Block-Chain Based Authorization and Access Control Mechanisms for IoT Environments: Challenges and Opportunities

Asra Kalim, Deepak Singh Tomar, Sheikh Ikhlaq

Abstract: ***Internet of Things (IoT) involves interconnecting smart devices for data collection and making intelligent decisions where, the usual devices become autonomous and smart. With the swift and fast paced developments in the area of smart cities, smart homes, and smart everything the Internet of Things (IoT) is creating an exceptional role that has scope for immense growth and potential. Its objective is the seamless integration of digital and physical worlds into one ecosystem that would lead to the latest intelligent era of the Internet. This state of the art technology can offer huge potential for businesses and offer opportunities for already existent areas like healthcare, energy etc. Yet due to insufficient security techniques IoT is not completely fool proof against security breaches and privacy issues. Since IoT is made up of devices that are resource-constrained and it has a complex environment, which makes enforcement of security measures even more complicated and tricky. This is where Blockchain's (BC) "security by design" comes in; that is capable of tackling IoT's foremost security requirements. Features like transparency, data encryption, auditability, operational resilience and immutability can help remove IoT's architectural shortcomings. This paper focuses on this relationship and surveys the most relevant work in this area, for analyzing how blockchain is capable of solving the issues related to authorization and access control for IoT environments.***

Keywords: Blockchain, Smart contract, Authentication, Access control, Ethereum

I. INTRODUCTION

Kevin Ashton, the well-known name in British technology in 1999 coined the term "Internet of Things" to outline a system in which sensors are utilized for connecting objects of the Internet with the physical world. This term was used by Ashton for explaining how powerful the connection of RFID (Radio-Frequency Identification) tags to the Internet is, that are used by supply chains to keep track of goods with no human involvement. At present, IoT has become quite the rage and is being used for describing situations where Internet connectivity and computing capability and are applicable for several types of devices, sensors, objects as well as everyday items. [1]

As for Blockchain (BC), it's a list of records that are linked cryptographically and maintained in a publicly verifiable ledger that doesn't have to be controlled by a central authority; hence it's a new concept with trust among entities of various application domains. Cryptocurrency application was the originator of BC's technology, but its rapid progress on other architectures encouraged researchers to try it on security-prioritizing domains. This new architecture is advantageous due to its inherent anonymity, trust, resilience, security, integrity, autonomy, scalability and its decentralized nature. Smart Contracts for interactions between BC and third party stakeholders are supported by some implementations. An appropriate application of Blockchain technology would be for Internet of Things that has witnessed incredible growth through these few years, since their security has room for improvement because of resource constraints, hence putting users' trust at stake. [2]

II. DISTINCT FEATURES OF IOT

"The IoT represents a promising future technology that shows some common features as follows:

1) Intelligence: IoT devices become smart with integration of hardware and software algorithms that make them interact intelligently in some situations. Interaction between devices is only through intelligence in the IoT, but device and user interactions are done through the GUI and usual input methods.
2) Sensing: there cannot be IoT in absence of sensors, as they are needed to detect alterations in the environment for generation of data that that would reflect their status or interact with the environment. Capabilities are provided by sensing technologies reflecting awareness of humans and the physical world. Even though sensing information is merely analogue input from physical world, it offers perception of our complex environment.
3) Large scale: IoT devices in use rise exponentially, which are in billions and they need to be managed to facilitate their communication with each other. Hence the generated data and their interpretation for applications is a crucial need.
4) Huge amount of data: Since there are billions of IoT devices creating so much data, focus is also on security and privacy.
5) Complex system: Constraints on energy, memory and time makes it very complex to perform operations on the billions of devices.

Revised Manuscript Received on October 30, 2020.

* Correspondence Author

Asra Kalim*, Deanship of E-learning and IT, Jazan University, Kingdom of Saudi Arabia. Email: rhetoric1979@yahoo.com

Deepak Singh Tomar, Associate Professor, CSE, MANIT, Bhopal, India. Email: deepaktomarmanit@gmail.com

Sheikh Ikhlaq, Cloud Consultant, Accenture, New Delhi, India. Email: ersikhlaq@gmail.com

6) Limited energy: IoT devices are designed to consume minimal energy, as they are light and small in size and have restricted resources.
7) Dynamic environment: IoT is continuously evolving and dynamic as objects are leaving and joining the network without finding out network boundaries and they can also adapt to the varying situations as per the operating conditions.
8) Unique identity: Every IoT device has an IP address like unique identifier and are provided by IoT manufacturers that can be used for upgrading the devices to the appropriate platforms. Also, interfaces of these devices permit users to control them remotely, monitor their status and query devices.
9) Self-configuring: IoT devices can self-configure that would enable many of them to operate together and offer a particular functionality. These devices can set up networking, configure themselves as well as get latest software updates in association with device manufacturer without need for manual or user intervention.
10) Heterogeneity: This system is made of various platforms, operating systems, devices and services that are connected to one another through different protocols.
11) Context awareness: So many sensors gather information about the environmental and physical features, hence, sensor nodes are considered as context-aware, as they have knowledge about surrounding context.
12) Connectivity: It enables compatibility and network accessibility and offers additional strength to IoT by bringing together daily objects. It also offers new avenues for business in IoT that can be developed by networking of applications and smart things. [3]

