Mathematical Statistician and Engineering Applications
SSN: 2094-0343
2326-9865

An Exhaustive Review of Blockchain Based Approaches for Enhancing Security in Internet of Things Environment

Author : Anil Verma
SP Jain School of Global Management
anil.dj21dba013@spjain.org

Co Author: Prof A.Seetharaman
SP Jain School of Global Management
seetha.raman@spjain.org

Article Info
Page Number: 1477-1486
Publication Issue:
Vol. 71 No. 3s (2022)

Article History
Article Received: 22 April 2022
Revised: 10 May 2022
Accepted: 15 June 2022
Publication: 19 July 2022

Abstract: Bridging the currently available trust domain remains as the biggest challenge in internet of things. Block chains have newly fascinated the attention of shareholders through an extensive duration of industries: from finance to several utilities. It is a hopeful expertise for instituting trust in IoT networks, where network nodes do not inevitably trust each other. Recent explosion of the internet around block chains would remain as a stable fit for security in internet of things sector. The block chain technology could provide synchronized as well as secure transactions over multiple users and it offer perfect shared time stamped records which can't be modified by anyone. It permits distributed peer-to-peer network in which non-trusting members could communicate with one other without the need for trusted intermediary, in an authenticated manner. This current research work presents a comprehensive review of the background of Internet of Things (IoT), the scope of block chain based IoT security systems and the research problem prevailing in this field.
Keywords: Block Chain, Security, Internet of Things, IOT.

I. INTRODUCTION

1.1 Importance of Security in Internet of Things (IoT)

Several innovative forms of technology on the intelligent processes for smart applications suitably prefer Internet of Things (IoT). Modern equipments are encompassed with multiple sensors and switches which communicate by means of central axis known as gateways. These gateways are the control systems that contain a user interface over mobile phone, tablet or computer and the communication networks are managed and monitored by the IoT. Numerous research works conducted which mainly focused on IoT was about privacy issues and the information security-based constraints. Research work in [3] conducted middleware that could integrate various IoT data and interrelate several data formats combined to a single format. Security in IoT is an effective area of research which attracts the research point of view from academics, industrial and government firms. Design and expansion of IoT centered system involves various organizations and the attacks on IoT devices were modest and relaxed to conduct. Some of the security types are general security, network security and application security. This includes security over perception layer, network layer, middleware layer and the application level [30].

1.2. Importance of block chain techniques in the IoT security systems

On a basic level, a block chain technology ought to be known as a distributed data structure with timestamp [20]. To achieve above mentioned characteristic of block chain, everyone can consider this technology as the interconnected mechanisms, and it can give few important features to the framework [26]. Generally, we can have signed transactions between peers at the lowest level of the framework. This signifies an understanding between two members which contain transfer of physical or digital resources and the completion of task. At any task, one member should sign the transaction as well as it should be dispersed to its neighbors. Any substance can interface with block chain known to be node. It can check all the rules of block

chain which are called as full nodes. These nodes make every transaction into blocks which are highly responsible to decide whether it is a valid or invalid transaction, and ought to be kept in block chain or not.

1.3 Contributions of the review study

A block chain provides trustless networks as anyone could transact even though they do not trust each other, and absence of any trusted intermediary means faster means of settlement among the transacting parties. Bulk usage of cryptography, which is a major key characteristic of block chain network, necessitates authoritative aspect behind all such interactions in network. Some of the smart contracts – self-executing scripts which relies on block chain interrelates these concepts and allow for proper, distributed and heavily automated workflows. This is the reason block chains are attractive to researchers and inventors working on the Internet of Things (IoT) field.

Main aim of this survey paper is to accomplish a study on the working aspect of block chains and smart contracts, to recognize the pros and cons that their introduction could bring to a system and to specify the ways block chain and IoT unites together. This means of survey and information would allow anyone to notify potentially newer cases for their IoT works and to make knowledgeable and educated means of approaches while working with such environment which integrates block chain and IoT.

