents an approach using trust management (TM) with next-generation IoT networks for healthcare, agriculture, and sustainable development goals.In which the integration of blockchain technology with IoT will be improved to address some security concerns.Blockchain is a technology derived from the Bitcoin cryptocurrency proposed by Satoshi ten years ago [21]. In this white paper, Satoshi explains for the first time the concept of peer-to-peer trading without involving a third party.All transactions are also stored digitally and are stored in all nodes of this network. Users of the application of the IoT need to build a relationship of trust between them.This paper explains the characteristics of reliability, the importance of trust management, and the goals of the IoT system.

2. LITERATURE SURVEY

Network implementation of the IoT is necessary to solve all the problems of security, as well as the problems of trust, reliability, stack, quality of service (QoS), and access control.Many modern studies show numerous gaps in research that need to be resolved because trust is one of the areas where a large number of studies are required to ensure adequate security.However, this is neglected, and such a mechanism for identifying malicious nodes based on trust parameters is not proposed. A significant amount of research has been conducted in various areas of health and intelligent agriculture, as explained in this section.

Since the time of technological advances on the Internet things in the health department have become smart from the perspective of tracking patients in real-time or fast information processing. Today, health insurance is an important area related to medical care. Each insurance case goes through different stages and requires a lot of documentation, but also time.The traditional and health insurance system has a lot of uncertainty, and there is no trust in patients, insurance companies, and hospitals. New technology IoT allows applications smart according to relevant technologies.The same technology, distributed digitally in an accounting blockchain technology, can protect the system from unauthorized access. Recently, several research articles were devoted to the use of health insurance in the IoT sector.The insurance industry has moved from a traditional approach to a new approach that uses technologies such as IoT, big data, and artificial intelligence[22].Detection technology use,

fraud machine learning programs health insurance was offered in the works[23].The IoT has already been used to monitor systems and public health patients in real-time. In the age of the internet, where everything is stored digitally, the leak of personal data and privacy of patients is down to real danger.Information sharing and data calculation must be carried out securely. The problem of implementation in the health sector is divided into the way, where everything is safely separated and calculated, is described[24].

In [25], a study on the digitization of smart cities and agriculture was published. The study found that it is important to use Arrowhead technology to improve network performance and help solve problems related to transmission speed, latency, etc.When it comes to intelligent agriculture, Arrowhead, which consists of components of a connector for data and a mechanism for data conversion connected to blocks of storage and auxiliary system, visualizes data solutions utilizing aggregation of the collected data and reporting part.Efficient use of energy resources is provided by an intelligent irrigation system[26]. The system uses the CC1310 SOC to design nodes with long-distance capability and low energy usage. Also, the proposed mechanism combines irrigation, to s 6LoWPAN and fuzzyfor irrigation forecasting.In [27], protecting and improving the safety of the proposed encryption algorithm, IoT irrigation system. In this study, he said, it is important to ensure the safety of less intensive, devices where encryption is one of the most noticeable solutions to maintain integrity and confidentiality in nodes.The work [28] offered solar system security intellectual irrigation system IoT. Security is ensured using arm LAC2148 built-in laser and solar panels with a GSM module.The main contribution to the study is the use of arm-controllers that ensure sufficient accuracy with minimal accuracy. The same mechanism for safe watering smart agriculture was offered for work [29].There is a method offered for using the small fences underwater consumption Android platform. This approach uses sensors to collect data (e.g. level of soil moisture, temperature, and more).

The decision was made using a nebulous theory of privacy and reliability.Also, existing studies on security at IoT require considerable attention to address several safety concerns, such as confidentiality, reliability, and data integrity, as stated [30-34].Also, IoT was offered several mechanisms of trust, indicating that it has a significant impact on logged malicious nodes [35-36]. IoT it is important to identify nodes that can affect the intelligent irrigation system.The paper [37] discussed the introduction of IoT in intelligent agriculture and the role of trust in minimizing risks. The study details the importance of trust and suggests that trust is key to the technology adoption model, and may also play an important role in building positive relationships between nodes.However, trust management in IoT has been neglected for decades, and IoT network requires robust mechanisms to maintain a secure environment between sensors.