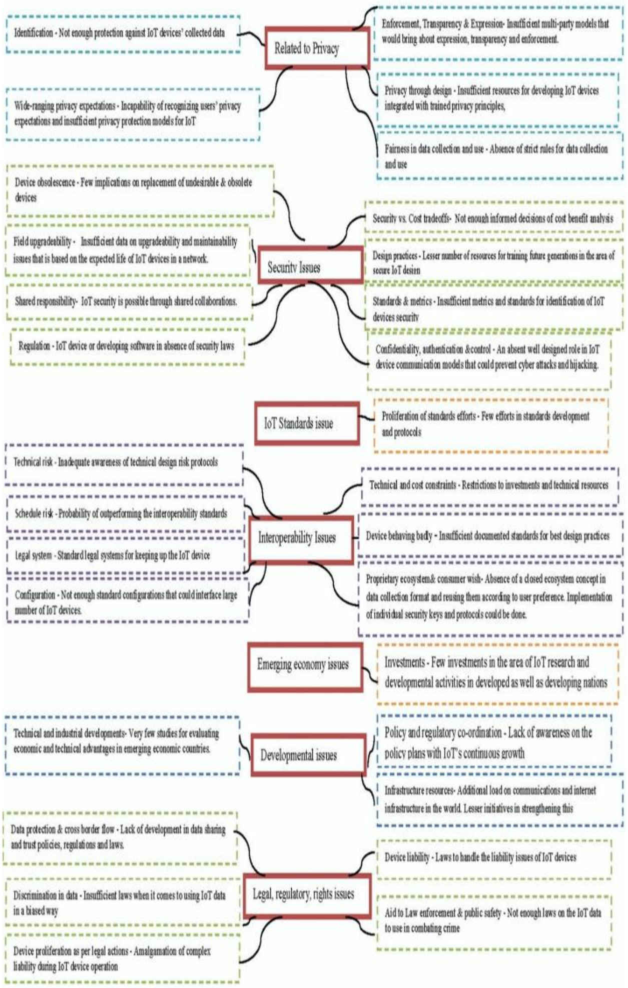
Identification - Not enough protection against IoT devices' collected data
Related to Privacy
Enforcement, Transparency & Expression- Insufficient multi-party models that would bring about expression, transparency and enforcement.
Wide-ranging privacy expectations - Incapability of recognizing users' privacy expectations and insufficient privacy protection models for IoT
Privacy through design - Insufficient resources for developing IoT devices integrated with trained privacy principles,
Fairness in data collection and use - Absence of strict rules for data collection and use
Device obsolescence - Few implications on replacement of undesirable & obsolete devices
Security vs. Cost tradeoffs- Not enough informed decisions of cost benefit analysis
Field upgradeability - Insufficient data on upgradeability and maintainability issues that is based on the expected life of IoT devices in a network.
Security Issues
Design practices - Lesser number of resources for training future generations in the area of secure IoT desion
Shared responsibility- IoT security is possible through shared collaborations.
Standards & metrics - Insufficient metrics and standards for identification of IoT devices security
Regulation - IoT device or developing software in absence of security laws
Confidentiality, authentication &control - An absent well designed role in IoT device communication models that could prevent cyber attacks and hijacking.
IoT Standards issue
Proliferation of standards efforts - Few efforts in standards development and protocols
Technical risk - Inadequate awareness of technical design risk protocols
Technical and cost constraints - Restrictions to investments and technical resources
Schedule risk - Probability of outperforming the interoperability standards
Interoperability Issues
Device behaving badly - Insufficient documented standards for best design practices
Legal system - Standard legal systems for keeping up the IoT device
Configuration - Not enough standard configurations that could interface large number of IoT devices.
Proprietary ecosystem& consumer wish- Absence of a closed ecosystem concept in data collection format and reusing them according to user preference. Implementation of individual security keys and protocols could be done.
Emerging economy issues
Investments - Few investments in the area of IoT research and developmental activities in developed as well as developing nations
Technical and industrial developments- Very few studies for evaluating economic and technical advantages in emerging economic countries.
Developmental issues
Policy and regulatory co-ordination - Lack of awareness on the policy plans with IoT's continuous growth
Infrastructure resources- Additional load on communications and internet infrastructure in the world. Lesser initiatives in strengthening this
Data protection & cross border flow - Lack of development in data sharing and trust policies, regulations and laws.
Device liability - Laws to handle the liability issues of IoT devices
Discrimination in data - Insufficient laws when it comes to using IoT data in a biased way
Legal, regulatory, rights issues
Aid to Law enforcement & public safety - Not enough laws on the IoT data to use in combating crime
Device proliferation as per legal actions - Amalgamation of complex liability during IoT device operation

Fig. 1 Issues and challenges in IoT Privacy and Security Issues

III. BENEFITS OF HAVING IOT INTEGRATION WITH BLOCKCHAIN:

This integration can bring about the following advancements (but are not limited to):

Identity: participants can identify each and every device through the common blockchain system. The data entered into the system is irrefutable and can uniquely identify the actual data that was fed by a device. Furthermore, blockchain is able to offer trusted distributed authorization and authentication of devices for IoT applications. This could help improve IoT field along with its participants.

Scalability and Decentralization: the bottlenecks and points of failure that are found in centralized architecture can be dealt with through a P2P distributed one and it will also prevent the system where some big companies will have a stronghold over the storage and data processing of large number of people. When decentralization of architecture is done, there is improved fault tolerance and system scalability. Hence, IoT silos will be decreased and will improve the IoT scalability.

Reliability: the information of IoT devices can stay indisputable and distributed over time through the blockchain system and the participants will have the freedom to verify data authenticity and ensure that it has not been altered. The technology also provides accountability and sensor data traceability. The key aspect that needs to be emphasized on in IoT is reliability of blockchain.