1.4 Organization of the paper

The current review paper is structured as follows. Section I describes the introduction part which includes Importance of Security in Internet of Things (IoT), Importance of block chain techniques in the IoT security systems, Contributions of the review study and Organization of the paper. Section II is the theoretical background of block chain based IoT security systems including IoT- an introduction, IoT applications, Architecture of IoT, Security aspects and trust management in IoT, block chain technology, types of block chain technology and Structures and techniques of block chain system. Section III is the block chain and smart contracts for IoT security comprising of Applications of Block chain and smart contract for trusted IoT and Security vulnerabilities in Block chain and smart contracts. Section IV gives the research gaps with respect to performance metrics and parameters evaluations. Section V is the conclusion part which presents the findings of the block chain based IoT security, and some suggestions will be recommended for the use of block chain based IoT security.

II. THEORETICAL BACKGROUND

This section presents the theoretical background of Block chain based IoT security systems. It covers

a) IoT - An introduction

An IoT system includes computers, sensors that could act concerning the data gathered by sensors through a machine learning approach. Machine learning is the way of the identical learning process to humans by assembling data from their environments and nature rules. Around the fourth industrial revolution, the equipment used in industry was linked to the internet to collaborate with other machinery available. Some of the components used in this process are sensors, actuators that possess an electronic unit. In these systems, the physical systems and embedded systems are incorporated which is defined as cyber-physical systems. These cyber-physical systems when connected to the internet, these systems form an “Internet of Things” (IoT) network [1].

Currently existing IoT systems are established on a highly centralized system architecture along with computation and communication abilities which provides physical environs. Here the

enormous, embedded devices were attached which assist services to end-users. Other than the data management capabilities, the system security flaws increase as the IoT systems become progressively complex and broad [2]. The IoT systems are assumed to operate in a distributed environment by having a reduced delay necessity and thus the several devices from numerous IoT systems could mingle with one another to establish value-added services. Hence the distributed security approaches were not found to be appropriate for IoT systems due to their centralized nature and scalability concerns. A decentralized way of lightweight block-chain authentication mechanism is presented [3] for IoT systems which is found to be applicable for a huge number of scenarios and the mechanism is mainly based on fog computing and public block chain concept.

b) IoT applications

The Internet of Things (IoT) and the billions of sensors that might be arrayed in the succeeding decade. IoT is proved to an effective technology in current wireless communication era; in which the basic element is interaction or connection between a combination of physical objects with the support of addressing systems. It could be applicable in diverse fields such as industry, healthcare systems, smart homes and agriculture. With agricultural systems, the IoT systems advocates the enhancement of cultivation yields [1]. Research in [2] denotes a wide range of technologies designed for several IoT applications including machine learning.

The machine learning methods are being used in numerous fields and they are projected to establish pervasive connections for the wireless nodes. Since agriculture evolves as an effective paradigm in country's economic status, it exhibits creative association on the way to human evolution. In smart agriculture, the intelligent systems and intelligent protocol along with the sensor devices has been established. In each smart system, diverse techniques were employed and IoT serves as the central part of all smart works [13]. Role of machine learning with IoT systems are associated in other features such as cloud down to embedded devices. Here, several uses of machine learning in IoT were executed for the purpose of application data processing and the management tasks [4].

Research work in [5] conducted middleware that could integrate various IoT data and interrelate several data formats combined to a single format. Security in IoT is an effective area of research which attracts the research point of view from academics, industrial and government firms. Design and expansion of IoT centered system involves various organizations and the attacks on IoT devices were modest and relaxed to conduct. Some of the security types are general security, network security and application security [22]. This includes security over perception layer, network layer, middleware layer and the application level [6].

Major advantages of IoT platform includes

- smart home applications,
- commercial benefits,
- customization benefits for better efficiency,
- compatibility and orchestration among the appliances
- automating for comfort benefits
- Reduced breach risks [1].

