International Journal of Engineering & Technology, 7 (4.6) (2018) 42-44

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Decentralized Secure Online Digital Data Registrations

Raman Dugyala[1]*, N Hanuman Reddy[2], Raghuram G [3] J Lakshminarayana[4]

[1]*Vardhaman College of Engg Hyderabad . india*
[2]*Vardhaman College of Engg.*
[3]*Vardhaman College of Engg.*
[4]*Department of Computer Science and Engineering MLR Institute of Technology, Hyderabad*
**Corresponding author E-mail: raman.vsd@gmail.com:*

Abstract

A potential challenge in the present secure transaction lies in illegitimate access to premium digital data available in various formats on various service-sectors for Government and Non-Government process models. This vulnerable scenario leads to identity attacks, man in the middle (MITM) attacks and denial of service (DoS) attacks. Our proposed model uses blockchain technology with machine learning classifiers to identify and detect possible attacks within a peer-to-peer network. Blockchain uses digital signatures, proof-of-work algorithm and consensus algorithms to protect system from possible integrity and denial of service attacks and machine learning classifiers deployed at every node offers confrontation to any intruder's attack.

Keywords: *DoS attacks, MITM attacks, Blockchain, Machine learning, Intrusion, Data Registration*

1. Introduction

The primary objective of the paper is to identify and evaluate different types of attacks. One among them is denial of service (DoS) attacks to identify patterns of attacks points us to produce essential data for various attacks. The two common dual attacks by DoS are direct and amplification attacks. The two important identity attacks are online shopping and social security number identity attacks. The two significant MITM attacks[1] are Rogue access point and packet injection attacks. Having seen behavior of these attacks an attempt is made in this paper to address the issues related to secure transactions of premium digital data across various services across the globe. The paper discusses about attacks along with machine learning classifier at every node in the registered offices of the grid to prevent intruder's attack.

2. Proposed System

The proposed system deals with blockchain[11] land registration, united with tough titling legislature, could hitherto demonstrate the superlative way to convey a protected, transparent and well-organized land records scheme in India. It will purge numerous of the paucities overwhelming the present system. The technology compromises an pioneering resolution to a range of concerns tormenting the nation.

2.1 Distributed:

The solution[11] we can provide to the above problem is by distributing the data about the land to all the terminals (computers at each registration office) in the network instead of storing at a single place. These terminals can be spread across all the regions in the country. The data is encrypted (hashed) before distributing.

2.2 Decentralized:

We have developed a protocol such that the information or power is not centralized at a particular place or office.

2.3 Transparent:

As the data is distributed throughout the network every terminal holds the information about every transaction (buy, sell, inherit). By possessing some permission a person can easily access the data and see the data.

2.4 Blockchain:

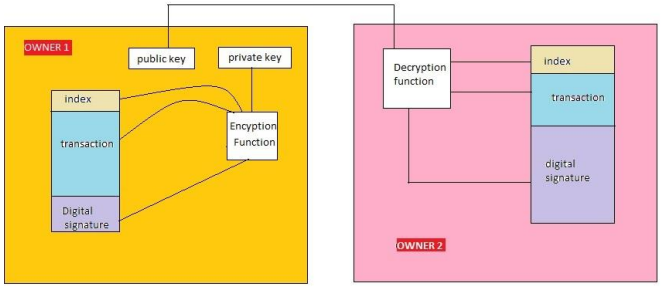
Blockchain is a continuously growing list of records called blocks which are connected to each other. Each block typically contains the cryptographic hash of previous block and timestamp. The blockchain is designed in such a way that it is inherently impossible to modify data .It is typically a distributed ledger managed by a peer-to-peer[2] network adhering to protocols for validating blocks. Once a data entered into a block it is highly impossible to change that data.