Autonomy: next-generation application features get additional power from blockchain technology and pave the way for development of smart autonomous assets and hardware as a service. Blockchain makes is possible for devices to interact with one another without any servers getting involved. This function could be advantageous for IoT application to offer them decoupled and device-agnostic applications.

Security: if information and communications are saved up as blockchain transactions, they can be secure. Blockchain can consider device message exchanges as transactions, validated by smart contracts, thereby securing device communications. Blockchain can help to secure the current standard protocols used in IoT.

Market of services: blockchain can help to quickly create an IoT ecosystem of data marketplaces and services, where transactions between peers can be done without any authorities' intervention. Deployment of micro services and doing micro-payments can be done safely in trustless environment. This would greatly lead to better access of IoT data in blockchain and IoT interconnection.

Secure code deployment: blockchain can provide its secure-immutable storage feature to safely and securely push code into devices. Manufacturers can efficiently track updates and states confidently. IoT middlewares can take advantage of this feature to securely update IoT devices. [5]

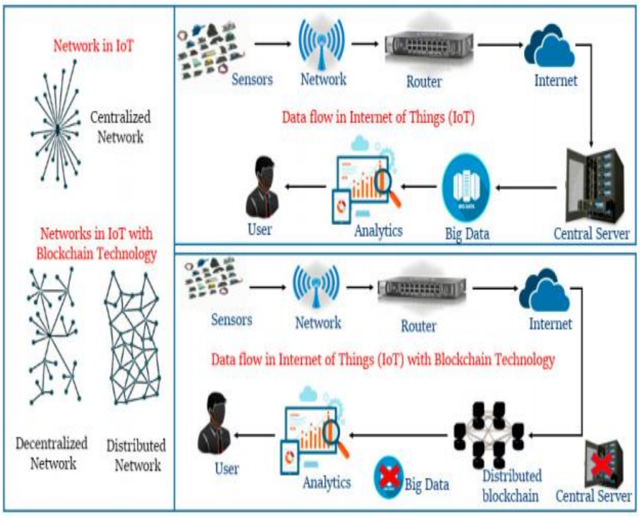

Fig.2. IoT network types, data flow in IoT, data flow in IoT with blockchain technology [4]

IV. KEY CHALLENGES OF BLOCKCHAIN IN IOT:

Despite the multiple benefits outlined above, there are still plenty of challenges and issues that need to be resolved before adapting blockchain technology in IoT. Some of them are as follows:

Time latency: in bitcoin blockchain, 10 minutes are taken up for transaction validation that can create problems for real time applications.

Storage and Computation issues: blockchain needs to be customized before its application can be considered as security solution in IoT since most the devices in IoT have limited storage and computation capabilities. To do away the adaptability issue, one way is to add a new application level that could hide the details of blockchain implementation, known as the PoW (Proof of Work). This solution would allow the IoT devices with limited resources to involve in the system without computing the PoW.

The anonymity: Actually, there are no guarantees that blockchain could offer a fully autonomous transaction. Of course, the peers that have been recognized through their pseudonyms could be tracked but they remain unlinkable (it's impossible to extract a person's identity from its pseudonym).

Consumption of Bandwidth: The generation of transactions is a lot in IoT devices; hence it would impose a major issue if it would be necessary to validate every transaction that consumes a lot of bandwidth.

Scalability issues: even though bitcoin blockchain is wildly popular and number of users keep multiplying every year, but for IoT environments blockchain technology is till date a non-scalable solution. According to CISCO, about 20 billion IoT devices will be connected to the Internet by the year 2020. [6]

V. LITERATURE SURVEY

A. Authorization

Axon, L. [7] demonstrated that a privacy-aware public key infrastructure (PKI) can be constructed by blockchain, at the same time doing away with some of the issues found in conventional PKI. The author carried out studied and suggested a method by which a privacy aware Public Key Infrastructure (**PKI**) can be created on the blockchain as well as unlinkable key updates and the decentralized control of information access- can be offered by this construction to fulfill the needs of varied emerging applications that need a certain level of privacy awareness. Brody. P. [8] devised the ADEPT (Autonomous Decentralized Peer-To-Peer Telemetry) platform that is an initiative for proving the foundational concepts of a decentralized technique, which offers security and more scalability for the IoT. Fromknecht, C. et. al. [9] developed Certcoin that is a substitute public and decentralized authentication technique for maintaining a public ledger of domains with their associated public keys. It has distinct features like transparency, redundancy, and fault tolerance along with providing efficient key retrieval that would make Certcoin a more convenient option for performance sensitive applications. Cha, S. C., et. al. [10] proposed gateway that is connected by blockchain that can adapt and securely maintain the end user's privacy preferences for blockchain networks' IoT devices. In order to securely manage privacy preferences and to authenticate, a fool proof signature mechanism is suggested. The proposed Blockchain Gateway that will be the mediator between IoT devices and the users where the users shall be able to retrieve device information as well as privacy policies of the IoT devices connected to a Blockchain gateway and get access to the gateway instead of getting direct access to the device.

