International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 8 Issue 2 July - December 2018
International Manuscript ID : 22308849072018-04

Blockchain Integrated Secured Architecture for Advance Wireless Networks in Internet of Things

[1] *KARRAR RASHID YASIR* [2] *JAMAL KH_MADHLOOM*

Ministry of Water Resources
General Commission for Irrigation and Reclamation Projects, Iraq

College of Computer Science & Information Technology
University of Wasit, Iraq

Abstract

The current era is surrounded with enormous devices and gadgets connected with each other using high performance technologies. Such type of technology loaded object communication is treated under the aegis of Advanced Wireless Integrated Internet of Things (IoT). A number of applications are using IoT based communication whether it is related to defense equipments, smart cities, smart offices, highway patrolling, smart toll collections, business communications, satellite televisions, traffic systems or interconnected web cams for social security. IoT is also known and associated with other terms including Ubiquitous Computing (UbiComp), Pervasive Computing or Ambient Computing in which number of devices and objects are virtually connected for remote monitoring and decision making. This manuscript is focusing on the integration of Blockchain Technology for the security and overall performance of the IoT. Blockchain is the encrypted, distributed computer filing system designed to allow the creation of tamper-proof, real-time records.

Keywords: Blockchain based IoT, Blockchain Security, IoT Security, Internet of Things

Introduction

As there are so many devices and equipments connected with each other using virtual environment, there are the stern issues related to security, privacy and overall performance of networks so that integrity aware communication can take place with greater efficiency. Since the inception of IoT devices and intercommunication, a significant work on security and privacy is going on because of the increasing vulnerability aspects and attacks from assorted sources [1, 2].

Different types of attacks are used to control and damage the IoT environment at different layers. The attackers can damage and control the IoT network by sending the malicious packets and signals and infrastructure can be virtually destroyed. Such attacks are in the high priority as these attacks affect the entire network. A number of attacks are prevalent for controlling and damaging the pervasive networks [3, 4, 5].

Denial of Service (DoS) Attack: In DoS attack, the network availability is jammed by the attacker node or malicious packet by capturing the bandwidth or communication channel. Here, the authentic and legitimate users are not able to access the network services. This is one of the prominent attacks that works on the network layer of IoT based scenario. Such type of attack is more dangerous when it becomes Distributed Denial of Service (DDoS) because this mechanism is involved as distributed in nature. In this attack, the malicious node or attacker perform the attack from multiple and different locations [6].

Sybil Attack: Sybil attack affects the network layer of vehicular network a lot. Using this attack, the manipulation of source identity takes place. The malicious node attempts to fabricate and manipulate the original identity and pretends to be a registered or original source node. In Sybil attack, the attacker node creates assorted vehicles or nodes of same identity by replication and forces other nodes to leave or move fast from the road. Using resource testing these attacks can be detected which works on the assumption that vehicles have limited resources. This problem of Sybil attack can be addressed using public key cryptography where public keys are used to authenticate vehicles [7].

Node Imitation Attack: In this type of attack, the transmission of messages takes place by the imitated node of other identity. In this way, the attacker can send the malicious or wrong messages to any node hiding or changing its own identity. The identity of IoT node can be disguised in this attack to capture the authentic and secured packet which can be very harmful and disaster prone for the entire scenario [8].

Application Level Attack: This type of attack in IoT environment tamper the messages and retransmit to the destination which can be very insecure. For example, in Internet of Vehicles (IoV) based implementation the high traffic lane can be broadcasted as Congestion Free Lane. With this approach, the upcoming congestion can be very high on that lane which can result in the disasters [9].

