© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 13 Issue: 02 | April - June 2022
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Peer Reviewed

Design of a Blockchain Based Security Model For IPV6 Addressing Communication

Harshal Wankar
Computer Science and Engineering
St. Vincent Pallotti College of Engineering & Technology, Nagpur, India
harshalwankar100@gmail.com.

Guided By,
Prof. R.C. Roychaudhary
Assistant Professor

***Abstract* -- Security plays a vital role in the design of any data & process intensive system, where in data must be communicated in such a manner that only the intended entities should be able to decode and understand it. In order to provide security, various protocols and security models have been developed by researchers, these include, encryption models, hashing models, public key infrastructure systems, Blockchain systems, secret sharing systems, etc. All these systems have their own nuances, advantages and limitations, which makes it difficult for system designers to select the most optimum security models for their designed application. For instance, security systems that are delay sensitive should be able to secure data at high speed with low complexity, but this property might reduce the system's security performance. In order to reduce the ambiguity of security protocol selection, this report evaluates statistical performance of different security systems in terms of operating speed, security level, quality of service, and applicability. Blockchain based systems incorporate encryption, hashing, key sharing, and other security steps, thus these systems are primarily discussed in this work. Apart from Blockchain systems, security can also be improved via efficient data distribution using secret sharing mechanisms. Therefore, this report also evaluates security performance of secret sharing mechanisms and evaluates their performance on different applications. It is observed that combination of blockchain with secret sharing mechanisms paves the way for future security systems, that possess high QoS and high security performane.**

***Keyword*--Blockchain, secret sharing, encryption, hashing, public key infrastructure.**

I. Introduction

Security is a significant concern for a wide range of network systems. For high security applications like banking, the need to make sure that secure information outperforms the need to advance the capacity cost, computational expense and even the running expense of the frameworks. So as to plan an IPv6 based security framework that satisfies all the above constraints, scientists have created effective procedures like blockchains and peer computing.

Blockchains work utilizing a straightforward P2P standard, which depends on agreement-based check. The most widely recognized case of a blockchain based IPv6 arrange is the Ethereum blockchain. Ethereum stores its value-based information on low controlled and computationally light weighted IPv6 network nodes via contracts.

In view of these boundaries a blockchain framework's intricacy can be tuned. For IPv6 security, a lower multifaceted agreement calculation, alongside lower intricacy mining and cryptographic calculations can be chosen. The magnificence of blockchain is that its security isn't subject to the unpredictability of the calculations, yet the quantity of IPv6 network nodes in the system can increase. Hence, an oversimplified blockchain execution is sufficient for an enormous IPv6 organization.

II. Literature Review

Data security is a complicated domain that requires effective implementation of complex mathematical models that convert input data from one format to another during transmission, and then convert it back into an understandable (usually original) format during reception. These security schemes are under constant analysis by ethical and non-ethical hacking entities, who aim at leveraging security loop holes in these systems. These loop holes assist researchers to develop better security models, thereby reducing the probability of future attacks. For instance, the work in [3] suggests a common vulnerability that occurs when storing large data with trusted third parties, wherein random data division is used in order to reduce probability of data identification & approximation attacks. But due to random division of data, the decoding unit takes a large amount of time for analysing exact data share positions, thereby reducing overall speed of operation for the system. This delay can be reduced via the use of neural cryptography, wherein Hebbian learning is used in order to synchronize input vectors between sending and receiving entities. These entities generate identical output bit sequences, and are trained using these sequences. This allows the systems to reduce calculation delays for evaluating share positions, thereby increase overall data communication speed, while maintaining high level of security. The architecture for neural key exchange protocol can be observed from figure 2.1, wherein Shamir (k, n) algorithm is responsible for generating 'n' shares. Each of these shares are encrypted via 'n' individual keys generated by the neural key exchange protocol. The protocol uses a combination of Hebbian Algorithm along with Tree Parity Machine, where the output is controlled using the following equation,

$$\partial = \prod_{i=1}^{k} sign(\sum_{j=1}^{n} rand[-L, +L + 1] * x_{i,j}) \dots (1)$$

Where, ∂ is the output generated at both transmitter and receiver side, 'L' is the range for each of the weights, 'k' is hidden number of neurons, 'n' is number of neurons which are connected to the hidden neuron, and 'x' is the input to the system, Signum(sign) is the activation function. This output is given to the Hebbian algorithmic transform, which evaluates the output weights for both transmitter and receiver sides using the following equation,

$$W_{ij_{interm}} = W_{ij_{old}} + X_{ij} * \partial * \emptyset \dots (2)$$

Where, $W_{ij_{old}}$ are the old weights, X_{ij} is the input of the sending or receiving unit, ∂ is evaluated from equation 1, while $\emptyset$ is an equality constant. The new value of weight is evaluated from this intermediate $W_{ij_{interm}}$ value, using the following equation,

$$W_{ij_{new}} = sign\left(W_{ij_{interm}}\right) * L \dots (3)$$

This value of weight is used for key generation at both transmitter and receiver sides, which keeps them in synchronization. But in order to provide this synchronization, it is necessary that constants like 'k', 'n', and, 'L' must be securely communicated between the communicating entities.