Ghuli, P. et. al. [11] described a distinctive technique to carry out peer to peer identification of ownership of the cloud environment's IoT devices. The mentioned technique will mean adding the device by the manufacturer (known also as Genesis) and then transferring to a user using blockchain technology; also transferring the ownership of devices between users by not involving any third parties can be done. A centralized authority or cloud is no longer needed for registration thereby making interoperability much more suitable. This system shall also be more secure against malicious attacks as they are dependent on good nodes being balanced and working well. Hardjono, T. et. al. [12] introduced the ChainAnchor architecture that offers device commissioning in a privacy-preserving technique. Objective of ChainAnchor is: (1) incentivize service providers and device-owners for sensor-data sharing in a privacy-preserving fashion, (2) support for anonymous device commissioning, (3) support the remuneration to device-owners for selling their device sensor-data to service providers. Hashemi, S. H et. al. [13] described a multiple granularity, multi-level and user-centric technique to share data to and fro between devices and people and organizations. Their mechanism utilizes access lists, capabilities and access rights as per well understood formal notions for reasoning about access. Their work describes a decentralized, transparent, auditable, distributed, publication-subscription based, robust mechanism and automation of these ideas in IoT that is finely matched to the current generation of clouds. And it draws inspiration from tried and tested practices and principles employed in crypto currencies exploiting block chains of transactions and put users as well as organizational entities in charge of control over the access to groups of sensory data. Authors outlined a deployment of these ideas to cover areas of autonomous cars, smart cities and health care. Huh, S. et. al. [14] proposed a mechanism for management of IoT devices through Ethereum, blockchain computing platform. Keys were managed through RSA public key cryptosystems in which private keys are saved on individual devices and public keys were stored in Ethereum. Ethereum's smart contract was utilized to develop their Turing-complete code to function on top of Ethereum. Hence, conveniently managing configuration of IoT devices as well as developing a key management system. Leiding, B. et. al. [15] proposed another approach, the Authcoin to replace the popular public key infrastructures like the PGP web of trust and central authorities. Authcoin intends to perform it in a distributed and decentralized way by utilizing a blockchain based storage system and an improved challenge response-based V&A process for public keys, email accounts as well as certificates. Thus, making Authcoin sturdy against Sybil attacks and with fewer downsides than existing solutions. Ouaddah, A. et. al. [16] proposed a framework called FairAccess that contains a conventional blockchain transaction specification which will contain more fields customized to the needs of a granular access control model. FairAccess will have the blockchain that shall be the database for storing the access control policies for every pair (requester and resource) in the form of transactions; it will also operate as logging database for performing auditing functions. Additionally, it will stop token forgery by transactions integrity checks and will point out token reuse by the double spending detection mechanism.

Shafagh, H. et. al. [17] presented a design for IoT based on blockchain that gives benefits of data management and distributed access control. This system offers compact access control as well as sharing of time series sensor data of different IoT applications. The early evaluation results show promise and a miniscule overhead because of their system. Zyskind, G. et. al. [18] proposed a peer to peer network, Enigma, that would allow various parties to mutually store and run computations on data and at the same time keep the data completely private. The computational model is based on a greatly optimized version of multi-party computation, guaranteed by a verifiable secret-sharing scheme. For storing data especially if it's secretly-shared, an altered distributed hashtable is utilized. An external blockchain will be used as the network controller to manage access control, identities and shall serve as a fool proof untamperable log of events. Wu, L. et. al. [19] proposed a scheme that uses an out-of band two-factor authentication scheme for blockchain based IoT devices. The authors used Eris Blockchain to implement the IoT and Blockchain integrated system and equivalent computing devices to emulate IoT devices. The overheads are measured that are run on Blockchain and smart contract services on the emulator devices. .Haenni, R. [20] developed the Datum network that will permit anyone to save structured data safely in a decentralized manner on a smart contract blockchain. The DAT smart token allows optional selling and purchasing of stored data whilst enforcing data usage rules as specified by the data owner. The DAT token will assist in the compensation of data sources and storage nodes and facilitate a novel era of safe and decentralized storage of data and exchange.

B. Access Control Of Data

Dorri, A. et. al. [21] proved that a Blockchain based smarthome framework is safe and secure by systematically analyzing its security based on the basic security objectives like integrity, confidentiality and availability. Furthermore, they demonstrated simulation results to emphasize that the overheads (as per traffic, energy consumption and processing time) introduced by their approach are irrelevant when considering privacy and security gains. Zhang, Y. et. al. [22] projected a business model for IoT, where they discussed particulars of the IoT E-business model right from the entity, commodity as well as the transaction process along with the four steps of conventional E-business (Pre-transaction preparation, Negotiation, Contract signing and Contract fulfillment) are later on redivided as per the characteristics of the IoT E-business model. For creating a total decentralized IoT E-business model, Blockchain's P2P transaction mode is suggested while another technique designed for transaction of smart property, paid data based on smart contract and encrypted coins proposed. Deters, R. [23] focuses on combination of two methods for supporting multi-tenancy in the IoT edge-computing environments, through pushing of the script engines onto the nodes and permitting third parties to push code onto these nodes, a handy technique to share low energy nodes can be done. For tackling security challenges, access control was performed by deploying blockchain. By treating access tokens like digital assets and exchange them through a blockchain is a practical way to control script distribution onto low energy components.

C. Access Control Of Device

Jentzsch, C. et. al. [24] developed the concept of Ethereum-based Blockchain, smart contracts and Slock.it (*smart lock* (slock)), the physical "Slock" devices. Slock.it can be utilized for renting & selling or peer to peer sharing and for other things that are based on smart contracts as well as commitments, without middlemen or a third party. It is open-source and has framework that is modular and event based. Novo, O. [25] proposed a system that consists of 6 components, i.e. Wireless sensor networks, Managers, Agent node, Smart contract, Blockchain network and Management hubs. This method will be beneficial for access control in IoT like: 1) accessibility, that would make sure the access control rules are obtainable at any time, 2) mobility, that can be used in isolated administrative systems, 3) lightweight, refers to IoT devices not needing any changes for adopting the system, 4) concurrency, that permits the access control policies to be changed concurrently; 5) transparency, in which system could preserve location privacy; 6) scalability, since IoT devices can be joined through diverse constrained networks.

