IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol-6, Special Issue-3, Apr 2018 E-ISSN: 2347-2693

On IoT Security Models:Traditional and Blockchain

Shahid Ul Haq[1*], Yashwant Singh[2]

[1*]Department of Computer Science and Information Technology, Central University of Jammu, Jammu & Kashmir, India
[2] Department of Computer Science and Information Technology, Central University of Jammu, Jammu & Kashmir, India

[*]*Corresponding Author: shahidulhaq.lone @gmail.com, Tel.: +91 9419013103*

Available online at: www.ijcseonline.org

***Abstract*—** Security and privacy is a much-needed aspect of the connected world. If these functionalities are not deployed properly then every economic or societal institution dependent on them are vulnerable to get crashed and might even cause a damage of catastrophic scale. People would eventually stop trusting these technological platforms that are supposed to make their lives better. Although security is a paramount functionality in any connected infrastructure, there is no silver bullet to it, there has been extensive research in this field but no one has come up with an idea that can secure the distributed and heterogeneous IoT network efficiently. IoT demands an autonomous access control methodology requiring minimal or no user interaction. There are several existing models that are good and effective however they have several implementation issues. In this paper we have described our survey of the existing security models of IoT and presented a brief comparative analysis of the discussed models also some of the main requirements for designing such models is given.

***Keywords*—**IoT, Security, blockchain, access-control, models

I. INTRODUCTION

Internet of Things represents a hyper connected world in which the Internet extends to everyday physical objects that can be remotely controlled. These objects act as sensors, detectors and actuators, the data from these things can be analyzed through IoT platforms to provide services and carry out appropriate decisions.

IoT is primarily the evolution of wireless sensor networks (WSN). WSN has various applications like environment monitoring, health monitoring, weather monitoring, pollution checking and various applications in defense and security. These networks were deployed having communication technology and network architectures specific to the application. Internet expanded the domain of WSN's; it brought all the disconnected networks of specific applications and all other devices capable of connecting to Internet under a common canopy, which is termed as Internet of things.

IoT networks are used for building smart environments like automating home, automatic traffic control systems and smart organizations. IoT is mainly used for inducing context awareness in devices so that various benefits are taken from them such as reducing energy consumption in homes, monitoring air pollution, intelligent traffic management and improving business processes.

IoT faces a seemingly intractable problem of device access control and data privacy. It was estimated that 8.4 billion devices will be connected in 2017 and will reach to 20.4 billion by 2020, insights by Gartner Inc.[1] as IoT connected devices are increasing exponentially so is increasing the complexity of managing them. These devices, which build up IOT, are highly vulnerable to attacks in-fact the devices are easy targets for attackers who use them for creating large-scale botnets to carry out DDoS attacks. Making such an infrastructure secure is a major challenge engineers are facing today. A main demonstration of security's importance is the major distributed denial of service (DDoS) attack in October 2016 that was carried out with numerous IoT devices infected by Mirai,[2] a simple malware program. Nowadays computing devices are also hijacked for mining crypto currencies [3], which present far greater threat to tackle. There are several centralized approaches to this problem but those are not scalable enough, also a trusted centralized authority presents a problem of data privacy and single point of failure. In order to maintain such a huge device base decentralized approaches have to be considered and now with the advent of Blockchain Technology IoT security can be perceived through new dimensions. Below are some of the reasons that make it difficult to deploy an efficient solution for securing IoT network. [4]

- IoT systems don't have well defined perimeters due to device mobility.

- IoT systems are highly heterogeneous systems in terms of communication media, protocols, platforms and devices.
- Some IoT networks can be physically unprotected and or controlled by other third parties or devices.
- No Universal network architecture and lack of fine-grained access control permissions.
- Some IoT devices have computational and energy constraints due to which cryptographic computations are not feasible to carry out on device.

In Recent years, a new technology has emerged which is termed as Blockchain Technology [5][6], that allows users to transfer values known as crypto currencies, securely without any trusted central authority, using a distributed ledger (or Blockchain) which is verifiable by public nodes participating in the network. There have been several demonstrations of how Blockchain technology can be put to other functions that require trusted and auditable computing [7]. One of the functions, which researchers are working on, is how security and privacy can be achieved using Blockchain technology in the domain of Internet of Things [8].
Remaining part of this paper is organized as follows: section II discusses the existing traditional security models of IoT; section III discusses the Blockchain based models; the requirements for designing the models is discussed in section IV, in section V comparative analysis is discussed and section VI concludes the work.

