ISSN 2278-3091

Volume 8, No.3, May - June 2019

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse14832019.pdf

https://doi.org/10.30534/ijatcse/2019/14832019

Security and Privacy via Optimised Blockchain

Monica Thomas[1], **Dr. Varghese S Chooralil**[2]

[1]Rajairi School of Engineering and Technology, India, monithofl@gmail.com

[2]Rajagiri School of Engineering and Technology, India, varghesesc@rajagiritech.edu.in

ABSTRACT

Security of IoT devices and applications can be improved by using the emerging Blockchain Technology which uses decentralised interaction and scalable architectures with security and distributed trust. In this work a review of Lightweight scalable Blockchain is proposed for security and privacy of IoT devices. An IoT scenario of smart home is used for illustrative purposes but this proposed architecture is well-suited for diverse IoT applications. Effectiveness of this architecture is analysed using common threat models which provides an appropriate assessment for security and privacy implementation for smart home.

Key words : Blockchain, IoT, Security

1. INTRODUCTION

IoT devices are now a major part of the mainstream electronics culture and consumers everywhere are adopting smart devices into their houses. Latest estimation shows that by 2020, there will be up to 30 billion connected devices all around the world connected to the internet. Along with the growth in number of sensors, everywhere the companies are now looking for secure and scalable mesh networks for automated transaction processing. The best way is to leverage the emerging blockchain technology. The stakeholders require their data to be transferred securely and this data is huge. Transfer of this data in secure fashion means there needs to be processing at different layers in the architecture. At each of these layers threats and malicious sources needs to be detected and eliminated.

This cryptographically secured, immutable distributed ledger technology called blockchain could enhance IoT frameworks with innate security and providing more auto-mated resource optimization all at the same time. By allowing devices to register and validate themselves against the network the overall help in maintaining system health is achieved. Thus network takes care of the network and validates each node within it and this forms the core concept of decentralisation in this technology. The Blockchain is a collection of blocks which are created cryptographically and sent across to the network. Once a new block is accepted, it is sealed permanently by hashing it along with the hash of previous block rendering them immutable and highly secure. Thus these blocks cannot be corrupted.

Transparency and immutability of data is always a huge point of discussion in security, among which immutability is mostly accepted but how much of the data should be transparent is a question. Immutability refers to unchangeable data.

The material presented in this paper is organised into 6 chapters. After this introductory chapter, chapter 2 defines the substantive findings as well as theoretical and methodological contributions done in the field of Blockchain for IOT.

Section 3 outlines the first work taken into study. This work is based on blockchain based architecture which does not employ the heavy POW for IoT that also eliminates problems faced in classic blockchain, while we still maintain security advantages and also those of privacy. Section 4 explores lightweight scalable Blockchain in a smart home setting which is a detailed implementation of the above methodology. Section 5 presents' brief summaries of the two significant works and compares their analysis. Finally, Section 6 compiles the suggestions of the two significant work chosen to propose enhanced Blockchain for IoT architecture and the future scope of this area.

2. LITERATURE REVIEW

In the last few years, different authors with their own advantages and disadvantages have proposed many efficient Blockchain architectures for different sectors which can be implemented along with IoT. Some of the works can also be used in energy sector, government sector, supply chain.

2.1 Existing Works

The paper review on how distributed peer-to-peer network can interact with each of the non trusting members without any intermediary in between them and also gives insight into the working of smart contracts scripts which helps in automating various processes within blockchain [1].

The authors also highlight various Blockchain embedded into IoT scenarios and what pointers the developers need to consider for their implementation.

In the work the authors' present access control for IoT – blockchain design that is distributed and helps in data management. Their design is tailor-made for data streams in IoT and along with enabling secure data sharing. The basis of access control management lies in using blockchain in the storage layer [2].

Paper provides a detail study on the storage of time-series IoT data via a locality-aware decentralized storage facility that is managed with the blockchain technology at the edge of the network [3]. Highlight is a system with cryptographically secure data sharing with frequent key updates available.