c) Architecture of IoT

In past two years alone, about 90% of the data in the world has been formed. This further increases day by day, due to IoT initiation, and population growth. As in IoT technologies and block-chain, the development prospects are wide; there ascends the symbiotic relationship of the two fields. Distributed wireless sensor networks are a prodigious support for technical and human fruition, despite their massive shortcomings [5]. The distributed wireless sensor network institutes that the block-chain possibly will expands IoT by declining its inefficiencies

and exploiting potential [5]. The challenging consideration for prompting decentralized IoT platforms are generally obsessed by means of block-chain expertise and its abilities [21]. To provide safe and auditable data exchange in heterogeneous context-aware improvements with interweaved smart devices are the key concern. Working in a decentralized and computerized way endows the scalability of the network. Confident and independent real-time payment services, public and private transport methods are aided by block-chain interoperability [18]. One such example is Filecoin, a memory storage purveyor or EtherAPI that expedites the API calls monetization. As expansion, IoT devices could be associated with their crypto currencies-based bank account. In this way, micro-transactions could be done in exchange for services whereas; similar way of system is also unfailing to the smart grid domain for the endowment of energy sale. Block-chain supports IoT based results for problems such as, high running cost of centralized means [20]. The security level of IoT and WSN is increased by a decentralized and protected P2P model [14]. This permits an advanced control of IoT devices for up-to-date systems.

d) Security aspects and trust management in IoT

Major specifications of IoT standards does not define an accurate security model and so the aim of each security model is to formulate against what threats an IoT system should be protected from; and who were the potential attackers (threat model or attacker model). Major goals of the security design will be formulated, and the security architecture should be developed which considers the potential threats in a comprehensive manner. Research work on the security economics in IoT and normalization extended slight attention so far. In terms of distributed schemes, the security economics of electricity metering were examined the reasons why trained products fail to full-fill standardized security requirements were analyzed. A context was anticipated to examine the economic viability of protocols all through the standard progression. The trade-offs concerning energy and security controls in the IoT ecosystem were defined [7]. IoT possess the prospective to contest or amend specific of recognized studies in the range of societal commerce field. Thus, the IoT is all about generating digital based connections and depictions of a real-world entities and the smart IoT objects were amplified by the radio-frequency identification, near-field communication, microprocessors or sensors built-in or devoted to them and it could facilitate the remote control over the internet [8].

e)Block chain technology

Block chain is an innovative technology which can synchronize ledger content of numerous clients through community validation. This technology was initially created to support renowned crypto currency bitcoin [1] in 2008 [2].

Block chain technology can provide synchronized as well as secure transactions over multiple users. It provides perfect shared time stamped records which can't be modified by anyone. This is known to be disruptive innovation which creates big revolution in user interaction, automate payments as well as transaction tracking and tracing. This technology is cost effective in wiping out the requirement for centralized authority over few members to verify transactions. Each transaction is cryptographically verified by mining hubs which generally hold a copy of the whole record [3].

Various issues related to block chain, for example, congestion issue, exchange delays, and expanded exchange expenses will raise concerns. Thus, the innovation may not be a reasonable methodology for government or private areas to fabricate their plan of action upon the block chain stage. In addition, substantial storage space is needed due to increased block size which causes delayed propagation in block chain, and it leads towards centralization as well as trust issues as clients might want to work and keep up such a huge block chain [14]. In this way, it has become an extraordinary test to manage the exchange off between block chain size and trust.

The important qualities of block chain are auditability, transparency, decentralization and immutability [5]. Block chain is generally known to be firmly connected blocks which has public and private ledgers with transactional data. In order to achieve above mentioned qualities, distributed consensus algorithms and asymmetric cryptographic techniques are utilized. These can make immutable transactions, which may not be altered once they are authoritatively approved and enrolled in the block chain. Simultaneously, robustness and reliability are also needed to consider providing highly trusted platforms of block chain [4].

Bitcoin is the most celebrated use of block chain and applied over diverse applications far beyond digital currencies. this can eliminate bank or any kind of intermediary for transactions among multiple users and this technology can plays vital role in many services like computerized resources, settlement and online instalment [6]. This technology can be utilized in many ventures including healthcare, finance, and government [7].

Extra uses of block chain incorporate crowd funding, identity management, governing public records, electronic voting as well distributed resources. Block chain technology has incredible potential and replaces current digital platforms but has few technical constraints. Scalability is the major issue in block chain technology [11]. In case of bitcoin, due to its frequency and size limitation, there will be a scalability issue on the network transactions [12].

f) Types of block chain technology

Different kinds of block-chain architecture exist, and each of them has unique design.

