International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 07 | July 2019 www.irjet.net p-ISSN: 2395-0072

An Approach to Authenticating Devise in IoT using Blockchain

Jayant Dilip Dabhade[1], Dr. Deepak Singh Tomar[2]

[1]Mtech Scholar, Maulana Azad National Institute of Technology, Bhopal
[2]Associate Professor, CSE Dept Maulana Azad National Institute of Technology, Bhopal

---

Abstract - *The Internet of things is a technology having extensive scope and can become a major part of our daily lives the future. In the recent years, the growth in the field of IoT and its applications have been relentless. Although it is still in its infancy, it has gained a massive interest of even the big players like IBM and Amazon. Different items that are used every moment are fitted with electronic devices and protocols to bind them to the Internet. Nonetheless, the IoT has a few major security issues that need to be addressed to ensure its steady and bright future. In IoT, as things process and exchange information without human interference, human participation is minimal. This complete autonomy obviously makes the malicious developers target these organizations evidently. It brings a drastic need to acknowledge and authenticate the entities and guarantee the integrity of their information exchanged. Because of IoT's comprehensive scope and other characteristics, creating an efficient centralized encryption scheme is almost unlikely. Now, another promising technology that might just resolve the security problems in IoT is Blockchain. In this approach, an initial decentralized system is suggested to resolve this restriction, which guarantees solid device identification and authentication. It also preserves the integrity and accessibility of information. This strategy is based on the safety elements granted by the blockchains in order to achieve such a objective and helps to generate safe virtual areas where items can define and trust each other. Major security issues that have been encountered in the IoT have been addressed and resolved using Blockchain.*

1. Introduction

The Internet of Things (IoT) is advancing rapidly in the research areas and in the industrial fields. Nonetheless, it still must deal with security and privacy issues as it is highly vulnerable. Existing privacy and security approaches are mostly proven to be unsuitable for IoT, primarily because of its decentralized ecosystem and the lack of resources to its devices. Blockchain have recently been used to ensure privacy and security in peer-to-peer networks with similar structure to IoT [1].

Blockchain involve high bandwidth delays and overhead and are computationally expensive, which seems unsuitable for IoT devices. This paper proposes a novel secure and private framework for IoT, based on Blockchain technology that enables most of its security and privacy benefits.

The ideology in IoT and its multiple applications is its ubiquity of a diversity of things where they can cooperate and interact, in order to enable a wide range of services. However, safety problems remain a significant barrier to IoT's vast ranging adaptation in different fields. It is therefore immensely prominent that only the authenticated users are enabled to make use of the system, otherwise the system will be vulnerable to security issues like information theft, identity usurpation and data altercation. The attackers can easily target IoT systems primarily for two reasons

Majority of the interactions and communications are wireless making them more prone to various attacks such as identity spoofing, message tampering and message eavesdropping.

Most of the devices involved in the system have limited resources in terms of energy, processing capacity and memory because of which advanced security solutions are less likely to be applied [2].

Authentication, confidentiality and information data integrity are critical to ensuring the proper running of each portion of such ecosystems. Because of the resource constraints and the heterogeneous nature of IoT, existing safety alternatives are not fully taken into account. In order to cope up, a mixtureof multiple security solutions is needed which may lead to extra high costs. Furthermore, efficient security solutions like the Public key infrastructure (PKI) are centralized limiting the scalability of the system. Thus, there is a grave need to propose new security solutions for the system-of-systems.

1.1 Background

Blockchain is a decentralized ledger developed to enable the exchange in the digitized currency, execute transactions and deals while ensuring the security. The Blockchain involves participation of members and every participant in the network has the access to latest version of encrypted ledger The Blockchain has a unique property where only the participating members can validate a new transaction. Basically, it's a distributed database put together with a view to maintain a continuously growing data structure blocks while conforming its validity and holds volumes of individual transactions [3].

Blockchain entails an immutable series of blocks just like any conventional public ledger which holds an entire list of records of transaction. Figure 1 shows the structure of a blockchain. A typical block has a unique parent block and in its block header it contains the previous block hash. The Ethereum blockchain also have the uncle blocks i.e. children of the ancestors of the block and their hashes are also stored. The first block of a blockchain having no parent block is called genesis block.

1.2 Smart Contracts

Indeed, smart contracts are the execution of a contractual agreement, the legal provisions of which are enforced into source code and evaluated over a peer network [4]. These contracts are defined by the protocol and performed or implemented by the code, without any involvement of a reliable third party. An instance of a smart contract is to impose a bargain among two customers on the highest rate of moisture. On a preceding day, as indicated by the contract itself, the agreement is inevitably finished by a software tool inspecting the moisture concentrations received from a competent geological survey or some specified devices, scanning and moving money to the victor's account from the loser. Another example is an inheritance gift on the eighteenth birthday of the child.