Fan, K. et. al. [26] proposed a secure and proficient technique based on blockchain for a content-centric network, that could ensure user's privacy that is in his data. The authors used a combination of encryption and access control policies to guarantee user's data security. The users who can convince the access strategy are permitted to receive the encrypted data saved in the cloud and users can develop a foolproof access policy control the data better. Miners participation not only makes the scheme efficient but can also resist attacks from adversaries. Lin, C. et. al. [27] presented a blockchain based system for secure mutual authentication, BSeIn that has detailed and minutely worked out access control policies. The proposed system that has features like message authentication code, multi-receivers encryption, integrated attribute signature, is developed to offer security and privacy guarantees like confidentiality, auditability and anonymous authentication. It scales nicely as it utilizes smart contracts. Lunardi, R. C. et. al. [28] proposed an IoT ledger based architecture to guarantee access control on heterogeneous situations. This method is applicable on the usual devices used on IoT networks like Raspberry and Orange Pi boards and Arduino. The proposed architecture could do these: (1) a solution suggested that would utilize an IoT ledger to help with IoT networks' Access management, (2) performance of diverse limited hardware sending encrypted data and updating IoT ledger, evaluated (3) IoT devices would be capable of handling AES and SHA256 algorithms for communicating with IoT Gateways and RSA could be employed for key exchange procedure. Xu, R. et. al. [29] proposed BlendCAC, a decentralized capability based access control framework leveraging the smart contract and blockchain technology, for handling the issues in access control techniques for IoTs. In the physical IoT network environment, a concept-proof prototype was created and the model is transcoded to smart contracts and operates on the private Ethereum BC network. The laptops and desktops work as miners to balance the inviolability of transactions that are recorded on the blockchain, while Raspberry PI devices serve as edge computing nodes to access and to provide IoT-based services. Future work would involve building a fully decentralized security mechanism for IoTs and edge computing and exploring the scheme in real world applications.

Dukkipati, C. et. al. [30] proposed a blockchain based model that is helpful in reducing the issues in privacy and security while offering the following advantages:

- Users can decrease processing speed and time wastage through usage of local databases
- Better user privacy through public and private blockchains
- Blockchain transactions help to find owner of the resource
- Since owner outlines the policy right after resource allocation, the user doesn't have to initiate the transaction for actions defined in the general policy
- Storage of policies through a link makes updations easier and reduces memory usage, also decreases number of transactions.
- Through the blockchain database any user of the network can find out who is presently accessing a resource.
- Resource owner can track the users who are denied or granted access to the resource.
- User-friendly as user can request the actions he needs on the resource.

Hammi, M. T**.** et. al.[31] presented Bubbles of trust, an original approach in which safe virtual zones are developed, where devices can communicate in a totally secure manner. Bubbles of trust approach can be applied to many IoT contexts, scenarios and services. It depends on a public blockchain and benefits from all its security properties.

Özyılmaz, K. R. et. al. [32] described a standardized IoT infrastructure in which data is saved on a DDOS proof, fault tolerant, distributed storage service and data access is looked after by a decentralized, trustless blockchain. The discussed system employed LoRa as the newer network technology, Ethereum as the blockchain platform and Swarm as the distributed data storage. Such type of data backend will make sure there is high availability with fewer security risks while replacing traditional backend systems with a single "smart contract". This is how all types of IoT end devices could be integrated to this infrastructure based on their storage and computing abilities. Such an accomplishment will lead to data- centric business models where application development and data processing can be carried out massively through usage of smart contracts as explained.

Sharma, P. K. et. al. [33] discussed DistBlockNet, a distributed secure SDN architecture for IoT that uses blockchain technique and adheres to the principles needed to design a scalable, secure and efficient network architecture. The essential role of the DistBlockNet model is generation and deployment of protections, that includes data protection, access control, threat prevention and mitigation of network attacks like DDoS/DoS attacks, security threats detection and cache poising/ARP spoofing. This model also concentrates on decreasing the attack window time by permitting IoT forwarding devices to swiftly check and download the newest table of flow rules in required. The model's performance evaluation would be done on factors like defense effects, accuracy rates, scalability and its performance overheads.

Alphand, O. et. al. [34] described an architecture IoTChain which is a combination of ACE authorization framework [42] and OSCAR architecture [43] for providing an E2E solution for the secure authorized access to IoT resources. While OSCAR utilizes the public ledger to arrange multicast groups for authorized clients, the blockchain provides a trustless and flexible way for handling authorization. Authorization blockchain on top of a private Ethereum network was implemented for evaluation of the architecture's feasibility.

Huh J. H. et. al. [37] proposed and implemented a combined automatic log-in platform based on mobile fingerprint recognition based on concept of blockchain. Utilizing a smartphone-based fingerprint recognition function, a useful, integrated automatic log-in platform with powerful security was created. The platform has three main functions: firstly, user authentication in mobile device, PC and IoT environments through fingerprint recognition is possible. Second, the platform consists of SDK for developing application software to authenticate users and provide IoT services. Lastly, its powerful security using the blockchain theory for securing against forging/tampering/leakage of user's fingerprint data by malicious users or hackers.