Public Block-chain

In public block-chain, each one in the network validates the transaction and they could take part in consensus gaining process. Decentralization is ensured by initiating a peer-to-peer transaction block. Before initiating to the system, each transaction is linked to the block-chain. Therefore, the transactions are confirmed and synced to all nodes in the network. Anyone with a computer and internet connection can be enumerated as a node and can be delivered with the complete block-chain antiquity. It states that each person can check the transaction and validate it and can also subsidize in the process of receiving consensus. The advantage of the public network is the concealment of the consumer and full pellucidity of the ledger [14].

Private Block-chain

In private block-chain, the nodes are found to be constrained in nature. Not all nodes can take part in this, needs austere expert control on the data admission. In confirmation and validation of all transactions, strict management is involved. A company or organization could confirm and validate their transactions anytime. This kind of approach provides an advanced efficacy in verification concern of transactions executed [5].

Consortium Block-chain

Consortium block-chain is a collection of public and private block-chain and can be inferred as partially decentralized. These block-chains are open to public, but the complete data is not accessible to all the participants. User privileges vary and blocks are endorsed based on the pre-defined rules. Consortium block-chains are hence, "partly decentralized". Consortium block-chains are the ones in which the consensus process is systematized by a pre-selected set of trusted nodes. A block is auxiliary to the chain after consensus is accomplished through the transaction validation by a group from the pre-selected set of nodes. In a consortium block-chain, the right of reading the block-chain can be public or made delimited only to participants. As well, consortium block-chains are dignified to be moderately decentralized unlike private block-chains. A collective block-chain model is more pleasing to trade companies, because of the point that it is decentralized unlike private block-chains [13].

g) Structures and techniques of block chain system

Each hub utilizes private key cryptography to start transaction in a block chain network. This is generally considered as a data structure which denotes transfer of digital resources among the

block chain network peers. Transactions are stored in an unsubstantiated transaction pool, and it has been propagated by flooding protocol which is known to be Gossip protocol. Based on few preset criteria peers need to select and validate the transactions. For instance, the hubs attempt to confirm and approve every transaction by checking whether an initiator has adequate equalization to trigger transactions or by attempting to trick the framework by implementing double spending.

Double spending is nothing, but similar input can be utilized for more transactions [24]. After the transaction verification process only, the transaction gets included in a block. The miners are known to be peers who can utilize complete computational power [25].

In order to publish a block, all minor hubs should solve computational puzzle. The first puzzle solving minor has the chance to create a new block. At the same time some incentive is given for effectively making another block. Consensus algorithms are utilized to verify the peers of network, which is a method that help a decentralized system goes to a concurrence on specific issues.

New block can be added to the current chain and neighbor duplicate of each companion's changeless record. Then the transactions are affirmed. Link has been created among next block and newly created block via cryptographic hash pointer. During this process the block can obtain its initial affirmation while the next transaction gets affirmation. Generally, a single transaction required 6 affirmations in the system to view as finals.

III. BLOCK CHAIN AND SMART CONTRACTS FOR IOT SECURITY

3.1. Applications of Block chain and smart contract for trusted IoT

Block-chain has turned out to be one of the major counsels in both business and technology. It is dignified as the technology that will rationalize the finance sector with its proficiency to function without any central authority or mediators. Furthermore, it is also supposed that block-chain will be helpful for further industries because of its ability of storing tamper-proof files and handling a vast track of records in a disciplined way. Though, parallel to other promising technologies, block-chain has its precincts and is not possible for all types of business model. This segment entitles the issues and contests of block-chain technology as following:

Block-chain based applications augment the digital approval of personal and academic learning procedure. Assembling, reporting, and analyzing facts about the school for performing decision making process is acknowledged by block-chain aided school statistics. Finally, in publication process block-chain is used moreover for well-organizing script submissions or for conducting peer review for manuscript verification process. Block-chain is examined to be an efficient viewpoint for refining security levels of big data and scalability. While combined with other storage systems, block-chain is found to be well- effective in carry out data mining techniques. Therefore, privacy and security are the chief factors that are concerned while depending on block-chain technology.