2.Literature Survey

2.1 Authentication issues in IoT

The aptness to secure data and bound it to only those with the correct permissions is a prominent feature that must be packaged with any system. One might wonder why associated objects from the start have not been subject to the same safety principles [5].

IoT devices can be categorized into many levels but they differ mostly in terms of security levels. Some connect using GPS, 4G or are hard-wired while others use proximity-based protocols such as Bluetooth, RFID, or Wi-Fi. It is usually easy to connect them simply by scanning for nearby devices, by feeding a small code that could be modified from a default or by applying a form of authentication to confirm device and receiver permissions.

Internet of things applications are as diverse as the IoT services they are using, but present developments indicate that change is needed, even though it could take some time for all manufacturers to pass through. A comparable strategy to IoT systems is PKI where virtual certificates demonstrate the validity of the IoT objects in this situation [6].

Digital certificates would guarantee a level of confidence in an IoT system that otherwise might be missing and could recognize and discourage access to unapproved systems with poor safety when coupled with IoT systems to supervise the installations.

With several appliances under an IoT scheme providing possible future defect points, object authentication and approval is vital to ensuring IoT systems security. Devices need to identify themselves before entry points and onshore facilities and applications can be accessed. Moreover, several other IoT systems collapse whenever it relates to object authentication, often using poor fundamental password encryption or using original passwords from their standard values.

Embracing an IoT Framework which really offers safety by standard enables solving these problems, including allowing two-factor authentication (2FA) and implementing the use of powerful passwords or certificates [7]. IoT Systems also include device permission facilities to ascertain which services, applications or assets are accessed across the environment by each machine.

With the advent of even more associated systems, IoT safety is becoming a significant subject. Security flaws that hackers frequently abuse include using weak passwords and fragile encryption. Consequently, IoT identification and authentication

are two of its most significant IoT safety techniques to be observed. The capacity to safeguard information and restrict it to those with the right authorizations alone is not a fresh concept and is widely used in several sectors.

2.2 Related Work

Ali Dorri et al. suggested an architecture specifically for intelligent households where an overlay network and cloud storage are used to coordinate blockchain operations to ensure privacy and safety [8]. Use of various blockchain kinds based on where the transaction takes place in the hierarchical network and provided a decentralized topology.

Bahga and Madisetti have suggested a blockchain-based Platform for the Industrial Internet of Things targeted at enhancing the features of current cloud-based production systems [9]. However, to secure the equipment, a key pair is used that is produced without any control system by the unit itself. Thus, it becomes susceptible to exploitation.

Ruta et al. proposed a Service-Oriented Architecture framework for registration, identity, selection and deposit depending on a semantic blockchain [10]. Such actions are carried out as smart contracts, enabling mutual nature to be shared and confidence to be enforced. Their proposal offers a framework for the Semantic Web of Things, where

a resource identity element is integrated into a basic blockchain structure to provide verifiable records for each transaction. This strategy, however, is based on a personal blockchain that restricts its use.

Dorri et al. suggested an strategy based on three interconnected blockchains made up of two personal blockchains and a government blockchain [11]. Their solution solves the identification problem, but it has a few drawbacks such as (1) each operation gives rise to at least 8 network communications that could quickly flood the entire communication channel if the nodes are highly active and (2) the adopted local blockchains are centralized.

ChainAnchor, an option for preserving privacy infesting an IoT machine into a cloud ecosystem, was suggested by Hardjono and Smith [12]. It promotes device owners to be reimbursed for distributing their sensor information to service suppliers and enables service users and device owners to share that sensor information while maintaining privacy as well. However, their objective is the complete anonymity of the involved systems and has not been adjusted to various IoT utilization instances in which user recognition is essential.

Xu et al. suggested a blockchain-based distributed storage system specifically for IoT-involved large-scale data analysis [13]. It depends mainly on the characteristics of the blockchain to store operations of IoT systems in a distributed way. This job, however, only covers the need for storage, but the safety problems of the IoT stayed unresolved.

2.3 Summary of Literature Survey

Author	Summary
Christidis et al.(2016)	Provide a description of how blockchain can be integrated in IoT
Malviya(2016)	Quick study of safe IoT with blockchain functionality
Bahga and Madisetti(2016)	Blockchain platform for Industrial IoT to enhance the existing CBM
Ruta et al.(2017)	Propose a service-oriented architecture for registering and deposit depending on semantic blockchain
Dorri et al.(2017)	Proposed a private blockchain based architecture for resolving the identity issue in IoT.
Hardjono and Smith(2016)	Proposed Chainanchor, a technique of privacy preservation to commission an IoT machine
Xu et al.(2018)	Proposed Saphire, large scale data analytics for IoT
Ouaddah et al.(2017)	Proposed Fairaccess, a access control framework in IoT.