2.5 Transactions

Every transaction whether it is buying or selling or inherit must be digitally signed. Digital signatures[13][15] are like regular signatures which help us to ensure that owner has approved for this
transaction. We should also prove a mechanism for others to verify whether the digital signature is legitimate or forged. This can be done by generating public key and private key pairs by every person. The owner then encrypts the transaction and its index with his private key and adds the enciphered value at the end of the

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

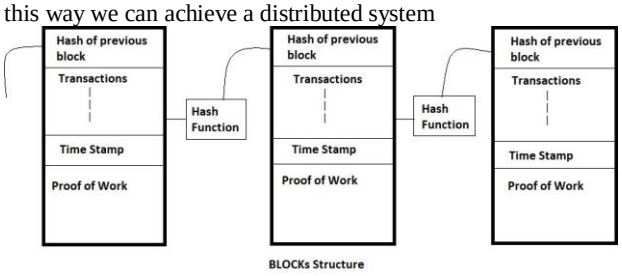
transaction and the new owner can verify by using the previous owner's public key.



But the problem is what if the owner again sell to another person (i.e. double selling).Generally this involves a third party to verify it like government authorities .This problem can be solved by distributing this transaction to every one so that the transaction is transparent and even if the owner tries to resell it is easy for the buyer to identify it

3. Blocks

A block is a set of transactions and block is the smallest unit of the distributed ledger. Each block[6][12][14] contains a set of transactions with the digital signatures of the owners hence a block contains legitimate. A block contains list of transactions, a timestamp which is used to indicate that the transactions in the block are performed at the specified time, hash of the previous block in order to maintain the record of the order in which the transactions are performed and a proof-of-work value. These blocks are broadcasted all over the network and everyone gets a copy of the node and appends them to their respective chain.by this way we can achieve a distributed system



BLOCKs Structure

4. Proof-of-work

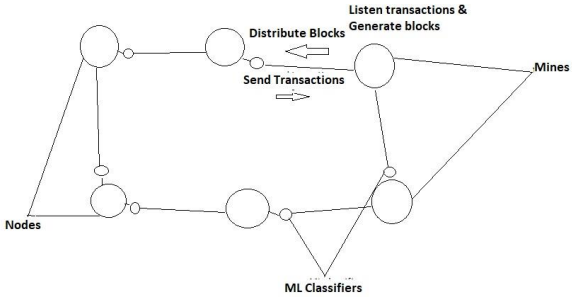
A proof-of-work[3][4][5] is a mechanism used to provide resistance to majority of attacks. In this case an attempt is made to find a value such that the SHA-256 hash of the entire block along with this value follows a particular pattern(like first 4 digits of the hash of every block should contain 0's).All the blocks in block chain should follow this pattern. As all the blocks are chained i.e., each block contains the hash of previous block, if an attacker wants to modify the transactions he must redo all the proof-of-works along the length of the chain and it is an impossible task.

Miners responsibility[12] is to do mining activity, the process of generating proof-of-work is called mining. Miners listen to the transactions in the network collect them make them into block, put timestamp, perform proof-of-work and distribute them through the network. This activity is of proof-of-work is done for every regular intervals of time based on CPU power.

The mining activity is done by a Government authority. As long as the computational power of honest nodes (government authority) is greater than the attacker nodes when can ensure safety. All the Government miners also compete among themselves to maintain a secure system.

5. Consensus algorithm

Consensus algorithm[16] is used for accepting a block of branch of the block chain which is large in length. Whenever a new block is obtained we do not simply accept it but simply wait until that branch is long enough to be legitimate. When there are conflicting blocks waiting for some time and accept the branch with longest length. As a result, if an attacker has to distribute the forged block he must constantly compete with the honest miners to keep his branch of the chain larger than the legitimate branch and this requires a large amount of computational power. This mechanism provides safety until the computational power of honest nodes is greater than the attacker nodes.



6. Machine learning Classifier

By placing ML classifier[7][8][9][10] in every node the system becomes more robust in identifying and classifying any malicious transactions or virus etc. The ML classifiers are trained using machine learning tools. The trained classifier used to identify virus by static analysis before accepting any transaction or executable file is statically scans and identify conflicting operations and identify patterns among them and classify them into malicious or benign if begin allows it else notifies the network about the possible attack.

7. Network

Therefore, the network should have the following characteristics

1. New transactions are broadcasted in the network
2. Every transaction must be digitally signed.
3. Miners listens them creates block with previous hash, timestamp and performs proof of work and distribute in the network.
4. Every node must perform consensus algorithm and accept only the longest branch of the chain.
5. Every node must contain machine learning classifier to identify and classify any potential threat to the system.