3. BLOCKCHAIN AND IOT INTEGRATION

Since its development, IoT has given interesting applications such as smart cities, smart houses, and smart health systems. Automation and digitization systems improve people's quality of life. However, data transmission per share calculation centralized management system is not reliable. The application needsto address security, confidentiality, reliability, and scalability issues.In this way, block chain introduces decentralized features such as scalability, autonomy, reliability, security, immutability, trust, and integrates block chain-conceptual fields that can benefit from the IoT to solve problems with IoT applications.

3.1 A variety of Attacks Solution using the Block chain

3.1.1 IoT Device Authentication and Authorization

Traditionally, authentication is done using a central server. The Blockchain-based smart contract provides the ability to authenticate IoT devices as distributed and peaceful multi-party authentication. Bubble trust-this is the technology offered to decentralized authentication devices IoT[38]. Smart-contracts are based on a complex comparison between traditional authorization and IoT devices.A smart contract is also used to update software or hardware, even to authorize devices to verify certain policies.

3.1.2 Confidentiality and Non-Repudiation

It is clear that each transaction is encrypted and the verification process before adding its block format. Each node uses its hash address authentication using the node's digital signature, based on ECC, a node that gives different permissions to smart contracts. Thus, the privacy of users is preserved in the blockchain system. Non-Repudiation is not possible in a blockchain system. Because each node sends a message and its digital signature to another node.Thus, the owner's details of the transaction are verified decrypted using the message sender's public key. In the latter part, no one can deny that the deal was not done for them. In the registration process, each node receives a unique identification number, which is written in the blockchain, so forge a node also can't.The term uses authentication to process cryptography with a public key. Proper authentication can prevent rejection and interference.

3.1.3 Data leakage and Trust Management

All data is cryptographically protected and signed by the sender with a digital signature. All topics in-network data formatsare stored in a digital ledger format.Thus, there is no possibility of a data leak or data transit attack in a blockchain-based system. All nodes have a copy of the same transaction, so they can verify any other transaction. The identity of the nodes can be identified using a unique key and their digital signature, which increases the trust of all users.

3.2 IoT Applications Blockchain Solution Approach

As shown in Fig. 1. An intelligent application based on the IoT is a blockchain design concept. The blockchain architecture can be either an authorized or an unauthorized model.The device IoT is connected to another intermediate system and may have peer fog. These intermediate nodes are connected broken down to serve communication and computing purposes.A single node is defined by multiphase calculations in the decision-making process to improve performance and reliability. As for the application requirements, it is necessary to develop a smart contract that will be deployed on the blockchain platform.Currently, two widely used blockchain platforms available, Ethereum and Hyperlegder fabric. A smart contract's output to the corresponding output in a program that is required as a self-executing program.Like the development of many applications, smart home monitoring systems can send alarm notifications in the event of a fire to a responsible user. Similarly, in smart healthcare systems, the information collected can be used to respond quickly through foggy computing and blockchain-based smart contracts.In some smart applications, actions can be done immediately if the event is known. Finally, because blockchain systems are secure, tamper-proof, distributed, and immutable makes the IoT systems will be more secure and reliable.