3. Proposed work

The proposed Blockchain based authentication of devices in the IoT ecosystem consists of three phases namely, The Initialization phase, Block formation phase and the Association phase.

3.1 Initialization Phase

The suggested strategy is extremely scalable and can be implemented to a multitude of IoT-based devices. This stage involves designating an item as a master of a certain network involving a private-public key pair and can be regarded as a licensing entity. Any object can be an authorized master and its followers are the rest of the objects that make up part of the system. Each follower is then enabled with a token construct, which is a 64-byte certificate composed of:

(1) a (grpid), the group identifier where the object is present.

(2) an (objid), the identifier of a follower in the group,

(3) pubaddr, the public address of a followerIt is made up of the very next 20 bytes of the public key record of the follower.

(4) an insignia structure containing the Elliptic Curve Digital signature (ECDS).

ECDS overhauls traditional signature algorithms like RSA showing advantages especially concerning signature times and key sizes and is more applicable to IoT contexts.

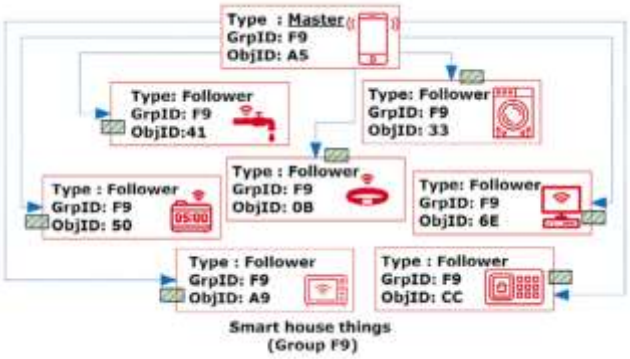

Fig 2. Initialization Phase

3.2 Block Formation

The Figure 3. shows details of the proposed approach and all the phases of the system. As shown in Fig. 2, phase (A), Connected objects may be involved in a number of fields. Once the group is formed, it is necessary to create the group at the tier of blockchain, i.e. the phase of block formation.

The master instigates a transaction by issuing a request to the blockchain where the requestincludes the designation of the master as well as the group identifier to be generated. The blockchain checks the individuality of the master's group ID as well as the object ID. If the transaction is legitimate, the group will be generated. Since a public blockchain is enacted, a group can be created by any approved consumer.

The followers then submit transactions to be affiliated with their concerning groups at the level of the blockchain and the smart contract confirms the individuality of the follower's identifier (object ID), then confirm the validity of the follower's token using the public key of the master.

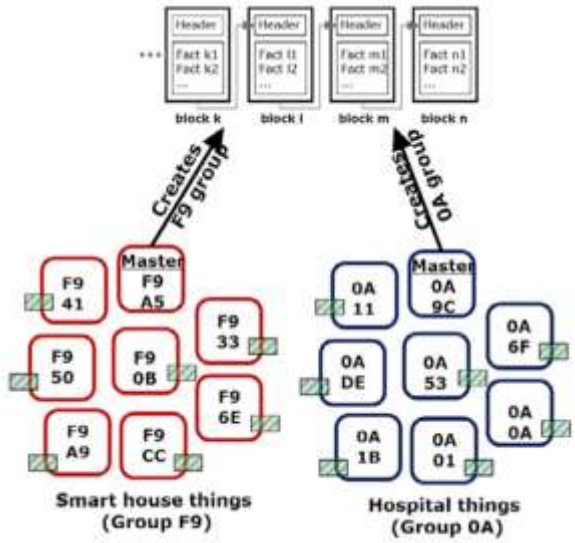

Fig 3. Block formation phase

3.3 Association phase

The follower completes its first transaction successfully and sends a request for association, thereafter the authenticated follower doesn't need to utilize its token to be authenticated for its further transaction.