Bezawada, B. et. al. [38] proposed an ABAC (Attribute-Based Access Control) architecture to address the security challenges that are prevalent in a home IoT environment. The authors highlighted many crucial security challenges in home IoT environments, with the two major issues being plug-and-play nature of the home IoT environment and home user awareness. To deal with these issues, the home IoT environment was modeled within the ABAC framework and enumerated the object, subject as well as the environmental attributes.

Kravitz, D. W. et. al. [39] described concept of Permissioned Blockchains that could prove to be effective in securing and managing the swarms of embedded devices and fulfill the requirements for agility, longevity and incremental adoption. Another main feature is Distributed Identity Management that can provide for robust user and device identity as well as attribute management. It was demonstrated how securing of transactions can be done through permissioned blockchain technology and also how these methods can be useful in improving the user identity robustness to secure against fraud by privately referencing the user's blockchain transactions. Another feature that was explored was the securing of swarms of devices that satisfy regular or ad hoc scheduled tasks, through a privacy-preserving rating system for early detection of anomalous device behavior that warrants potential device revocation.

Zhang, Y. et. al. [40] investigated a crucial access control issue in IoTs and presented a smart contract-based framework, that consists of one judge contract (JC), one register contract (RC) and multiple access control contracts (ACCs) to accomplish distributed and reliable access control for IoT systems. Every ACC offers one access control method for a subject-object pair, and implements both static access right validation based on predefined policies and dynamic access right validation by inspecting the subject's behavior. The JC implements a misbehavior-judging method for facilitating the dynamic validation of the ACCs by receiving misbehavior reports from the ACCs, judging the misbehavior and returning the corresponding penalty. The RC registers the information of the access control and misbehavior-judging methods as well as their smart contracts, and also provides functions (e.g., update, register and delete) to manage these methods.

Ourad, A. Z., et. al. [41] proposed a blockchain based solution for user authentication and secure access to IoT devices and the approach deals with the limitations of the prevailing authentication techniques. It was explained how this BC based solution that uses Ethereum smart contracts can offer fool proof records and decentralization for improving the existing techniques while guaranteeing integrity, accountability and traceability through use of tamper proof logs. Real life scenarios were considered to design and implement the solution using available IoT devices and technologies and the technique resisted crafted attacks that were trying to hijack legitimate sessions and brute force credentials.

FINDINGS AND CONCLUSION

1. Exploring advanced development of the privacy aware PKI framework using blockchain, for satisfying particular cases and make efforts to improve efficiency of the system.
2. Further enhancements in the security and scalability features offered by ADEPT (Autonomous Decentralized Peer-To-Peer Telemetry).
3. Finding advanced optimizations to calculate results empirically and reveal the viability of Certcoin.
4. Advanced features for the proposed Blockchain Gateway that can be a mediator between all types on IoT devices.
5. Add further features to the unique technique for peer to peer identification using Genesis.
6. In the ChainAnchor architecture, create industry wide permissioned BC for cost effective IoT devices that preserve privacy of device owners and are more scalable than PKI-based services.
7. The mechanism discussed by Hashemi, S.H. et. al. [13] to work on their scalability and deploy them in more areas.
8. Develop a completely scalable IoT system containing multiple devices, with improvements for convenience of technology users that would be efficient and fast and which would remove hurdles about synchronization and denial of service attacks, as proposed by Huh, S. et. al. mechanism. [14].
9. Include implementation and testing Authcoin in real life scenario, and leveraging concepts of V&A process. Improvements in security can be done, like for biometric identifiers, fingerprinting, voice samples, retina or iris information. Additionally, trust metrics on top of it using data records that make up blockchain can be used to offer estimation of a keys reliability.
10. Improvements in FairAccess to handle all types of token forgery through transactions integrity checks.
11. Finalizing a total reference implementation of the system and creating many IoT applications on top of it as presented by Shafagh, H. et. al.
12. Adding Fees and security deposits that could incentivize the operating accuracy and fairness of system in the peer to peer network, Enigma.