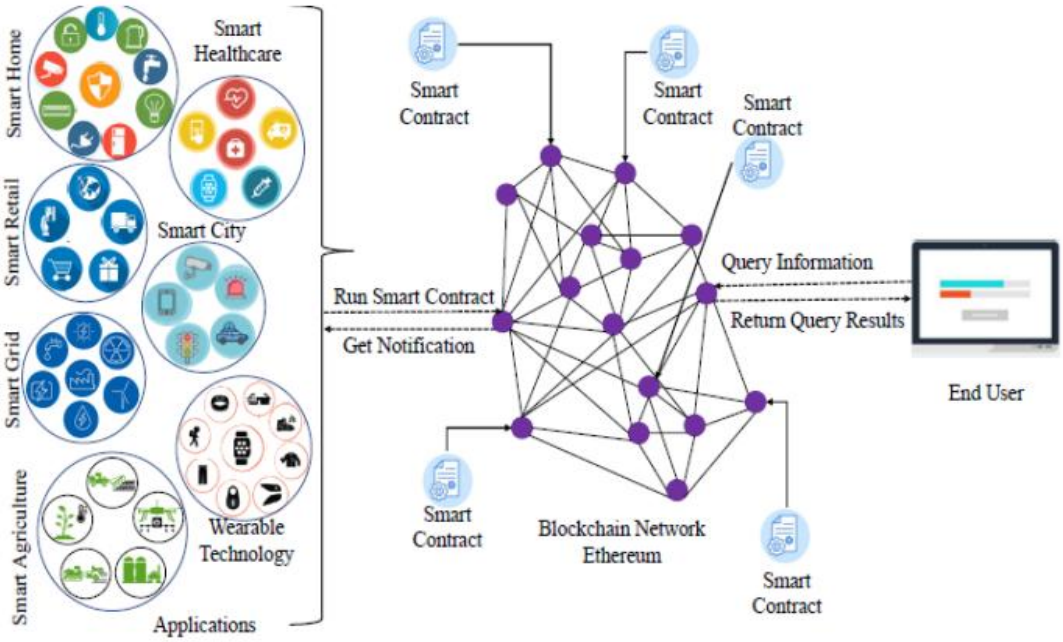

Figure 1: IoT applications integrated based on blockchain architecture [40].

4. PROPOSED FRAMEWORK FOR HEALTHCARE

The insurance sector is one of the most demanding sectors today. There are many different types of insurance coverage, as insurance can be medical, transportation, home, and any electronics. Patients can register through the hospital or start health insurance directly through the online system. The insurance company will review the insurance claim and approve it accordingly.Finally, the hospital, after the patient's treatment was over, claimed the final money directly to the insurance company. If the hospital receives the approval of the insurance company, the patient will be discharged.Problems with traditional systems are:

- The patient never really knows how much the insurance company paid, as well as the date and time of release.
- Communication occurs between two or more parties mainly related to the two parties.
- There is no transparent way of communicating information.
- There is no trust between users.

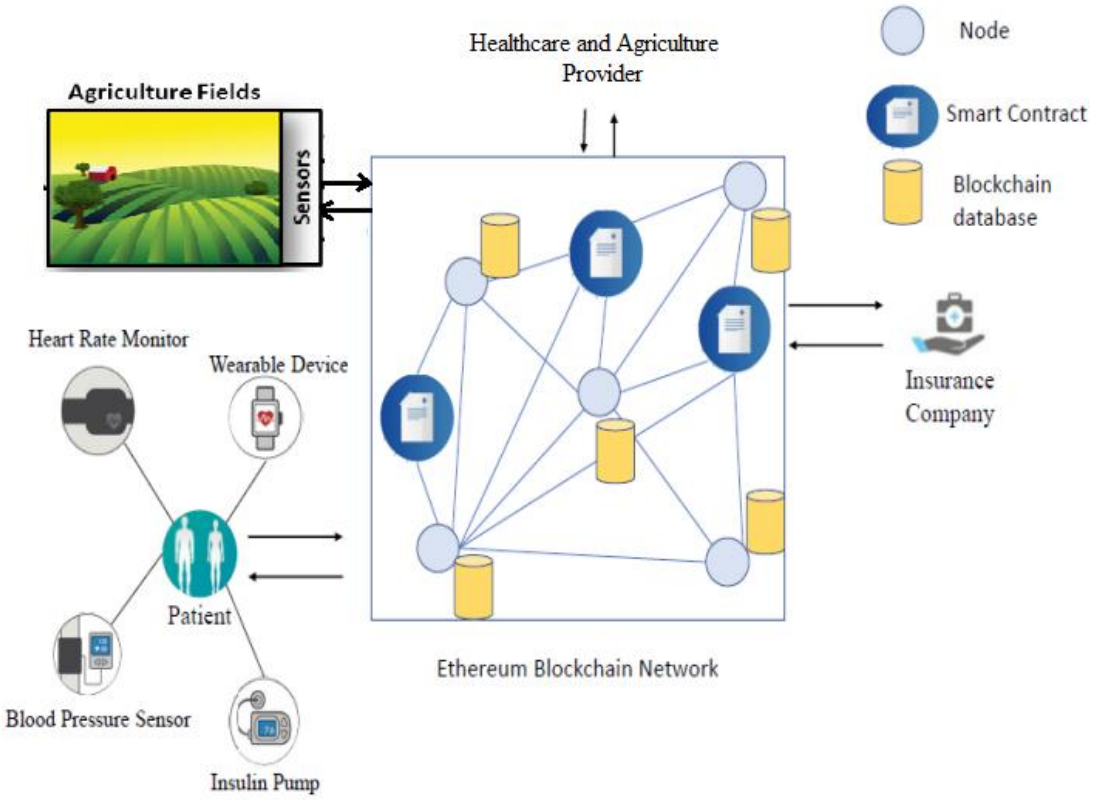

Figure 2: The proposed framework for health and agricultural insurance claims on a distributed Blockchain network.