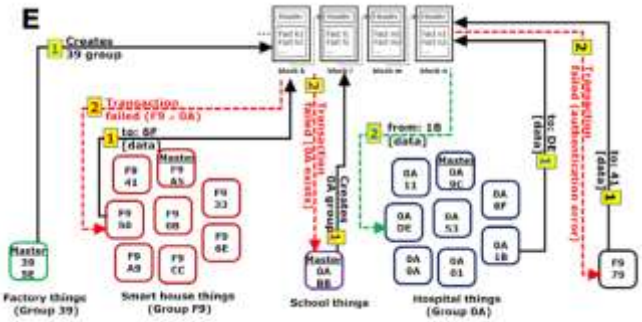

Fig 4. Association phase

For example, in the figure 4 follower device called F is described which have been provided a token signed by master M. The token entails a public key PubKey_F, a grpID = XX and an objID = YY.

The first operation is an association request. The signal to be sent is marked along with its token with the personal key of the follower. Upon receiving the request at the blockchain, the record is verified with the public key of the follower to confirm its integrity. Then the token of the Follower is checked using the public key of the master as the master is the one who publishes it. If the token is found to be valid, its group ID, object ID and public key association will be stored by the blockchain.

The situation in which f9 initiates the next transaction after requesting the affiliation. This transaction involves: the data being exchanged, the group ID, the object ID and the signing of the ECDS using the private key of the follower. Again, as the blockchain receives the transaction, it verifies the certificate with the public key of the follower and thus verifies the validity.

If the certificate is found to be valid, the blockchain will confirm whether the public key used to verify the transaction already exists and is associated with the same group ID and object ID included with the transaction.

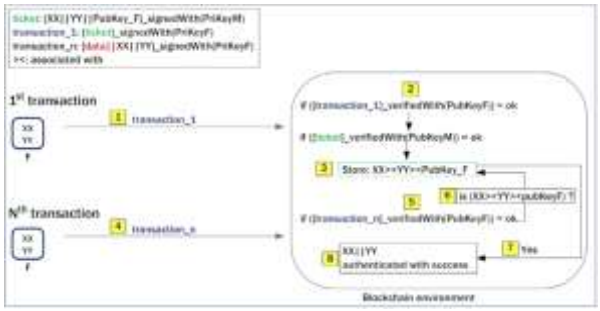

Fig 5. Communication within the system

If the relation is discovered to be available and legitimate, the object will be authenticated effectively.

3.4 Programming Environment and Dependencies

3.4.1 Qt framework

Qt (phonetically "cute") is indeed a free open source runtime environment for generating visual customer models along with multi-platform apps running on multiple operating systems including Linux, Windows, macOS, Android or integrated devices with little or no shift in the fundamental codebase while still being a indigenous implementation with indigenous capacities and precision. Qt is currently being reviewed under open-source governance by The Qt Company, a publicly listed company, and the Qt Project, with personal developers and groups working to promote Qt. Qt is accessible within GPL 2.0, GPL 3.0 and LGPL 3.0 permits under either business and open source licenses.

3.4.2 QJsonRpc

QJsonRpc is a JSON-RPC procedure Qt application. It fits well with Qt, consolidating Qt's pseudo object scheme to deliver facilities across the JSON-RPC interface. QJsonRpc is approved as a versatile information exchange method under the LGPLv2.1.JSON. JSON-RPC, like XML-RPC, is a compact distant call method protocol.

3.4.3 Ethereum Client

A client of Ethereum like [TestRPC] or [geth] is a virtual machine multipurpose tool that operates a complete Ethereum node introduced in "Go". It provides three features: subcommands and choices for the command line, a Json-rpc server, and an interactive console.

4. Result Analysis

Attempts were made to resolve the authentication issues in IoT by applying centralized techniques like PKI (Public Key Infrastructure), but the proposed system involves adaptation of Blockchain for resolving those major security issues. Blockchain and IoT have been collaborated previously but as this is a novel approach the juxtaposition of the proposed system is done with respect to existing centralized authenticating approaches. The figure 6(a) and 6(b) is the graphical representation of the time versus power consumption of the IoT ecosystem with blockchain at the backend. It can be clearly observed that the proposed approach is performing considerably well when compared with the PKI based IoT system.

The comparison done is two-fold which includes time and power consumption.