The authors of facilitates a Blockchain based infrastructure to provide privacy and security into vehicles [4]. Privacy of the involved users in this vehicular eco system is ensured by a changeable Public Key (PK) created for each user. By hiding the users' identity, security is increased. Management of transactions are managed by the block managers. This way the users' identity remains secure while sending transactions.

In paper a thorough review on how to adapt blockchain for the peculiar requirements of IoT application design [5]. The Design objectives are finalised by keeping cloud centered architecture in mind while involving blockchain. Possible optimizations are detailed that provides aesthetics to the design, development, and deployment. Despite several limitations that blockchain technology faces in todays world the authors try to highlight its advantages for the future.

3. PROPOSED ARCHITECTURE

The proposed architecture [6] is an optimized blockchain for IoT security and privacy issues. Which has mainly 3 tiers as shown the figure 1 below: Smart Home Overlay, Cloud storage. Smart home consists of 1.IOT Devices, 2.Local Immutable ledger (IL) 3. Local storage. Similar to distributed network as advertised by blockchain but is maintained by Smart Home Manager (SHM) centrally. Overlay is a P2P network, where nodes are clustered with cluster Heads(CH) who maintain the Public Key of requesters and requestees.

It also has multi signature transaction (signed by requesters and requestees). Each cluster head maintains a public blockchain ledger. Verification of a transaction occurs in 3 steps: 1.Checks if the device has right to append, 2.Verify the signature, 3.Increment the count of transaction.

Cloud[9] Storage consists of Blocks with a unique block number assigned to it. Each of these blocks are identical and are used to store users' data. This block-number is used for authentication by Smart Home Manager (SHM) along with the hash of stored data. User authentication can be done by locating the data in a block by using the block number and hash given by the smart home manager.

3.1 Observations

The transactions are handled by classifying them into 3 types: 1. Store: store device data on cloud. 2. Access: access a stored data 3. Monitor: Real time data of requested device is sent.

Distributed Trust method is used to ensure the validation of the received blocks. This method also reduces the overhead as compared to bitcoin in the case for block verification. A new user is initially considered malicious and all its transactions are verified with other blocks. Transaction verification is done by confirmation that the requester has the right to append transactions. This is done by comparing the public key hash of the present transaction with the previous transaction output Public Key. After this step, the requester signature is verified using his Public Key. Next either one, successful transactions count or failed transactions count is increased by one. If the count of successful transaction is increased, the transaction is verified.

For the security[8] and privacy analysis, it the malicious adversary can be: a Cluster Head, a device at home or a node in the overlay, or maybe even the cloud storage. The actions of adversaries can be anything, they could modify data, discard data or transactions, create fake transactions etc. However, they will not be able to break the encryption. The authors monitor the system for various types of attacks such as Denial of Service, Modification Attack:, Dropping Attack, Appending Attack etc are used for the case study. The behaviour of system for each of these attacks are analysed if the system is able to defend against it.