5. IMPLEMENTATION DETAILS AND RESULT DISCUSSION

Ethereum is a decentralized, open-source, public, and hassle-free block chain platform that offers a computer application to run on top of it. This allows developers to program their smart contracts using the solidity language without having to create their blockchain. Applications running on the block chain can interact with each other in the block chain network, and a complete network of connected applications, called decentralized applications (dApps), will be developed.Since the Ethereum platform has a shorter blocking time than bitcoin, it is more convenient to run the application. The blocking and recording of crypto transactions are done by Ethereum and are very fast, resulting in faster transactions.Ethereum handles a large number of transactions that occur on the Internet without the user waiting for a long time.

5.1 Experimental Setup

When creating a block chain virtual network for deploying Ethereum, a system with an Intel Core i5-5200U 2.2 GHz processor and 8 GB of Linux RAM is used as an operating system. We are creating an Ethereum platform of ten users with a unique hash ID created for a network connection. With a unique identifier, nodes can transmit a message from one to another using the signature concept.Digital signature means adding digital code to an electronic message so that others can control it. The advantages of using digital signature include content verification, user identity verification, which prevents the user from being rejected.The uniqueness of a digital signature is that each document has a unique code. In a block chain system, each node's digital signature can be forwarded to a message using its signature and other nodes to verify it.

5.2 IoT application Smart Contract

Smart contracts make small computer programs of the block chain. This is similar to a physical contract, but it doesn't require you to trust a third party to work.This allows you to automatically perform a specific task when certain predefined conditions are triggered.Since the smart contract is stored inside the blockchain, it works

completely decentralized.With this method, no one on the network can gain control of the property. Since they are stored in the blockchain, they inherit some interesting features:

- It is immutable, meaning a smart contract can never be changed once it is entered into the blockchain. So that no one can forge the code of the smart contract behind your back.
- It is distributed, that is, each online confirms the conclusion of the smart contract. Thus, an attacker cannot force a contract in a certain way, because this attempt will be noticed by other nodes of the blockchain network and they will mark this attempt as invalid.
- It can work as multiple endorsement accounts, so a smart contract is only executed if the required number of nodes is supported.
- It can store useful information about the application, such as registration and domain name information.

The use of smart contracts in various applications and tasks of the IoT is described in [39]. As shown in figure 2. A smart contract can be written and implemented in the Ethereumblockchain network.

5.3 Smart Contract-based Health Insurance System for Experimental Purposes

In this paper, after the blockchain, a system will be created based on the Ethereum platform, and for verification and verification; the health insurance system will be treated as an IoT application.As shown in Figure 2. The healthcare system has three divisions: the patient, the insurance company, and the healthcare system. The smart contract of all these entities is written with power and deployed in the blockchain network.In this example, the patient's first smart contract is executed automatically each time the patient's input criteria are met and the message is forwarded to the network. Both the hospital and the insurance company show the message. All events that occur are then recorded digitally and are available to all three divisions of the blockchain network.Security and privacy concerns with this system relate to address space, authentication, and authorization, secure communications, trust management, data authentication, integrity, and secure computing for IoT devices.

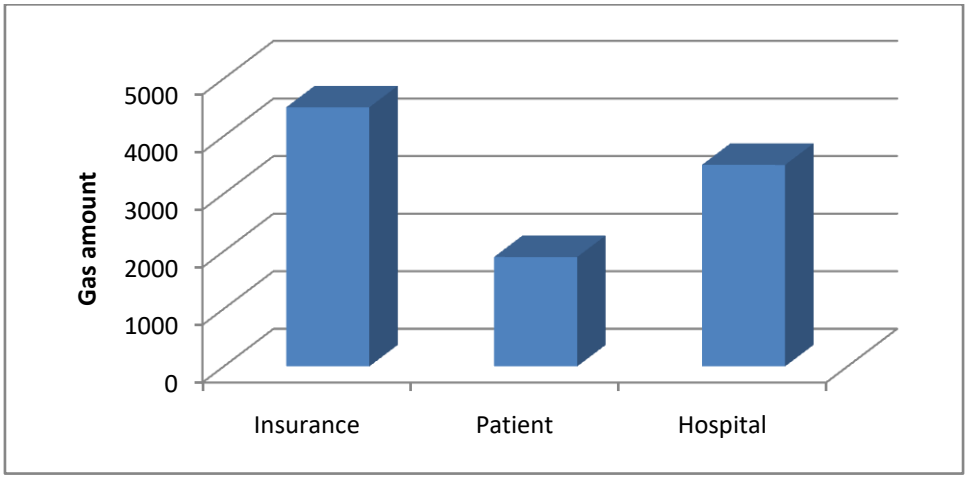

Figure 3: Gas consumption by various smart contracts of the Ethereum network in a deployed state.