13. Working to perfect Secondary Authentication of the scheme using Eris Blockchain as it can prevent access of external malicious devices, for instance if the attacker steals access tokens.
14. Improvements and security features in the Blockchain based smarthome framework as well as IoT E-business model and Slock.it.
15. Enhancing Espruino platform's reconfigurability for instance control the API that a given JS program could execute.
16. Explore the optimizing of performance of the BSeIn system using hardware implementation, and collaboration with small factory operator for implementing and evaluating the prototype (possibly a hybrid software and hardware based prototype) in a real-world setting.
17. Improve the IoT Ledger in the following ways: (1) discussing how data from devices could be saved on clouds to decrease overhead on limited gateways (2) improvement of solutions for supporting different blockchain implementations like HyperLedger, (3) evaluating different consensus algorithms for appending new blocks from devices onto the IoT ledger taking into view a scenario on bigger scale.
18. Considering the smart surveillance system as a case study, the BlendCAC could be extended to secure network cameras and motion sensors in the urban surveillance platform.
19. The model proposed by Dukkipati, C. et. al. [30] could be made more accurate and simpler to use to avoid failures. The aim would be to utilize machine learning concepts that make the model more accurate and reliable. Deployment of the model into the hardware that replicates the case study that was considered in validation of their study.
20. Bubbles of trust could focus on these: (1) implement a revocation mechanism for compromised devices, (2) evolve the system to facilitate controlled communication between a selected set of bubbles, (3) study and design a protocol that would target the optimization of the miner's number in a defined system and how the selected miners could be placed.
21. Develop features in the system that employs LoRa as the newer network technology, Ethereum as the blockchain platform and Swarm as the distributed data storage.
22. Future of DiskBlockNet model would focus on extension of this research work to create a cloud computing architecture with secure fog nodes at the edge of IoT network.
23. Future of IoTChain would be in implementation of different applications on top of it, to measure its performance and sturdiness. Also updation of the private Ethereum blockchain network so that the PoS based version of the ledger could be used, when it is released by Ethereum developers.
24. Further work for the mobile fingerprint recognition automatic login platform, would be improving the proposed system's security levels that will be considered by divulging the source codes off-line and online as an open source through the author's work.
25. Future scope for the ABAC (Attribute-Based Access Control) architecture system would be the exploration of multiple considerable challenges that might still be prevalent in the home IoT environment domain.
26. Permissioned Blockchain Technology could be made to include more swarms of devices with its enviable features of longevity, agility and incremental adoption as well as improve Distributed Identity Management feature.
27. Perform more case studies to confirm the feasibility in achieving distributed and reliable access control for the IoT in the smart contract-based framework devised by Zhang, Y. et. al. [40]
28. Future work would involve extension with a huge access and authentication to cover a large number of IoT devices and end users. The technique proposed by Ourad, A. Z., et. al. [41] has to be tested on an actual Ethereum blockchain network and evaluation of performance is to be done on the basis of cost (or gas) usage and scalability. Monetization aspects could also be considered related to IoT devices and their data, whereby usage is paid by crypto-token of ether.

REFERENCES

1. Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview understanding the issues and challenges of a more connected world. *The Internet Society (ISOC)*, *22*.
2. Kouzinopoulos, C. S., Spathoulas, G., Giannoutakis, K. M., Votis, K., Pandey, P., Tzovaras, D., ... & Nijdam, N. A. (2018, February). Using blockchains to strengthen the security of internet of things. In *International ISCIS Security Workshop*(pp. 90-100). Springer, Cham.
3. Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Internet of Things: state-of-the-art, challenges, applications, and open issues. *Int. J. Intell. Comput. Res.*, *9*(3), 928-938.
4. Kumar, N. M., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. *Procedia Computer Science*, *132*, 1815-1823.
5. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173-190.
6. Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*, 199-221.
7. Axon, L. Privacy-Awareness in Blockchain-Based PKI. Available online: https://ora.ox.ac.uk/objects/uuid:f8377b69-599b-4cae-8df0-f0cded53e63b (Accessed 19 June 2019).
8. Brody, P. IBM ADEPT Practitioner Perspective. Available online: http://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/55f73e5ee4b09b2bff5b2eca/55f73e72e4b09b2bff5b3267/1442266738638/IBM-ADEPT-Practictioner-Perspective-Pre-Publication-Draft-7-Jan-2015.pdf%3Fformat%3Doriginal (Accessed 19 June 2019)
9. Fromknecht, C., Velicanu, D., & Yakoubov, S. (2014). Certcoin: A namecoin based decentralized authentication system 6.857 class project. *Unpublished class project*. Available online: https://www.semanticscholar.org/paper/CertCoin-%3A-A-NameCoin-Based-Decentralized-System-6-Fromknecht-Velicanu/72889440eaeb7a1a17a8be830feff236b5a62b67 (Accessed 19 June 2019)
10. Cha, S. C., Chen, J. F., Su, C., & Yeh, K. H. (2018). A blockchain connected gateway for BLE-based devices in the internet of things. *IEEE Access*, *6*, 24639-24649.