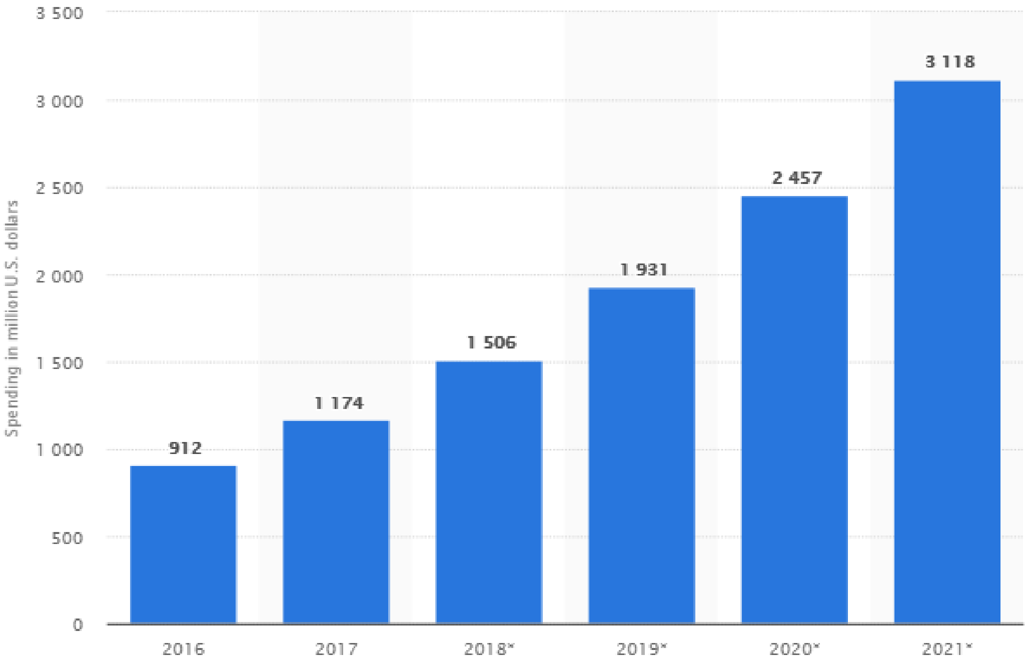

Figure 1: Internet of Things Security Predicted Spending Worldwide from 2016 to 2021 (in million U.S. dollars) [Source: Statista, The International Statistics Portal]

This statistic shows the Internet of Things (IoT) security spending worldwide from 2016 to 2021. In 2017, the IoT security spending amounted to 1.2 billion U.S. dollars.

IPv6 and Blockchain in Wireless Technologies and Internet of Things (IoT)

Security and integrity is the main issue in IoT based network environment in which interception free secured communication is required. To enforce and integrate the higher degree of security, there is need to implement IPv6 for IoT scenarios with dynamic hybrid cryptography in the keys generation and authentication. The IPv6 based approach can be enabled with fully secured algorithms and non vulnerable towards the interceptions. With the increasing implementations of IoT in diversified domains, it becomes necessary to work out the security aspects of IoT with the secured routing of packets so that the intrusion cannot take place and all the transmission can be fully secured [10].

A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network. This allows the participants to verify and audit transactions inexpensively. A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. They are authenticated by mass collaboration powered by collective self-interests. The result is a robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double spending. Blockchains have been described as a value-exchange protocol. This blockchain-based exchange of value can be completed quicker, safer and cheaper than with traditional systems. A blockchain can assign title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block. Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any blockchain has a specified algorithm for scoring different versions of the history so that one with a higher value can be selected over others. Blocks not selected for inclusion in the chain are called orphan blocks. Peers supporting the database have different versions of the history from time to time. They keep only the highest-scoring version of the database known to them. Whenever a peer receives a higher-scoring version (usually the old version with a single new block added) they extend or overwrite their own database and retransmit the improvement to their peers. There is never an absolute guarantee that any particular entry will remain in the best version of the history forever. Because blockchains are typically built to add the score of new blocks onto old blocks and because there are incentives to work only on extending with new blocks rather than overwriting old blocks, the probability of an entry becoming superseded goes down exponentially as more blocks are built on top of it, eventually becoming very low.:ch. 08 For example, in a blockchain using the proof-of-work system, the chain with the most cumulative proof-of-work is always considered the valid one by the network. There are a number of methods that can be used to demonstrate a sufficient level of computation. Within a blockchain the computation is carried out redundantly rather than in the traditional segregated and parallel manner.