8. Conclusion

By eradicating central authority (except for mining) there will be fewer chances of corruption and hacking, this mechanism provides a transparent system and reduces the chances of forgery. The system provides resistance to various cyber-attacks. Even in the case of mine attack, detection will be done by the machine learning classifier even if the attack was successful the other mines can compensate it. An attacker cannot modify any data in the chain because he redo all the proof of work. Machine learning classifier can prevent the man in the middle attack and even if the attack is possible as long as the computational power of the honest nodes is greater it is nearly impossible to do so.These make the system a secure way to perform transactions.

References

[1] F.F. Wu, K. Moslehi and A. Bose, "Power system control centers: Past, present, and future," *Proc. IEEE*, vol. 93, no. 11, pp. 1890–1908, 2005.

[2] F. Luo, J. Zhao, Z.Y. Dong, Y. Chen, Y. Xu, X. Zhang and K.P. Wong "Cloud-based information infrastructure for next-generation power grid: conception, architecture, and applications," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1896–1912, Jul. 2016.

[3] NCCIC/ICS-CERT, "Cyber-attack against Ukrainian critical infrastructure," released 25 February 2016. [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 [Accessed: 22 Jan. 2018].

[4] E-ISAC and SANS, "Analysis of the cyber attack on the Ukrainian power grid: Defense use case," released 18 March 2016. [Online]. Available: https://ics.sans.org/duc5 [Accessed: 22 Jan. 2018].

[5] G. Liang, S.R. Weller, J. Zhao, F. Luo and Z. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[6] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. and Syst. Security (TISSEC)*, vol. 14, no.1, May 2011.

[7] G. Liang, J. Zhao, F. Luo, S.R. Weller, and Z. Dong. "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630 – 1638, Jul. 2017.

[8] R. Deng, G. Xiao, R. Lu, H. Liang and A.V. Vasilakos, "False data injection attack on state estimation in power systems – attacks, impacts, and defense: A survey," *IEEE Trans. Industrial Informatics*, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[9] O. Kosut, L. Jia, R.J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Oct. 2011.

[10] Raman Dugyala,N Hanuman Reddy,N Chandra Shaker reddy,J Phani prasad "A Roadmap to Security in IoT" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 19 (2017) pp. 8270-8272

[11] Raman Dugyala, Bruhadeshwar Bezawada, Rajini Kanth V. Thatiparthi, Sai Sathyanarayan "Static Program Behavior Tracing for Program Similarity Quantification" Proceedings of the First International Conference on Computational Intelligence and Informatics Volume 507 of the series Advances in Intelligent Systems and Computing pp 321-330 DOI 10.1007/978-981-10-2471-9_31 Print ISBN 978-981-10-2470-2 Online ISBN 978-981-10-2471-9,May 2016

[12] Raman Dugyala, Prashanthi Muddam "Graphical Password Authentication for Secure Online Services" International Research Journal of Engineering and Technology ,Vol 3, Issue 8,Aug 2016

[13] Shojafar, M.; Cordeschi, N.; Baccarelli, E. Energy-efficient adaptive resource management for real-time vehicular cloud services. IEEE Trans. Cloud Comput. 2016. [CrossRef]

[14] Javanmardi, S.; Shojafar, M.; Shariatmadari, S.; Ahrabi, S.S. Fr Trust: A fuzzy reputation based model fortrust management in semantic P2P grids. Int. J. Grid Util. Comput. 2015, 6, 57–66. [CrossRef]

[15] Du, Q.H.; Li, W.Y.; Song, H.B. Security enhancement via dynamic fountain code for wireless multicast. In Proceedings of the International Conference on Wireless Algorithms, Systems, and Applications, Guilin, China, 27 May 2017; pp. 509–521

[16] K Suma Rani, D Raman "A Study Of Cross Site Scripting Compulsion Against Web Applications" International Journal of Eminent Engineering Technologies",Vol 2, Issue 3,Apr 2015