Maintaining high level of privacy in transactions is the extremely complicated part of block-chain technology. In evolving anonymity of block-chains, several ways have been predicted [11]. They are zero knowledge proofs or mixing facilities. Mixing services focuses on transactional privacy by changing the amount from input addresses to output addresses. By doing this, the users could have an option to neglect using the same address.

The block-chain is frequently vulnerable to transactional privacy leakage as the details of all public keys are perceptible to one and all in the network. The suggested solutions for attaining obscurity in block chains can be extensively categorized into mixing and anonymous solution. Mixing is a service that propositions anonymity by transferring resources from info delivers, to various yield addresses [11].

One of the major application requirements of IoT systems is healthcare systems in which multiple devices are associated and synchronized to establish an IoT based network devoted to healthcare systems. The healthcare-based internet of things are the systems which would gather data from diverse sensing devices using middleware and for effective handling of such heterogeneity, IoT necessitates interoperability and trust issues provision. One of the methods to assure noteworthy IoT information is with the support of distributed service trusted by entirety of its members. This could ensure that information stays immutable in nature and the block chain technology assures all such requirements. Some of the commercial based examples of IoT devices include smart health and fitness wearable such as the Fitbit and the Garmin Vivofit, smart thermostats such as the Nest learning thermostat, and smart home lighting products such as the Philips Hue, among many others. In the ideal version of a wired future, all devices in smart homes communicate with one or more in a seamless manner. Smart home technology based on IoT has transformed human life by providing connectivity to everyone irrespective of time and place. Home automation systems have become progressively sophisticated in current years. These systems deliver infrastructure and approaches to exchange all types of usage information and services. A smart home is a domain of IoT, which is the network of physical devices that afford electronic, sensor, software, and network connectivity inside a home network [4].

3.2. Security vulnerabilities in Block chain and smart contracts

Block chain environment plays a vital task in cyber security and with the applied efforts for realizing huge-scale quantum computers, utmost current cryptographic mechanisms might be hacked. Therefore, requires a quantum tool utilized for scheming block chain backgrounds to have the capability to be accomplished in the level of digital computers and resist the possible attacks from equally digital and quantum computers. Quantum walks might be utilized as a quantum-inspired typical model for planning innovative cryptographic algorithms. A new authentication and encryption protocol is presented based on quantum-inspired quantum walks (QIQW) [1].

IV. RESEARCH GAPS

This section summarizes the research gaps with respect to performance metrics and parameters evaluations.

Due to the wide diversity in the communication media deployed in establishing potentially sensitive way of data, an IoT application could be vulnerable to several security-based susceptibilities. All these vulnerabilities could be unique in nature and mainly based on the corresponding medium involved. Wireless medium is one such vulnerable medium and here the nature is broadcasting. Appropriately, the transmission method based on this kind of media is exposed to eavesdropping, replay attack, and tampering attacks. The attacker could similarly introduce malicious code into the wireless routing node, thus distressing the communication of the entire wireless network. Collision is likewise an issue in wireless networks: even if channel is existing, it cannot assure that the communication is dependable. Alternative critical problem is delay, mostly for applications that enforce real-time restraints. In intricate environments, there is huge-scale deployment of sensor nodes through numerous ad hoc technologies, making manageability a non-trivial concern. Lastly, the network topology is susceptible to environs and node failure, which could compromise the consistency of information transmission [16]. Of course, the transition to a decentralized network might not continually make sense. On top of that, even if such a transition is anticipated, the application's requirements might be such that a block chain-based network cannot fulfil them. Block chains and smart contracts bring a slew of advantages to the table, but as seen, they also originate with a bag of drawbacks [17]. Once the

blocks are mined into the block chain, it is guaranteed that the inter-node connections recorded in the block's transactions are strongly recorded and are tamper-proof. Providing a tamper-proof audit trail of inter-node interactions is a compulsory but inadequate constituent to convey end-to-end trust in IoT. Storing the hash of the data on the block chain does confirm that the reliability of the stored data could be confirmed by relating its hash against the block chain-stored hash value. The authenticity of the observational data itself in the first place, however, is not guaranteed. As IoT data is a statement of the physical environment, its capture could include noise, bias, sensor drift, or manipulation by a malicious entity. The immutability of block chain does not defend against this risk related with data capture, as inaccurate observational data that is secured with block chain might not be useful to the IoT end users [19].