II. TRADITIONAL SECURITY MODELS

A. *Role Based Access control(RBAC) model*

This model is given by Zhang [9], in this model, there is a security administrator who assigns the appropriate permissions for the role according to the characteristics and context of physical objects and the contextual information is provided using web-services. The model is explained using a housekeeping example shown in fig. 1 below:

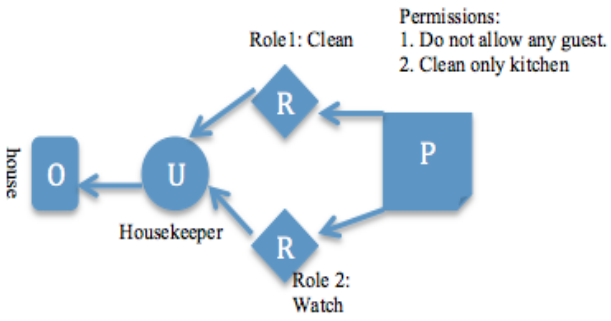

Figure. 1. Role based approach example.

In this example housekeeper is the user (U), house is the object (O), and housekeeper has two roles assigned: cleaning (R1) and watching the house (R2), both the roles have appropriate access permissions (P). This explains the role-based approach. Although this model achieved a very good context based access control management but its feasibility is not demonstrated in constrained devices.

B. *Distributed Capability based access control model (DCapBAC)*

This model is given by Hernandez-Ramos [10], in this model a device or an entity receives a capability token that defines its role and access privileges, the capability token uses JSON (JavaScript object notation) format for data representation, when this device wants to access another device it presents its capability token to the requested device, the requested device checks the capability token and offers a service to the token after proper verification. The figure 2 below shows a CapBAC in which the authorization decision is carried out by a central entity PDP (policy decision point), the distributed version of CapBAC implements the PDP directly in IoT device so that the device itself carries out the decision of authorization based on its contextual information.

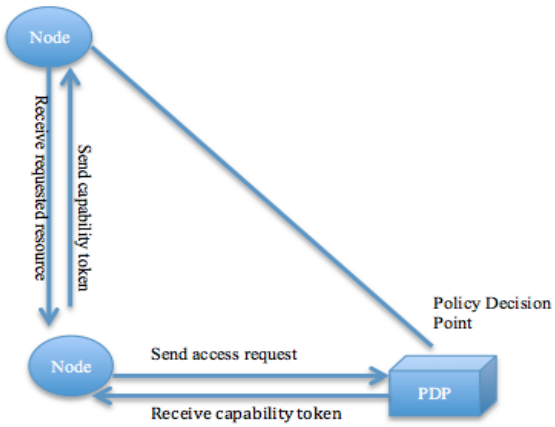

Figure. 2. Distributed capability based example [10].

C. *Usage Control model (UCON)*

This model is given by Ravi Sandhu and Jaehong Park [11], UCON model as shown in fig. 3, is built around three decision factors which are, A-authorizations, B-obligations and C- conditions and two decision properties which are mutability and continuity. Authorization is based on attributes assigned to subject and object. Obligations are some requirements that have to be fulfilled by the subject in order to gain access. Conditions are system and environment factors, which are independent of the subject and object that needs to be satisfied for device access. UCON treats obligations and conditions as the crucial decision factors. The mutability property of ABC model allows change of

attributes as a consequence of access and the Continuity property of UCON allows the access to be checked at regular intervals, which means that the decision to allow access to a device is not a one-time decision, but the decision also is carried out at regular intervals during device access.

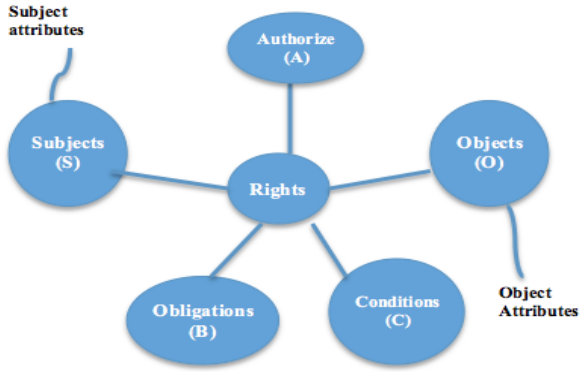

Figure. 3. Usage Control model components [11].

D. Attribute-Based Access control model

This approach of access control is given by Vincent C. et al. [12], it is a flexible approach that can implement access policies based on attributes, it enables the large number of subjects to access the large number of objects without specifying any individual relations between them, making it a very good model for distributed and rapidly changing environments. ABAC is a type of access control model that manages access to entities by formulating rules against the attributes of subject and object, type of operations, and the environmental conditions relevant to a request. ABAC implementation in a distributed environment becomes very complex to manage, as it requires attribute management infrastructure, machine enforceable policy manager and various functions to support the ABAC implementation. However it has drawn attention from corporate and government organization including NIST (national institute of standards and technology), which issued a special publication regarding the concepts of this model.