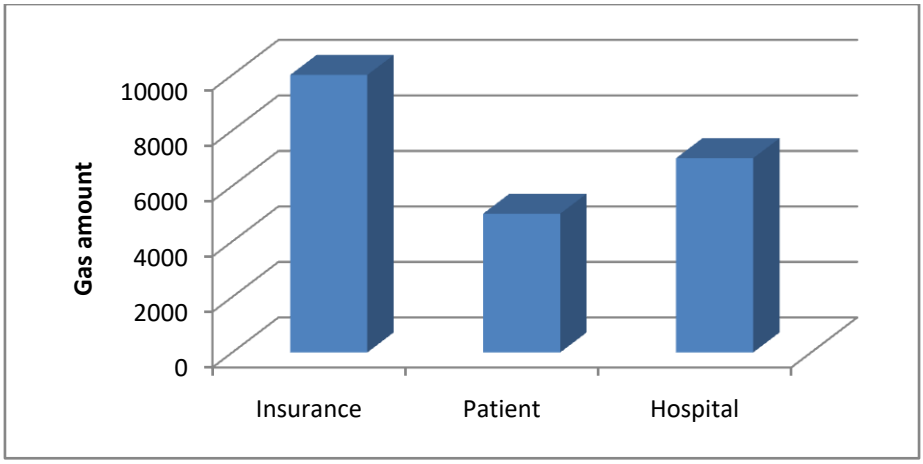

Figure 4: Gas consumption by various smart contracts of the Ethereum network in the executionstate.

The use of the gas of the Ethereum virtual machine in the execution of various smart contracts, as shown in Fig. 3 and Fig. 4. If you run a block chain network deployed in a smart contract, the event will be triggered automatically.All transactions in the proposed distributed network are recorded only in digital format. In this work, it will be used to be implemented as a private block chain.First, all nodes are authenticated in the system. Input data is collected from various sensor devices and transmitted to the block chain for processing. Every organization is capable of smart contracts.It functions as the execution of smart contracts, as well as events corresponding to triggers. When sending a message, the digital signature is used together with the message to avoid rejection.

6. CONCLUSION

IoT is one of the most promising areas of research in the last decade. This is the concept of developing a smart home, intelligent environmental monitoring, intelligent traffic management, including the development of many applications using Trust Management with IoT.All of these apps are great for use without human interaction. The application can operate in real-time using various sensors, actuators, and intelligent devices.Health insurance is one of the most promising areas in the world. In the traditional insurance system, there are problems such as trust management, the clarity of the requirements, delays in the processing, and settlement issues.In this article, we propose a structure based on block chain technology, in which all participating entities are connected in a distributed manner. The Ethereum virtual machine was used as a block chain platform for implementation purposes.Since this is a private block chain, all units are registered initially. The smart contract designs different functionality for each block. The results showed that the smart contract is triggered when a smaller amount of gas during the performance.Here, the entire insurance payment process is recorded in a digital ledger format using a digital signature that builds trust between related users.In the future, implements a public blockchain environment so that more users can handle network and multi-party computing.

REFERENCES

1. *N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han, ''Data collection and wireless communication in Internet of Things (IoT) using economic analysis and pricing models: A survey,'' IEEE Commun. Surveys Tuts., vol. 18, no. 4, pp. 2546–2590, 4th Quart., 2016.*
2. *R. Minerva, A. Biru, and D. Rotondi, ''Towards a definition of the Internet of Things (IoT),'' Tech. Rep., 2015. [Online]. Available: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_ Internet_of_Things_Revision1_27MAY15.pdf*
3. *A. Gharaibeh et al., ''Smart cities: A survey on data management, security, and enabling technologies,'' IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2456–2501, 4th Quart., 2017.*
4. *G. Acampora, D. J. Cook, P. Rashidi, and A. V. Vasilakos, ''A survey on ambient intelligence in healthcare,'' Proc. IEEE, vol. 101, no. 12, pp. 2470–2494, Dec. 2013*