V. CONCLUSION

This research work provides a review on block chain-based approaches for enhancing security in internet of things environment. Owing to the decentralized infrastructure and peer-to-peer nature, block-chain technology is remarkably predictable. Undeniably, block-chain is the embryonic topic in this present year. Some of the concerns are being enriched formerly along with the different methods developed on the application side. Combination of IoT and block chains could be a powerful tool as presented, as it gives resilient, truly distributed peer-to-peer systems and the capability to interconnect with peers in a trustless and auditable manner. The smart controllers allow to automatically initiate the complex multi-step processes and devices in IoT ecosystem are the points of contact with physical world. When all of them are joined, it would lead to automate time-consuming workflows in new and exclusive methods, accomplishing cryptographic verifiability, as well as substantial cost and time savings in the manner. Moreover, it is believed that the constant integration of block chains in the IoT domain would cause momentous transformations across several industries, bringing about novel business models and having to reassess how prevailing systems and processes are executed.

REFERENCES

1. Abd El-Latif, A.A., Abd-El-Atty, B., Mehmood, I., Muhammad, K., Venegas-Andraca, S. E., Peng, J., 2021. Quantum-Inspired Blockchain-Based Cybersecurity: Securing Smart Edge Utilities in IoT-Based Smart Cities. Inf. Process. Manag. 58 (4), 102549. https://doi.org/10.1016/j.ipm.2021.102549.
2. Abou-Nassar, E.M., Iliyasu, A.M., El-Kafrawy, P.M., Song, O.-Y., Bashir, A.K., El-Latif, A.A.A., 2020. DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems. IEEE Access 8, 111223–111238. https:// doi.org/10.1109/Access.628763910.1109/ACCESS.2020.2999468.
3. Abraham, S., Beard, J., Manijacob, R., 2017. Remote environmental monitoring using Internet of Things (IoT). GHTC 2017 - IEEE Glob. Humanit. Technol. Conf. Proc. 2017-Janua, 1–6. https://doi.org/10.1109/GHTC.2017.8239335
4. Arellano-Zubiate, J. ., J. . Izquierdo-Calongos, A. . Delgado, and E. L. . Huamaní. "Vehicle Anti-Theft Back-Up System Using RFID Implant Technology". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 5, May 2022, pp. 36-40, doi:10.17762/ijritcc.v10i5.5551.
5. Alaa, M., Zaidan, A.A., Zaidan, B.B., Talal, M., Kiah, M.L.M., 2017. A review of smart home applications based on Internet of Things. https://doi.org/10.1016/j. Jnca.2017.08.017
6. Ali, J., Ali, T., Alsaawy, Y., Khalid, A.S., Musa, S., 2019. Blockchain-based smart-IoT trust zone

measurement architecture. ACM Int. Conf. Proceeding Ser. Part F1481, 152–157. https://doi.org/10.1145/3312614.3312646.