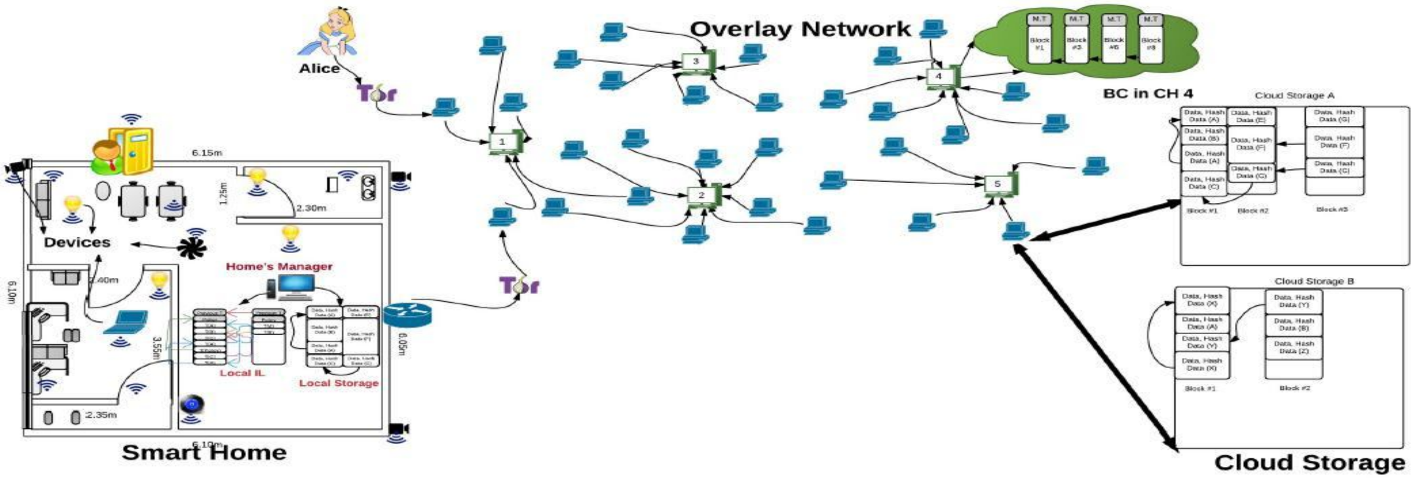

Figure 1: Architecture of smart home, overlay and cloud storage

4. LIGHTWEIGHT SCALABLE BLOCKCHAIN

Most of current instantiations of Blockchain cannot be readily adopted into the creation of the IoT application due to Complex consensus algorithms, Latency, Security overheads, throughput. In this paper, a Lightweight Scalable Blockchain (LSB) is proposed for the IoT security and privacy [7].

It consists of similar tiered framework as seen in the previous section. This work incorporates lightweight consensus algorithm, a distributed throughput management strategy, a distributed trust method and a separation of the data flow from the transaction traffic. Here the cluster head is known as Overlay Block Manager (OBM). Overlay Node transactions are secured using asymmetric encryption, cryptographic hash functions (e.g. SHA256) and digital signatures.

Overlay transaction is stored in public Blockchain network by the OBMs. One of the main highlights of this work is that it uses a Consensus Algorithm to reduce the overhead instead of more resource intensive algorithms such as POW. OBM waits random time before generating block and due to this waiting period difference reduces the number of duplicate blocks that can be generated simultaneously. Only one block can be generated during the consensus period. This helps in restricting OBM from creating multiple blocks. This consensus-period is adjusted by Distributed Throughput Management, which monitors Blockchain utilisation. Verification of block is done in following steps: 1. validate signature, block is valid only if all transaction in it are valid. 2. Distributed trust algorithm to verify block: notion of direct and indirect evidence.

Direct evidence: OBM B has direct evidence about OBM A if it previously verified at least one block that was generated by B.

Indirect evidence: If OBM A does not have direct evidence about OBM B, but if either of the other OBMs has at lest once verified a block generated by B as valid, then A has indirect evidence about B. If no evidence then all transactions are verified.

4.1 Observation

Interactions between different tiers are facilitated by transactions. All the transactions that are exchanged between nodes in same smart home are called as local transactions. Encryptions of these transactions take place by using a shared key between the respective nodes. It involves genesis transaction, store locally transaction, data exchange transaction. Overlay nodes must first create a genesis transaction to initiate in the public Blockchain. If the requester and the requestees are both overlay nodes then the transaction is known as overlay transaction. Overlay transactions use asymmetric encryption for overlay nodes. It involves Genesis transaction, store cloud transaction, access and monitor transaction.

This work handles the requirement of Confidentiality (by encryption), integrity (each transaction includes hash of other transactions), Availability, Authentication, Non repudiation, which allows LSB to meet the security requirements. This blockchain architect also uses anonymity for protecting users privacy in the overlay or in the smart home and also in the cloud storage.