5. *S. Pellicer, G. Santa, A. L. Bleda, R. Maestre, A. J. Jara, and A. G. Skarmeta, ''A global perspective of smart cities: A survey,'' in Proc. 7th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS), 2013, pp. 439–444.*
6. *M. Elsaadany, A. Ali, and W. Hamouda, ''Cellular LTE-A technologies for the future Internet-of-Things: Physical layer features and challenges,'' IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2544–2572, 4th Quart., 2017.*
7. *C.-W. Tsai et al., ''Data mining for Internet of Things: A survey,'' IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 77–97, 1st Quart., 2014.*
8. *D. Georgakopoulos, P. P. Jayaraman, M. Fazia, M. Villari, and R. Ranjan, ''Internet of Things and edge cloud computing roadmap for manufacturing,'' IEEE Cloud Comput., vol. 3, no. 4, pp. 66–73, Jul./Aug. 2016.*
9. *N. Zhao, F. R. Yu, H. Sun, A. Nallanathan, and H. Yin, ''A novel interference alignment scheme based on sequential antenna switching in wireless networks,'' IEEE Trans. Wireless Commun., vol. 12, no. 10, pp. 5008–5021, Oct. 2013.*
10. *J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, ''Internet of Things (IoT): A vision, architectural elements, and future directions,'' Future Generat. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013*
11. *C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, ''Context aware computing for the Internet of Things: A survey,'' IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 414–454, 1st Quart., 2014.*
12. *M. Nitti, V. Pilloni, G. Colistra, and L. Atzori, ''The virtual object as a major element of the Internet of Things: A survey,'' IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1228–1240, 2nd Quart., 2015.*
13. *S. Verma, Y. Kawamoto, Z. M. Fadlullah, H. Nishiyama, and N. Kato, ''A survey on network methodologies for real-time analytics of massive IoT data and open research issues,'' IEEE Commun. Surveys Tuts., vol. 19, no. 3, pp. 1457–1477, 3rd Quart., 2017.*
14. *Z. Yan, P. Zhang, and A. V. Vasilakos, ''A survey on trust management for Internet of Things,'' J, Netw. Comput, Appl., vol. 42, pp. 120–134, Jun. 2014.*
15. *J. Caminha, A. Perkusich, and M. Perkusich, ''A smart middleware to perform semantic discovery and trust evaluation for the Internet of Things,'' in Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC), Jan. 2018, pp. 1–2.*
16. *L. C. C. De Biase, P. C. Calcina-Ccori, F. S. C. Silva, and M. K. Zuffo, ''The semantic mediation for the swarm: An adaptable and organic solution for the Internet of Things,'' in Proc. IEEE Int. Conf. Consum. Electron. (ICCE), Jan. 2017, pp. 78–79.*
17. *M. Nitti, R. Girau, and L. Atzori, ''Trustworthiness management in the social Internet of Things,'' IEEE Trans. Knowl. Data Eng., vol. 26, no. 5, pp. 1253–1266, May 2014.*
18. *J. Guo, I.-R. Chen, and J. J. P. Tsai, ''A survey of trust computation models for service management in Internet of Things systems,'' Comput. Commun., vol. 97, pp. 1–14, Jan. 2017.*
19. *Kalsoom, T.; Ramzan, N.; Ahmed, S.; Ur-Rehman, M. Advances in Sensor Technologies in the Era of Smart Factory and Industry 4.0. Sensors **2020**, 20, 6783.*
20. *Din, I.U.; Guizani, M.; Hassan, S.; Kim, B.S.; Khan, M.K.; Atiquzzaman, M.; Ahmed, S.H. The Internet of Things: A review of enabled technologies and future challenges. IEEE Access 2018, 7, 7606–7640*
21. *S. Nakamoto, ―Bitcoin: A peer-to-peer electronic cash system,‖ 2008.*
22. *Silvello, A. "IoT and Connected Insurance Reshaping The Health Insurance Industry. A Customer-centric" From Cure To Care" Approach." ICST Trans. Ambient Systems 4, no. 15 (2017): e5.*
23. *Sun, Chenfei, Qingzhong Li, Hui Li, Yuliang Shi, Shidong Zhang, and Wei Guo. "Patient cluster divergence based healthcare insurance fraudster detection." IEEE Access 7 (2018): 14162-14170.*
24. *McGhin, Thomas, Kim-Kwang Raymond Choo, Charles Zhechao Liu, and Debiao He. "Blockchain in healthcare applications: Research challenges and opportunities." Journal of Network and Computer Applications (2019)*
25. *Marcu, I.; Suciu, G.; B ˘al ˘aceanu, C.; Vulpe, A.; Dr ˘agulinescu, A.M. Arrowhead Technology for Digitalization and Automation Solution: Smart Cities and Smart Agriculture. Sensors 2020, 20, 1464.*
26. *Jiang, X.; Yi, W.; Chen, Y.; He, H. Energy efficient smart irrigation system based on 6LoWPAN. In Cloud Computing and Security, Proceedings of the International Conference on Cloud Computing and Security, Haikou, China, 8–10 June 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 308–319.*