7. Aman, M.N., Sikdar, B., Chua, K.C., Ali, A., 2018. Low Power Data Integrity in IoT Systems 4662. https://doi.org/10.1109/JIOT.2018.2833206
8. Asiri, S., Miri, A., 2016. An IoT trust and reputation model based on recommender systems. 2016 14th Annu. Conf. Privacy. Secur. Trust. PST 2016, 561–568. https://doi.org/10.1109/PST.2016.7907017. Attack-Resistant Trust Management Model Based on Beta Function for Distributed Routing in Internet of Things | Request PDF [WWW Document], n.d. URL https://www.researchgate.net/publication/285739133_Attack-Resistant_Trust_Management_Model_Based_on_Beta_Function_for_Distributed_Routing_in_Internet_of_Things (accessed 4.10.21).
9. Atzori, L., Iera, A., Morabito, G., 2010. The Internet of Things: A survey. Comput. Networks 54 (15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010. B, A.Z.O., B, B.B., B, K.S., 2018. Using Blockchain for IOT Access Control. Springer International Publishing. https://doi.org/10.1007/978-3-319-94370-1
10. Baker, S.B., Xiang, W.E.I., Member, S., Atkinson, I.A.N., 2017. Internet of Things for Smart Healthcare.pdf. IEEE Access 5, 26521–26544. Bao, F., Chen, I.R., 2012. Dynamic trust management for internet of things applications. Self-IoT'12 - Proc. 2012 Int. Work. Self-Aware Internet Things, Co-located with ICAC'12 1–6. https://doi.org/10.1145/2378023.2378025
11. Beck, R., Czepluch, J.S., Lollike, N., Malone, S., 2016. Association for Information Systems AIS Electronic Library (AISeL) BLOCKCHAIN – THE GATEWAY TO TRUST- FREE CRYPTOGRAPHIC TRANSACTIONS. Twenty-Fourth Eur. Conf. Inf. Syst. (ECIS), _ Istanbul,Turkey 6, 4013–4027
12. Ben Saied, Y., Olivereau, A., Zeghlache, D., Laurent, M., 2013. Trust management system design for the Internet of Things: A context-aware and multi-service approach. Comput. Secur. 39, 351–365. https://doi.org/10.1016/ j.cose.2013.09.001.
13. Bhattacharjee, S., Salimitari, M., Chatterjee, M., Kwiat, K., Kamhoua, C., 2018. Preserving Data Integrity in IoT Networks Under Opportunistic Data Manipulation. Proc. - 2017 IEEE 15th Int. Conf. Dependable, Auton. Secur. Comput. 2017 IEEE 15th Int. Conf. Pervasive Intell. Comput. 2017 IEEE 3rd Int. Conf. Big Data Intell. Compu 2018-Janua, 446–453. https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.87 Blockchain Identity Management: The Definitive Guide (2021 Update) [WWW Document], n.d. URL https://tykn.tech/identity-management-blockchain/#A_Blockchain_based_Identity_Management_Solution (accessed 6.2.21).
14. Boyes, H., Hallaq, B., Cunningham, J., Watson, T., 2018. The industrial internet of things (IIoT): An analysis framework. Comput. Ind. 101, 1–12. https://doi.org/ 10.1016/j.compind.2018.04.015.
15. Butt, Talal Ashraf, Iqbal, Razi, Salah, Khaled, Aloqaily, Moayad, Jararweh, Yaser, 2019. Privacy Management in Social Internet of Vehicles: Review, Challenges and Blockchain Based Solutions. IEEE Access 7, 79694–79713. https://doi.org/ 10.1109/Access.628763910.1109/ACCESS.2019.2922236.
16. Varun, B. N. ., S. . Vasavi, and S. . Basu. "Python Implementation of Intelligent System for Quality Control of Argo Floats Using Alpha Convex Hull". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 5, May 2022, pp. 60-64, doi:10.17762/ijritcc.v10i5.5554.
17. Chen, Dong, Chang, Guiran, Sun, Dawei, Li, Jiajia, Jia, Jie, Wang, Xingwei, 2011. TRMIoT: A trust management model based on fuzzy reputation for internet of things. Comput. Sci. Inf. Syst. 8 (4), 1207–1228. https://doi.org/10.2298/ CSIS110303056C
18. Chen, Kejun, Zhang, Shuai, Li, Zhikun, Zhang, Yi, Deng, Qingxu, Ray, Sandip, Jin, Yier, 2018. Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. J. Hardw. Syst. Secur. 2 (2), 97–110. https://doi.org/10.1007/ s41635-017-0029-7.
19. Christidis, K., Devetsikiotis, M., 2016. Blockchains and Smart Contracts for the Internet of Things.