5. EXPERIMENTAL SETUP

Performance evaluation of this Lightweight architecture was done by running simulations on number of nodes. Simulations are conducted using NS3 simulator and Cooja. Cooja which is a network simulator specifically designed for Wireless Sensor Networks is used to review the performance of this smart home tier. Cooja is highly recommended for analysing low resource devices that are mostly found in smart home applications and also helps in implementation of various IoT- protocols. NS3 is a discrete event simulator used to evaluate the overlay networks performance. The distributed trust strategy can also be employed in other Blockchain b ased systems. These two highlighted paper setup can be employed as a basis of IoT Blockchain integration.

6. CONCLUSION

The original blockchain architecture is difficult to be used for IoT applications due to bandwidth and scalability difficulties and for its heavy validation algorithms. To address these difficulties, the suggested Lightweight Scalable Blockchain (LSB) is one concept that can be further researched for integrating into IoT applications. This architectures distributed trust approach reduces the processing time for validating new blocks by the OBMs as they gradually start to build their trust on each other. Another encouraging feature is the use of distributed trust management which helps in controlling the network parameters. Security analysis by studying the different types of attacks suggest a secure network, where blokchain and detect and manage the security threats easily. The performance evaluation also suggests positive results that renders this system to be highly effective for IoT. This idea can be further researched into to be implemented in other areas of technology.

.

ACKNOWLEDGEMENT

I would like to thank the Department of Computer Science and Engineering of Rajagiri School of Engineering and Technology, for allowing me to do this paper, and for providing the facilities needed for this Work. I am also grateful to Dr Varghese S Chooralil, for reviewing my progress periodically and giving valuable suggestions that helped me to improve my work.

REFERENCES

1. M. Fernndez-Carams and P. Fraga-Lamas, **A review on the use of blockchain for the internet of things**,IEEE Access , pp. 123, May 2018. doi: 10.1109/ICI-CICT.2014.6781379
2. A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, **BlockChain: A Distributed Solution to Automotive Security and Privacy**, IEEE Commun. Mag., vol. 55, no. 12, pp. 119125, dec 2017. https://doi.org/10.1109/MCOM.2017.1700879
3. Shafagh, H.; Hithnawi, A.; Duquennoy, S. **Towards blockchain-based auditable storage and sharing of IoT data.** In Proceedings of the 9th ACM Cloud Com-puting Security Workshop (CCSW 2017), Dallas, TX, USA, 3 November 2017. https://doi.org/10.1145/3140649.3140656
4. K. Christidis, M. Devetsikiotis, "**Blockchains and Smart Contracts for the In-ternet of Things**", IEEE Access, pp. 2292-2303, May 2016. https://doi.org/10.1109/ACCESS.2016.2566339
5. A. Kousaridas, S. Falangitis, P. Magdalinos, N. Alonistioti, and M. Dillinger, **Systas: Density-based algorithm for clusters discovery in wireless networks, in Personal, Indoor, and Mobile Radio Communications (PIMRC)**, 2015 IEEE 26th Annual International Symposium on. IEEE, 2015, pp. 21262131. https://doi.org/10.1109/PIMRC.2015.7343649
6. A. Dorri, S. S. Kanhere, and R. Jurdak, **Towards an optimized blockchain for iot**, in IEEE/ACM International conference on Internet-of-Things Design and Implementation (IoTDI), 2017. https://doi.org/10.1145/3054977.3055003
7. A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram, LSB: **A lightweight scalable blockchain for IoT security and privacy**, Dec. 2017
8. N.Saritha Devi, K.S.R.Raju, A.Madhu, R.Raja Sekhar, **Safety and Security for School children's Vehicles using GPS and IoT Technology,** International Journal of Advanced Trends in Computer Science and Engineering, Volume 7, No.6, November - December 2018. https://doi.org/10.30534/ijatcse/2018/03762018
   Goodubaigari Amrulla, Murlidher Mourya, Rajasekhar Reddy Sanikommu and Abdul Ahad Afroz**, A Survey of :Securing Cloud Data under Key Exposure,** International Journal of Advanced Trends in Computer Science and Engineering, Volume 7, No.3, May- June 2018. https://doi.org/10.30534/ijatcse/2018/01732018