E. OSCAR: Object security architecture for the IoT

This model[13] of IoT security follows REST (Representational state transfer) architecture that serves application level end-to-end security. Its prime concern revolves around the security considerations of constrained devices in IoT. Constrained nodes or CoAP (constrained application protocol) nodes have computational and memory limitations, which make it difficult to deploy secure access control solutions among these devices. OSCAR presents a solution to this problem by giving a model that suggests outsourcing the access control requirements to authorization servers. In this model devices are categorized into four classes: producers, consumers, authorization servers and proxy servers. Producers are devices that generate data such as sensors, monitors, and motion detectors while as Consumers are devices, which consume data such as actuators, storage devices, and humans. Authorization servers are used to manage access secrets between communicating devices (producers and consumers). Authorization servers distribute access secrets between parties who are interested in communication through a secure DTLS (datagram transport level security) protocol, which creates a secure channel for communication between two devices. At first all CoAP nodes register themselves with authorization servers by publishing their certificates and when a client needs to request any resource from a CoAP node, the client contacts authorization server and gets access secret from which an encryption key is derived that is used for secure communication between nodes. Proxy servers have also been used for caching purposes. The main focus of this model is to reduce computation overhead and energy utilization in constrained nodes while providing a scalable solution for secure device communication.

III. BLOCKCHAIN BASED MODELS

A. Blockchain for IoT security- Smart Home case study

This model is given by Ali Dorri et al [14] and is based on Blockchain Technology. In this model the authors have used smart home, overlay network and cloud storage as the three architectural components. The smart home consists of all the smart devices in the home and the service provider. The devices in smart home are managed in the form of clusters and each cluster has a cluster head (CH). The cluster head is connected to a local miner that manages all the incoming and outgoing requests in a smart home using a local Blockchain. It does authentication, authorization and audit of transactions. It also performs the function of key distribution and updation. Due to its better processing capabilities it appends the recorded transactions to the Blockchain (BC) in the form of a block. The Blockchain is used to enforce access control policies among the devices. Every block in the Blockchain has a block header and policy header, the block header contains hash of previous block, while the policy header contains access control parameters and transactions. Overlays are used to connect multiple smart homes with each other this is the part of architecture, which makes the whole network decentralized. Cloud storage is used to store the device data securely in the cloud that is generated by the smart devices and sensors. The overview of the architecture is shown in fig. 4 below.

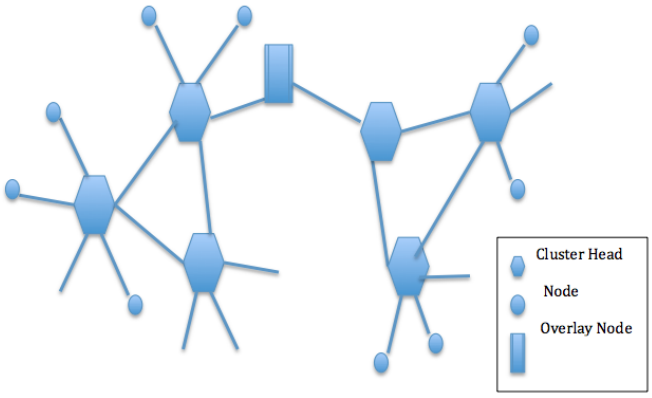

Figure. 4. Blockchain for IoT security Smart Home case [14].

B. *FairAccess: Access-control model based on Blockchain Technology.*

This Blockchain based access control model is given by Ouaddah et al. [15], In this model the access control logic is carried out using tokens replacing the bitcoin. A token represents the access rights defined by its creator for the requestor. The Blockchain stores all the access control policies in the form of transactions for each device pair. FairAccess framework is based on five basic access control functions that are, Register device, GrantAccess, GetAccess, DelegateAccess and RevokeAccess. When a device A wants to access any service hosted by device B, the device A sends a request to device B owner (RO), the device B owner then encapsulates its access rights for device A in the form of a GrantAccess transaction and then the RO broadcasts the transaction to all the nodes, the nodes verify the transaction and in case of successful validation the transaction is added to the Blockchain. When the transaction is added to the Blockchain a token TXN appears in the requester's wallet. In the next phase the device A will generate a GetAccess transaction, this transaction utilizes the token that was previously added in its wallet, this transaction is also broadcasted to all the nodes in the network and after the verification is successful it is added to the Blockchain. The device B then checks if the transaction redeeming the token is added in the Blockchain, if yes then device B allows allows access to device A. If device B wants to Revoke the access rights for device A it creates a new GrantAccess transaction with new access policies overwriting the previous one. Device A can also delegate access rights or some of the access rights which have been provided by device B to any other device C through a Delegate Access transaction type.