IEEE Access 4, 2292–2303. https://doi.org/10.1109/ ACCESS.2016.2566339.
20. Conti, Mauro, Sandeep Kumar, E., Lal, Chhagan, Ruj, Sushmita, 2018. A survey on security and privacy issues of bitcoin. IEEE Commun. Surv. Tutorials 20 (4), 3416–3452. https://doi.org/10.1109/COMST.973910.1109/COMST.2018.2842460.
21. Dedeoglu, V., Jurdak, R., Sydney, Putra UNSW, G.D., Ali Dorri, A., 2019. A Trust Architecture for Blockchain in IoT. Proc. 16th EAI Int. Conf. Mob. Ubiquitous Syst. Comput. Netw. Serv. https://doi.org/10.1145/3360774. Definition of Internet Of Things (iot) - Gartner Information Technology Glossary [WWW Document], n.d. URL https://www.gartner.com/en/informationtechnology/glossary/internet-of-things (accessed 4.9.21).
22. Di Pietro, R., Salleras, X., Signorini, M., Waisbard, E., 2018. A blockchain-based trust system for the internet of things. Proc. ACM Symp. Access Control Model. Technol. SACMAT 18, 77–83. https://doi.org/10.1145/3205977.3205993.
23. Dika, A., Nowostawski, M., 2018. Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree. Proc. - IEEE 2018 Int. Congr. Cybermatics 2018 IEEE Conf. Internet Things, Green Comput. Commun. Cyber, Phys. Soc. Comput. Smart Data, Blockchain, Comput. Inf. Technol. iThings/Gree 955–962. https://doi.org/10.1109/Cybermatics
24. Djedjig, N., Tandjaoui, D., Romdhani, I., Medjek, F., 2018. Trust management in the internet of things, in: Security and Privacy in Smart Sensor Networks. IGI Global, pp. 122–146. https://doi.org/10.4018/978-1-5225-5736-4.ch007
25. N. A. Farooqui, A. K. Mishra, and R. Mehra, “IOT based Automated Greenhouse Using Machine Learning Approach”, Int J Intell Syst Appl Eng, vol. 10, no. 2, pp. 226–231, May 2022.
26. Dorri, Ali, Kanhere, Salil S., Jurdak, Raja, 2019. MOF-BC: A Memory Optimized and Flexible BlockChain for Large Scale Networks. Futur. Gener. Comput. Syst. 92, 357–373.
27. Dwivedi, A.D., Srivastava, G., Dhar, S., Singh, R., 2019. A decentralized privacypreserving healthcare blockchain for IoT. Sensors (Switzerland) 19, 326. https://doi.org/10.3390/s19020326
28. El-Latif, Ahmed A. Abd, Abd-El-Atty, Bassem, Venegas-Andraca, Salvador E., Elwahsh, Haitham, Piran, Md. Jalil, Bashir, Ali Kashif, Song, Oh-Young, Mazurczyk, Wojciech, 2020. Providing End-to-End Security Using Quantum Walks in IoT Networks. IEEE Access 8, 92687–92696. https://doi.org/10.1109/ Access.628763910.1109/ACCESS.2020.2992820.
29. Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang, J., Shu, L., 2017. Authentication Protocols for Internet of Things: A Comprehensive Survey. Secur. Commun. Networks. https://doi.org/10.1155/2017/6562953
30. Fortino, Giancarlo, Fotia, Lidia, Messina, Fabrizio, Rosaci, Domenico, Sarne, Giuseppe M.L., 2020. Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges. IEEE Access 8, 60117–60125. https://doi.org/10.1109/ Access.628763910.1109/ACCESS.2020.2982318.
31. Frahat, R.T., Monowar, M.M., Buhari, S.M., 2019. Secure and Scalable Trust Management Model for IoT P2P Network. 2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2019, 1–6. https://doi.org/10.1109/CAIS.2019.8769467.
32. Frustaci, Mario, Pace, Pasquale, Aloi, Gianluca, Fortino, Giancarlo, 2018. Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet Things J. 5 (4), 2483–2495. https://doi.org/10.1109/ JIoT.648890710.1109/JIOT.2017.2767291.
33. Ghasempour, Alireza, 2019. Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges. Inventions 4 (1), 22. https://doi.org/10.3390/inventions401002
34. J. . Hermina, N. S. . Karpagam, P. . Deepika, D. S. . Jeslet, and D. Komarasamy, “A Novel Approach to Detect Social Distancing Among People in College Campus”, Int J Intell Syst Appl Eng, vol. 10, no. 2, pp. 153–158, May 2022.