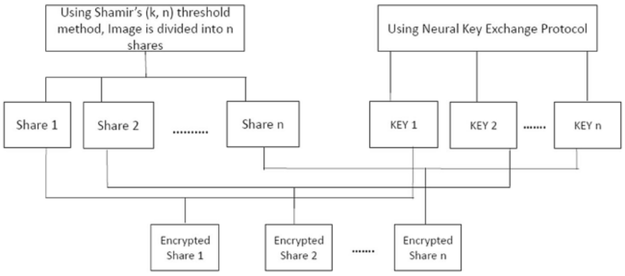

Figure 2.1: Neural key exchange for reducing delay of synchronization.

- Initially user generates an authentication request to the gateway node.
- Gateway node requests blockchain network to send privacy policies to the authenticating user.
- The user node agrees to these policies, and sends an agreement token.
- The agreement token is verified by the blockchain network, and the gateway node informed about this token.
- Once the token is authenticated by the gateway node, then the gateway provides an access token to the user for accessing specific information from the IPv6 device.
- Details about this information access token, and the accessed information is updated on the blockchain for future tracking and analysis.

Due to this overall security is improved, and delay of communication is reduced. But this protocol does not support ownership transfer, which can be researched and added to the system for improving its real time deploy-ability.

In real-time use cases, a single authentication must be able to perform multiple transactions, wherein processes like registration, communication, validation and access control must be carried out. In order to perform this task, the work in proposes a blockchain-cloud fusion scheme, via Decentralized Attribute-Based Signature mechanism. This mechanism is able to perform data sharing across multiple entities, thereby facilitating multi-transaction interface for users.

III. Blockchain.

In recent years Blockchain technology got more attention because of its Blockchain is a decentralised, distributed, immutable digital ledger. As this is decentralised mechanism for storing transactions; there is no central authority involves in it. These transactions are stored in the form of blocks and chain of these blocks form the blockchain. The size of the blockchain keeps on increasing as an when blocks are added to the chain. Since this technology avoids the need of third parties or intermediaries; it is used in various application domains like finance, digital assets, Insurance sector, Supply chain, healthcare, Internet of Things (IPV6) and so on. he drawback of single point of failure in case of centralised system can be removed with the use of decentralised, Peer-to-Peer(P2P) blockchain system.

A. Blockchain Architecture:

In this each user acts as a node who is responsible for performing various operations like initiating and validating transactions. All these nodes are connected with each other in a decentralised fashion as shown in figure 3.1. Each node has a copy of blockchain maintained with them which keeps on updating on regular basis.

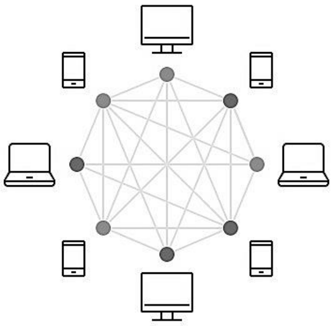

Figure 3.1 Blockchain architecture

B. Block Structure

The sequence or Chain of blocks form the blockchain. In this any block can initiate transaction and broadcast this transaction to all nodes in a network. Network nodes perform validation of the transaction. Number of transactions occurring at one particular time are grouped together to form the block and this block is then added into the blockchain.

Each block is made up of two parts namely block header and block body. Block header is the metadata of the block and is made up of following components as shown in figure 3.3:

a. Block version: I It tells which set of block validation rules to follow
b. Merkle tree root hash: the hash computed from all the transactions in the block.
c. Timestamp: current time
d. Nonce: It is 4-byte field, which usually starts with 0 and increases for every hash calculation
e. Previous block hash: 256-bit hash of previous block is computed and inserted in new block in the blockchain which makes the blockchain tamperproof.

The block body is made up of a transaction counter and transactions. Depending upon the size of block and size of each transaction one can decide number of transactions the block can have. The authentication of transactions in blockchain is done by using asymmetric cryptography mechanism.