C. *Blockchain Based Multi-Layer Network Model*

The authors of paper[16] proposed a model for IoT security that has a multilayer type of architecture. In this model as shown in fig. 5, IoT is composed of two types of layers, which are: Edge layers and High-level layers. Edge layers connect all the objects to a central cloud server. In order to reduce bandwidth throttling and maintain high communication efficiency only limited number of devices is allowed per edge layer. Different edge layers connect together forming a high-level layer. An edge layer acts as a node to high level-layer. High-level layers are decentralized in nature that implements Blockchain technology for maintaining contract records between devices. Several high level layers can connect together forming a super high-level layer. High-level layers are only used for authentication and authorization purposes for devices present in edge layers. Authentication is realized through smart contracts and privacy is also implemented by using pseudonym for objects. This model proposes to use Byzantine Fault Tolerance (BFT)[17] algorithm for distributed consensus.

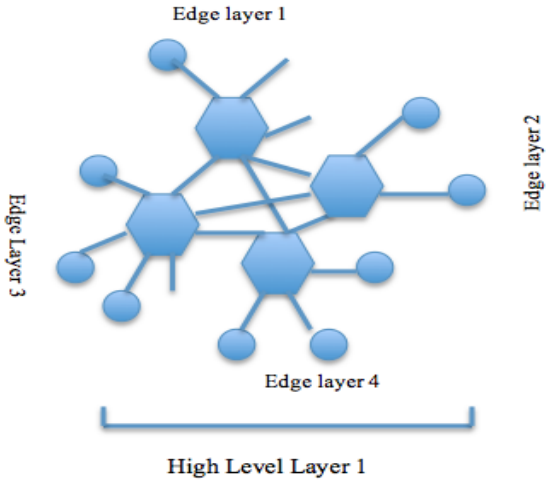

Figure. 5. Multi-layer network model [16].

IV. DESIGN REQUIREMENTS

After thorough review of the IoT models, below are some of the requirements that needs to be considered while designing a model.

- *Architecture*: Access control model for IoT needs to have decentralized or distributed architecture. Centralized approaches have problems of single point failure as well as data privacy issues.
- *Energy Consumption*: Low power devices needs to be taken in consideration while proposing a model for IoT security because sensors are mainly battery operated and lack direct electric supply.
- *Computational power*: IoT devices usually have low computational power, so cryptographic functions are difficult to carry out on these devices.

- *Scalability*: IoT model should be highly scalable to manage a huge device base.
- *Security*: The model must be secure enough to thwart attacks like DDos and Replay attacks.
- *Privacy*: Device and data privacy are important requirements for the model. Anonymization techniques should be implemented to impart this functionality.
- *Deployment*: Model should be easily deployable requiring minimum cost. It should be mostly autonomous requiring minimal user interaction.
- *Performance*: Access control should work in real time, requiring less energy, computations and should generate less network traffic.

V. COMPARATIVE ANALYSIS

The comparative analysis of the discussed models based on some of the important parameters is described in a table 1. The parameters in the table are defined on the scale of 1-10 while Low being (1-3), Medium (4-6) and High (7-10). The analysis is carried out after a thorough study of the models. It is found that traditional centralized model such as RBAC, UCON or ABAC does not scale up when deployed in a larger context such as smart cities. Centralized models also suffer from communication bottleneck because all the device requests have to go through a limited bandwidth channel connected to a central entity. Device and data privacy is not maintained in centralized models which leaves a scope for eavesdropping. Blockchain technology offers a better way to decentralize access control functions in IoT but may impart some delay because adding a block in a Blockchain is a computationally intensive task. Blockchain models are highly scalable and are secure from the replay and DDoS attacks. Privacy is also implemented in Blockchain by using Pseudonymous identities. We argue in favor of Blockchain-based models because it offers a balanced approach to IoT security.