RPL is the IPv6 Based Protocol for IoT. It is primarily integrated for IPv6 over Low power Wireless Personal Area Networks (6LowPAN). It works with the dynamic creation of Destination-Oriented Directed Acyclic Graph (DODAG) having unidirectional as well as bi-directional communication. It is having multiple instances with the localized behavior for higher optimization. RPL enables each node in the framework to pick if packets are to be sent upwards to their root or downwards to their child nodes.

Need of Blockchain Technology

There is need to integrate and associate the high performance approaches of security in IoT including Blockchain with Quantum Cryptography. By using blockchain to manage access to data from IoT devices any attacker would have to bypass an additional layer of security that is underpinned by some of the most robust encryption standards available. In addition, because there's no centralized authority, single-point failure concerns become a distant memory, no matter how populated a particular network is. The usage and elevation of security with device independent cryptography can be done in IoT for the cumulative performance. The integration of Block-Chain based cryptography and security mechanism is required for the overall efficiency of the IoT environment [11].

Following are the key points from the study which can be worked out for security and challenges with IoT with the integration of blockchain security and quantum cryptography

- Advance Wireless based
    - IoT API Security with Blockchain layers
    - IoT Tokens Generation with Quantum Cryptography
    - IoT PKI
    - IoT Encryption
    - IoT Authentication

Conclusion

Enormous increment in IoT communication originates from processing gadgets and implanted sensor frameworks utilized in modern machine-to-machine (M2M) communication, brilliant vitality matrices, home and building robotization, vehicle to vehicle communication and wearable registering gadgets. The fundamental issue is that on the grounds that systems administration machines and different articles is moderately new, security has not generally been considered in item plan. IoT items are frequently sold with old and un-fixed inserted working frameworks and programming. Moreover, buyers frequently neglect to change the default passwords on brilliant gadgets - or in the event that they do transform them, neglect to choose adequately solid passwords. To enhance security, an IoT gadget that should be specifically open over the Internet, ought to be portioned into its very own system and have organize get to confined. The system fragment should then be checked to distinguish potential peculiar movement, and move ought to be made whether there is an issue.

References

[1] Meyer S, Ruppen A, Magerkurth C. Internet of things-aware process modeling: integrating IoT devices as business process resources. InInternational conference on advanced information systems engineering 2013 Jun 17 (pp. 84-98). Springer, Berlin, Heidelberg.

[2] Farooq MU, Waseem M, Khairi A, Mazhar S. A critical analysis on the

security concerns of internet of things (IoT). International Journal of Computer Applications. 2015 Jan 1;111(7).

[3] Xu T, Wendt JB, Potkonjak M. Security of IoT systems: Design challenges and opportunities. InProceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design 2014 Nov 3 (pp. 417-423). IEEE Press.

[4] Mahmoud R, Yousuf T, Aloul F, Zualkernan I. Internet of things (IoT) security: Current status, challenges and prospective measures. InInternet Technology and Secured Transactions (ICITST), 2015 10th International Conference for 2015 Dec 14 (pp. 336-341). IEEE.

[5] Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: The case study of a smart home. InPervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on 2017 Mar 13 (pp. 618-623). IEEE.

[6] Raymond DR, Midkiff SF. Denial-of-service in wireless sensor networks: Attacks and defenses. IEEE Pervasive Computing. 2008 Jan 1(1):74-81.

[7] Demirbas M, Song Y. An RSSI-based scheme for sybil attack detection in wireless sensor networks. InProceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks 2006 Jun 26 (pp. 564-570). IEEE Computer Society.

[8] Pirzada AA, McDonald C. Circumventing sinkholes and wormholes in wireless sensor networks. InIWWAN'05: Proceedings of International Workshop on Wireless Ad-hoc Networks 2005 May 23 (Vol. 71).

[9] Zhang Y, Lee W, Huang YA. Intrusion detection techniques for mobile wireless networks. Wireless Networks. 2003 Sep 1;9(5):545-56.

[10] Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems. 2018 May 1;82:395-411.

[11] Yli-Huumo J, Ko D, Choi S, Park S, Smolander K. Where is current research on blockchain technology?—a systematic review. PloS one. 2016 Oct 3;11(10):e0163477.