11. Ghuli, P., Kumar, U. P., & Shettar, R. (2017). A review on blockchain application for decentralized decision of ownership of IoT devices. *Adv. Comput. Sci. Technol*, *10*, 2449-2456.
12. Hardjono, T., & Smith, N. (2016, May). Cloud-based commissioning of constrained devices using permissioned blockchains. In *Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security* (pp. 29-36). ACM.
13. Hashemi, S. H., Faghri, F., Rausch, P., & Campbell, R. H. (2016, April). World of empowered IoT users. In *2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)* (pp. 13-24). IEEE.
14. Huh, S., Cho, S., & Kim, S. (2017, February). Managing IoT devices using blockchain platform. In *2017 19th international conference on advanced communication technology (ICACT)*(pp. 464-467). IEEE.
15. Leiding, B., Cap, C. H., Mundt, T., & Rashidibajgan, S. (2016). Authcoin: validation and authentication in decentralized networks. *arXiv preprint arXiv:1609.04955*.
16. Ouaddah, A.; Elkalam, A.A.; Ouahman, A.A. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In Europe and MENA Cooperation Advances in Information and Communication Technologies; lvaro Rocha, Á., Serrhini, M., Felgueiras, C., Eds.; Springer: Cham, Germany, 2016; pp. 523–533.
17. Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017, November). Towards blockchain-based auditable storage and sharing of iot data. In *Proceedings of the 2017 on Cloud Computing Security Workshop* (pp. 45-50). ACM.
18. Zyskind, G.; Nathan, O.; Pentland, A. Enigma: Decentralized Computation Platform with Guaranteed Privacy. arXiv **2015**, arXiv:1506.03471.
19. Wu, L., Du, X., Wang, W., & Lin, B. (2018, March). An out-of-band authentication scheme for internet of things using blockchain technology. In *2018 International Conference on Computing, Networking and Communications (ICNC)* (pp. 769-773). IEEE.
20. Haenni, R. Datum Network: The Decentralized Data Marketplace. Available online: https://datum.org/ (Accessed 16 June 2019)
21. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops) (pp. 618-623). IEEE.
22. Zhang, Y., & Wen, J. (2015, February). An IoT electric business model based on the protocol of bitcoin. In 2015 18th International Conference on Intelligence in Next Generation Networks (pp. 184-191). IEEE.
23. Deters, R. Decentralized Access Control with Distributed Ledgers. Available online: www.cloudrobotics.info/files/papers/ICCR17_paper_6.pdf (Accessed 16 June 2019)
24. Jentzsch, C.; Jentzsch, S.; Tual, S. Slock.IT. Available online: https://slock.it (Accessed 16 June 2019).
25. Novo, O. (2018). Scalable Access Management in IoT using Blockchain: a Performance Evaluation. IEEE Internet of Things Journal.
26. Fan, K., Ren, Y., Wang, Y., Li, H., & Yang, Y. (2017). Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G. IET Communications, 12(5), 527-532.
27. Lin, C., He, D., Huang, X., Choo, K. K. R., & Vasilakos, A. V. (2018). BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. Journal of Network and Computer Applications, 116, 42-52.
28. Lunardi, R. C., Michelin, R. A., Neu, C. V., & Zorzo, A. F. (2018, April). Distributed access control on iot ledger-based architecture. In NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium (pp. 1-7). IEEE.
29. Xu, R., Chen, Y., Blasch, E., & Chen, G. (2018). Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the iot. *Computers*, *7*(3), 39.
30. Dukkipati, C., Zhang, Y., & Cheng, L. C. (2018, March). Decentralized, blockchain based access control framework for the heterogeneous internet of things. In *Proceedings of the Third ACM Workshop on Attribute-Based Access Control* (pp. 61-69). ACM.
31. Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security*, *78*, 126-142.
32. Özyılmaz, K. R., & Yurdakul, A. (2018). Designing a blockchain-based IoT infrastructure with Ethereum, Swarm and LoRa. *arXiv preprint arXiv:1809.07655*.
33. Sharma, P. K., Singh, S., Jeong, Y. S., & Park, J. H. (2017). Distblocknet: A distributed blockchains-based secure sdn architecture for iot networks. *IEEE Communications Magazine*, *55*(9), 78-85.
34. Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., ... & Zanichelli, F. (2018, April). IoTChain: A blockchain security architecture for the Internet of Things. In *2018 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1-6). IEEE.
35. M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, R. Guizzetti, "OSCAR: Object Security Architecture for the Internet of Things", *Ad Hoc Networks*, vol. 32, pp. 3-16, 2015.
36. L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, H. Tschofenig, "Authentication and Authorization for Constrained Environments (ACE)", *Internet Engineering Task Force Internet-Draft draft-ietf-ace-oauth-authz-07*, Aug. 2017, [online] Available: https://datatracker.ietf.org/doc/html/draft-ietf-ace-oauth-authz-07.
37. Huh, J. H., & Seo, K. (2019). Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing. *The Journal of Supercomputing*, *75*(6), 3123-3139.
38. Bezawada, B., Haefner, K., & Ray, I. (2018, March). Securing Home IoT Environments with Attribute-Based Access Control. In *Proceedings of the Third ACM Workshop on Attribute-Based Access Control* (pp. 43-53). ACM.
39. Kravitz, D. W., & Cooper, J. (2017, June). Securing user identity and transactions symbiotically: IoT meets blockchain. In *2017 Global Internet of Things Summit (GIoTS)* (pp. 1-6). IEEE.
40. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the internet of things. *IEEE Internet of Things Journal*.
41. Ourad, A. Z., Belgacem, B., & Salah, K. (2018, June). Using Blockchain for IOT Access Control and Authentication Management. In *International Conference on Internet of Things* (pp. 150-164). Springer, Cham.
42. L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, H. Tschofenig, "Authentication and Authorization for Constrained Environments (ACE)", *Internet Engineering Task Force Internet-Draft draft-ietf-ace-oauth-authz-07*, Aug. 2017, [online] Available: https://datatracker.ietf.org/doc/html/draft-ietf-ace-oauth-authz-07.
43. M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, R. Guizzetti, "OSCAR: Object Security Architecture for the Internet of Things", *Ad Hoc Networks*, vol. 32, pp. 3-16, 2015.

AUTHORS PROFILE

Asra Kalim Lecturer & Website Content Manager at Jazan University, Saudi Arabia and is pursuing PhD from Banasthali Vidyapith. She completed her Masters in Computer Application. She has published 6 research papers, 3 books and 1 book chapter. Major research areas are Web App Security, Block-chain, IoT and Cloud Computing.

Dr. Deepak Singh Tomar Associate Professor in CSE Department, MANIT, Bhopal (MP), India has completed PhD in Computer Science and Engg., and M.Tech & B.E. in Computer Technology. He has more than 25 years of teaching and administrative experience. Major research areas are Data Mining, Internet Technology, Computer & Network Security, Digital Forensics, Machine Learning on which he has published more than 77 research papers with 04 book chapters.

Dr. Sheikh Ikhlaq, Cloud Consultant at Accenture, New Delhi, completed his PhD from Suresh Gyan Vihar University. Major research areas are Big Data, Machine Learning, Data Warehousing, Data Mining, Software Engineering. He has published 4 journal papers in peer-reviewed Scopus indexed journals of repute and 2 papers in Tier-II conference. He has published 2 patents, in US and India.