27. *Mousavi, S.K.; Ghaffari, A.; Besharat, S.; Afshari, H. Improving the security of internet of things using cryptographic algorithms: A case of smart irrigation systems. J. Ambient. Intell. Humaniz. Comput. 2020, 1–19. doi:10.1007/s12652-020-02303-5.*
28. *Azhar, M.; Kuntoji, N.; Kumar, P.; Balaraj, T.; Muralidhara, G.D. Solar based security and smart irrigation system for agriculture. Int. J. Adv. Res. Ideas Innov. Technol. 2018, 4, 1298–1300*
29. *Munir, M.S.; Bajwa, I.S.; Cheema, S.M. An intelligent and secure smart watering system using fuzzy logic and blockchain. Comput. Electr. Eng. 2019, 77, 109–119.*
30. *Kamienski, C.; Kleinschmidt, J.; Soininen, J.P.; Kolehmainen, K.; Roffia, L.; Visoli, M.; Maia, R.F.; Fernandes, S. SWAMP: Smart water management platform overview and security challenges. In Proceedings of the 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Luxembourg, 25–28 June 2018; pp. 49–50.*
31. *Tzounis, A.; Katsoulas, N.; Bartzanas, T.; Kittas, C. Internet of Things in agriculture, recent advances and future challenges. Biosyst. Eng. 2017, 164, 31–48.*
32. *Elijah, O.; Rahman, T.A.; Orikumhi, I.; Leow, C.Y.; Hindia, M.N. An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. IEEE Internet Things J. 2018, 5, 3758–3773.*
33. *Villa-Henriksen, A.; Edwards, G.T.; Pesonen, L.A.; Green, O.; Sørensen, C.A.G. Internet of Things in arable farming: Implementation, applications, challenges and potential. Biosyst. Eng. 2020, 191, 60–84.*
34. *Haseeb, K.; Ud Din, I.; Almogren, A.; Islam, N. An Energy Efficient and Secure IoT-Based WSN Framework: An Application to Smart Agriculture. Sensors 2020, 20, 2081.*
35. *Sharma, A.; Pilli, E.S.; Mazumdar, A.P.; Gera, P. Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes. Comput. Commun. 2020, 160, 475–493.*
36. *Chahal, R.K.; Kumar, N.; Batra, S. Trust management in social Internet of Things: A taxonomy, open issues, and challenges. Comput. Commun. 2020, 150, 13–46.*
37. *Jayashankar, P.; Nilakanta, S.; Johnston, W.J.; Gill, P.; Burres, R. IoT adoption in agriculture: The role of trust, perceived value and risk. J. Bus. Ind. Mark. 2018, 33, 804–821.*
38. *M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, ―Bubbles of trust: A decentralized blockchain-based authentication system for IoT,‖ Computers & Security, vol. 78, pp. 126–142, September, 2018.blockchain cloud architecture for IoT,‖ IEEE Access, vol. 6, pp. 115–124, February, 2018.*
39. *Fotiou, Nikos, and George C. Polyzos. "Smart contracts for the internet of things: Opportunities and challenges." In 2018 IEEE European Conference on Networks and Communications (EuCNC), Ljubljana, Slovenia,2018,pp. 256-260.*
40. *Bhabendu Kumar Mohanta, Debasish Jena, UtkalikaSatapathy, "Trust Management in IOT Enable Healthcare System using Ethereum based Smart Contract", International journal of scientific & technology research volume 8, issue 09, september 2019.*