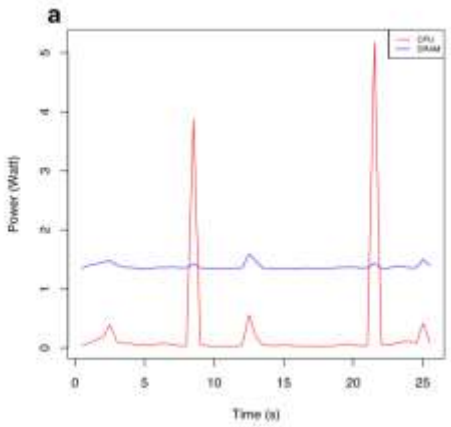

Fig 6(a). Impact of Blockchain approach on data exchange

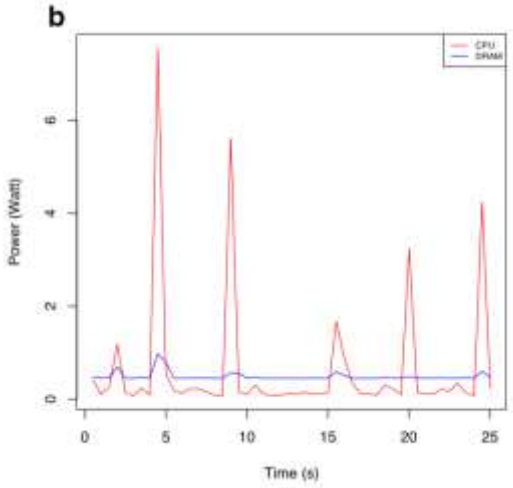

Fig 6(b)Impact of PKI approach on data exchange

Standard deviation and Average of obtained results								
	Association Time		Data exchange time		CPU		NIC	
Approach	Avg	Sd	Avg	Sd	Avg	Sd	Avg	Sd
PKI	27.09	0.54	1.88	0.028	62.13	8.29	89.26	14.21
Blockchain	1.56	0.13	0.04	0.001	9.76	2.04	16.14	2.69

As the proposed approach primarily focuses on securing and authenticating devices the network delay is assumed to be negligible. The realized approach is run for 100 test cases and the average and standard deviation values are calculated.

5. Conclusions

Reliable virtual areas are generated in the suggested framework where the objects can interact in a completely safe way. Each unit is marked with a token certificate that had to justify its validity. It depends on a Public Blockchain taking advantage of all

its safety features. Thus, with the enhanced advantages of blockchain's safety characteristics, the suggested method can be discovered robust against authentication service-related assaults such as the sybil attack, spoofing assault, etc.

It also allows the structure more practical and accessible to any consumer by using a public blockchain. This strategy can be applied to countless IoT situations, products, and environments.

References

[1]R.Alur, E. Berger, A.W. Drobnis, L. Fix, Fu K., G.D. Hager, D. Lopresti, K. Nahrstedt, E.Mynat, S . Patel, *et al.*Systems computing challenges in the internet of things arXiv preprint arXiv: 160402980 (2016), pp.43-47

[2] E.G. AmorosoFundamentals of computer security technology Prentice-Hall Inc. (1994) Bahga, Madisetti, 2016 A. Bahga, V.K. MadisettiBlockchain platform for industrial internet of things J Softw Eng Appl, 9 (10) (2016), pp. 533

[3] Bentov, Lee C., A. Mizrahi, M. RosenfeldProof of activity: extending bitcoin's proof of work via proof of stake ACM SIGMETRICS Perform Eval Rev, 42 (3) (2014), pp. 34-37

[4] D. Bong, A. PhilippSecuring the smart grid with hardware security modules ISSE 2012 securing electronic business processes, Springer (2012), pp. 128-136

[5] M. Castro, B. Liskov, *et al.*Practical byzantine fault tolerance Proceedings of symposium on operating system design and implementation, OSDI, 99 (1999), pp. 173-186

[6]Chang S.j., R. Perlner, W.E. Burr, M.S. Turan, J.M. Kelsey, S. Paul, L.E. BasshamThird-round report of the sha-3 cryptographic hash algorithm competition NIST Interagency Report 7896, NIST (2012), pp. 57-63

[7] K. Christidis, M. Devetsikiotis Blockchains and smart contracts for the internet of things IEEE Access, 4 (2016), pp. 2292-2303

[8] Dorri, Ali, Salil S. Kanhere, and Raja Jurdak. "Blockchain in internet of things: challenges and solutions." *arXiv preprint arXiv:1608.05187* (2016).

[9] M Ruta, F Scioscia, M Di Summa, S Ieva, E Di Sciascio, M Sacco International Journal of Semantic Computing 8 (04), 491-514

[10] Bahga, A. and Madisetti, V. (2016) Blockchain Platform for Industrial Internet of Things. *Journal of Software Engineering and Applications*, **9**, 533-546.

[11] Hardjono, Thomas, and Ned Smith. "Cloud-based commissioning of constrained devicesusing permissioned blockchains." *Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security*. ACM, 2016.

[12] Xu, Quanqing, et al. "A blockchain-based storage system for data analytics in the internet of things." *New Advances in the Internet of Things*. Springer, Cham, 2018. 119-138.

[13] A Ouaddah, A Abou Elkalam, A Ait Ouahman Security and Communication Networks 9 (18), 5943-5964