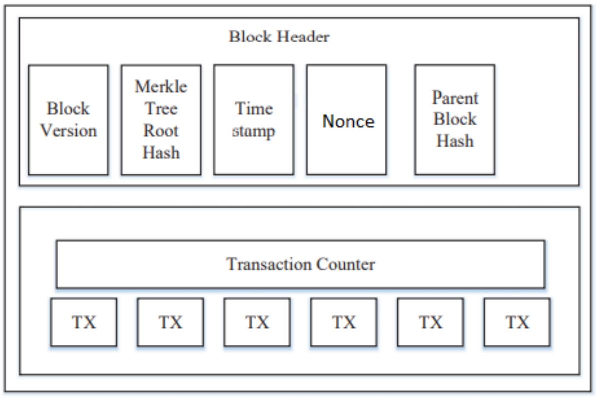

Figure 3.2: Block structure

IV. Motivation

Due to the advent of blockchain technologies, it is evident that future security models will be based on it. Moreover, blockchain has some inherent issues, which relate to its scalability, and data sharing capabilities, which can be solved in order to generate high efficiency networks while maintaining high security performance. Also, data ownership transfer is a big issue when the highly sensitive and valuable information is to be unconditionally or conditionally transferred to other parties. Therefore, the motivation of this work is to design such a system that can be helpful in improving blockchain performance via the use of PoW consensus, that will assist in enhancing security performance of the IPv6 network.

The following are the objectives of our research,

- To study different blockchain and machine learning architectures in order to select the most effective combination that provides good security with high QoS
- To design a blockchain network that can be applied to IPv6 networks
- Optimize the system for fine tuning of system parameters.

In order to define the scope of this work, the following aims have been pre-set,

- Design of blockchain networks and assess their QoS & security performance.
- Optimize the system for fine tuning of system parameters.

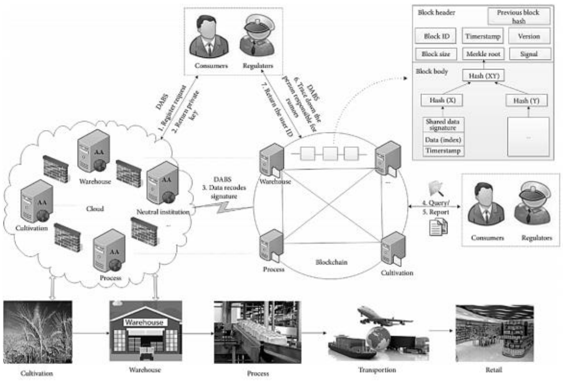

Figure IV.1. A multi-transaction interface using DABS mechanism.

This model is able to reduce overall delay by 15% when compared to a non-edge computing model, and also reduces network overhead by 10% due to computation offload on edge devices. This concept can also be extended for enhancing blockchain based data storage & recovery performance using distributed verification as suggested in. The work uses a fault-tolerant distributed storage architecture, wherein redundant data values are stored across a distributed series of nodes. The nodes are updated with redundant data at regular intervals, thereby facilitating effective fallback in case of node failures due to network attacks. The network is resilient to single and multiple node failures, and is able to correctly regenerate data from multiple nodes using random data selection process. Due to this, there an improvement of 15% in the overall data repair rate, when compared with hierarchical & multi-node exact repair methods.

Other schemes for enhancing authentication and validation performance of blockchain can be observed from and, wherein identity based secure and verifiable data sharing schemes are described. These schemes assist in improving overall network security performance, and allow the system to provide better access control via the usage of fine-grained access flags for the system.

V. Result

From the reviewed approaches, it can be observed that current blockchain systems either lack in terms of QoS, or security performance or data access control. Thus, our problem definition is to develop a highly secure data access system it is necessary to design a stochastic data division protocol with blockchain support. This will allow for application to IPv6 networks. In order to control system QoS performance, a blockchain model will be integrated in the system that will allow for automatic retuning of system parameters like block length, chain division thresholds, etc. This will assist in improving overall security and QoS performance of the network, and make it context-aware depending upon the application for which the network is being designed.

Following are the possible contributions of this work,

- Identification of the most efficient blockchain architectures for improving network security
- Identification of the most effective data division models for better access performance.
- Design of a blockchain network that can be implemented for IPv6 networks.

Based on this, the following flow can be used,

- IPv6 network deployment will be done in order to establish node to node communication
- Central Blockchain will be deployed for better trust levels in the network.
- Central blockchain will be divided into blockchains using IPv6 model.
- The model will be used to further optimize system performance (if needed)

VI. Conclusion.

From the result analysis it can be observed that blockchain and secret sharing models have good security performance, but have limited QoS performance. This QoS performance can be improved via the use of machine learning models like reinforcement learning, incremental learning, LSTM-based learning, etc. All these models can be integrated with concurrent processing to further improve its QoS performance. Furthermore, computational complexity of these models is usually high, which can be reduced via the use of blockchain sharding, wherein a single blockchain is divided into multiple chains in order to reduce mining and verification delays. Moreover, there are limited systems that combine blockchain with secret sharing models, thus one must design systems that combine these models for improved security with reduced complexity and high QoS performance for real-time systems.