Table 1. Comparative Analysis of Existing Models

S. No.	Model	Architecture Type	Computational Requirement	Energy Requirement	Target Node	Achieved Functionalities	Attack Prevention	Scalability
1	RBAC[9]	Centralized	Low	Medium	IP-based	Authentication, Authorization	N/A	Low
2	DCapBAC[10]	Distributed	High	High	IP-based	Authentication, Authorization	N/A	High
3	UCON[11]	Centralized	Medium	Medium	All	Authentication, Authorization	N/A	Low
4	ABAC[12]	Centralized	Medium	Medium	All	Authentication, Authorization	N/A	Low
5	OSCAR[13]	Centralized	Low	Low	CoAP	Authentication, Authorization	Replay, DDoS	Low
6	Blockchain Based: SmartHome Model [14]	De-Centralized	Low	Medium	All	Authentication, Authorization, Audit	N/A	High
7	Blockchain Based: FairAccess[15]	Centralized	High	High	All	Authentication, Authorization	Replay, DDoS	Medium
8	Blockchain based: Multi-layer Network Model[16]	Multi-layer, Decentralized	Medium	Medium	All	Authentication, Authorization, Device Privacy	Tempering	High

VI. CONCLUSION

In this paper we have reviewed some of the security models of IoT and presented a brief comparison among them. Blockchain technology presents a scope for a decentralized approach of IoT security mainly due to its distributed consensus property. Our aim of research was mainly to cover security aspect of IoT and we will further continue to understand how Blockchain can be effectively implemented for IoT security and a new model will be proposed based on this technology while keeping in view of all the requirements described in section IV.

REFERENCES

[1] I. Gartner, "Gartner Analysis." [Online]. Available: https://www.gartner.com/newsroom/id/3598917. [Accessed: 06-Feb-2018].

[2] J. A. Jerkins, "Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code," *2017 IEEE 7th Annu. Comput.*

Commun. Work. Conf. CCWC 2017, 2017.

[3] "Hijacking Computers to Mine Cryptocurrency Is All the Rage - MIT Technology Review." [Online]. Available: https://www.technologyreview.com/s/609031/hijacking-computers-to-mine-cryptocurrency-is-all-the-rage/. [Accessed: 06-Feb-2018].

[4] E. Bertino, "Botnets and Internet."

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Www.Bitcoin.Org*, p. 9, 2008.

[6] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, pp. 557–564, 2017.

[7] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an Optimized BlockChain for IoT," in *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation - IoTDI '17*, 2017, pp. 173–178.

[8] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?," *IT Prof.*, vol. 19, no. 4, pp. 68–72, 2017.

[9] G. Zhang, "An extended role based access control model for the Internet of Things," *2010 Int. Conf. Information, Netw. Autom.*, pp. V1-319-V1-323, 2010.

[10] J. L. Hernández-Ramos, A. J. Jara, L. Marín, and A. F. Skarmeta Gómez, "DCapBAC: embedding authorization logic into smart things through ECC optimizations," *Int. J. Comput. Math.*, vol. 93, no. 2, pp. 345–366, 2016.

[11] P. J. Sandhu R., "Usage Control: A Vision for Next Generation Access Control," *Comput. Netw. Secur.*, vol. 1, pp. 42–56, 2003.

[12] V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, "Attribute-based access control," *Computer (Long. Beach. Calif).*, vol. 48, no. 2, pp. 85–88, 2015.

[13] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "OSCAR: Object security architecture for the Internet of Things," *Ad Hoc Networks*, vol. 32, no. January, pp. 3–16, 2015.

[14] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. (PerCom Work.*, pp. 618–623, 2017.

[15] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," in *Advances in Intelligent Systems and Computing*, 2017, vol. 520, pp. 523–533.

[16] C. Li and L. J. Zhang, "A blockchain based new secure multi-layer network model for internet of things," *Proc. - 2017 IEEE 2nd Int. Congr. Internet Things, ICIOT 2017*, pp. 33–41, 2017.

[17] M. Castro, M. Castro, B. Liskov, and B. Liskov, "Practical Byzantine fault tolerance," *OSDI {'}99 Proc. third Symp. Oper. Syst. Des. Implement.*, no. February, pp. 173–186, 1999.

Authors Profile

Mr. S Haq pursed Bachelor of Technology from Graphic Era University, India in 2015 and is currently pursuing Master of Technology from Central University of Jammu. His main research work focuses on IoT, Network Security, Blockchain Technology, Cryptography and Automation.

Dr Y Singh pursed Bachelor of Engineering from Sant Longowal Instituite of Engineering and Technology and Master of Engineering from Punjab Engineering College, India. He pursued Ph.D. from Himachal Pradesh University and is currently working as Associate Professor in Department of Computer Science and Information Technology, Central University of Jammu, India. He is a member of IEEE ,CSI, ACM and a life member of the ISTE. His main research work focuses on Wireless sensor networks, Routing, Communication, Event Detection, Security and Privacy, Software Engineering and Software Architecture.