VII. Reference

[1] Mohanta, Bhabendu & Jena, Debasish & Panda, Soumyashree & Sobhanayak, Srichandan. (2019). Blockchain Technology: A Survey on Applications and Security Privacy Challenges. 8. 100107. 10.1016/j.IPv6.2019.100107.

[2] Sarosh, Parsa & Parah, Shabir & Bhat, Gm. (2021). Utilization of secret sharing technology for secure communication: a state-of-the-art review. Multimedia Tools and Applications. 80. 1-25. 10.1007/s11042-020-09723-7.

[3] Ghasemi, R. Resolving a common vulnerability in secret sharing scheme–based data outsourcing schemes. *Concurrency Computat Pract Exper*. 2020; 32:e5363. https://doi.org/10.1002/cpe.5363

[4] Gupta, M., Gupta, M. & Deshmukh, M. Single secret image sharing scheme using neural cryptography. *Multimed Tools Appl* **79,** 12183–12204 (2020). https://doi.org/10.1007/s11042-019-08454-8

[5] Abidi, MH, Alkhalefah, H, Umer, U, Mohammed, MK. Blockchain-based secure information sharing for supply chain management: Optimization assisted data sanitization process. *Int J Intell Syst*. 2021; 36: 260- 290. https://doi.org/10.1002/int.22299

[6] Gupta, R, Kumari, A, Tanwar, S. Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications. *Trans Emerging Tel Tech*. 2021; 32:e4176. https://doi.org/10.1002/ett.4176

[7] Mostafa Yavari, Masoumeh Safkhani, Saru Kumari, Sachin Kumar, Chien-Ming Chen, "An Improved Blockchain-Based Authentication Protocol for IPv6 Network Management", *Security and Communication Networks*, vol. 2020, Article ID 8836214, 16 pages, 2020. https://doi.org/10.1155/2020/8836214

[8] Menghui Lou, Xiaolei Dong, Zhenfu Cao, Jiachen Shen, "SESCF: A Secure and Efficient Supply Chain Framework via Blockchain-Based Smart Contracts", *Security and Communication Networks*, vol. 2021, Article ID 8884478, 18 pages, 2021. https://doi.org/10.1155/2021/8884478

[9] Azees Maria, Vijayakumar Pandi, Jeatha Deborah Lazarus, Marimuthu Karuppiah, Mary Subaja Christo, "BBAAS: Blockchain-Based Anonymous Authentication Scheme for Providing Secure Communication in VANETs", *Security and Communication Networks*, vol. 2021, Article ID 6679882, 11 pages, 2021. https://doi.org/10.1155/2021/6679882

[10] Teng Li, Jiawei Zhang, Yangxu Lin, Shengkai Zhang, Jianfeng Ma, "Blockchain-Based Fine-Grained Data Sharing for Multiple Groups in Internet of Things", *Security and Communication Networks*, vol. 2021, Article ID 6689448, 13 pages, 2021. https://doi.org/10.1155/2021/6689448

[11] Yan Wang, Jixin Li, Wansheng Liu, Aiping Tan, "Efficient Concurrent Execution of Smart Contracts in Blockchain Sharding", *Security and Communication Networks*, vol. 2021, Article ID 6688168, 15 pages, 2021. https://doi.org/10.1155/2021/6688168

[12] Deepak Prashar, Nishant Jha, Muhammad Shafiq, Nazir Ahmad, Mamoon Rashid, Shoeib Amin Banday, Habib Ullah Khan, "Blockchain-Based Automated System for Identification and Storage of Networks", *Security and Communication Networks*, vol. 2021, Article ID 6694281, 7 pages, 2021. https://doi.org/10.1155/2021/6694281

[13] Q. Tao, Q. Chen, H. Ding, I. Adnan, X. Huang, X. Cui, "Cross-Department Secures

Data Sharing in Food Industry via Blockchain-Cloud Fusion Scheme", *Security and Communication Networks*, vol. 2021, Article ID 6668339, 18 pages, 2021. https://doi.org/10.1155/2021/6668339

[14] S. Buda et al., "Empowering Blockchain in Vehicular Environments With Decentralized Edges," in IEEE Access, vol. 8, pp. 202032-202041, 2020, doi: 10.1109/ACCESS.2020.3036399.

[15] W. Liang, Y. Fan, K. -C. Li, D. Zhang and J. -L. GaudIPv6, "Secure Data Storage and Recovery in Industrial Blockchain Network Environments," in IEEE Transactions on Industrial Informatics, vol. 16, no. 10, pp. 6543-6552, Oct. 2020, doi: 10.1109/TII.2020.2966069.

[16] K. Fan et al., "A Secure and Verifiable Data Sharing Scheme Based on Blockchain in Vehicular Social Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5826-5835, June 2020, doi: 10.1109/TVT.2020.2968094.