International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Blockchain Architecture with Sliding Windows for the Internet of Things

Ms.M.ANITHA[1], Mr. CH. SATYANARAYANA REDDY [2], Ms.SHAIK RAMEEJA [3]

#1Assistant professor in the Master of Computer Application in the SRK Institute of Technology, Enikepadu, Vijayawada, NTR District

#2Assistant professor in the Master of Computer Application in the SRK Institute of Technology, Enikepadu, Vijayawada, NTR District

#3MCA student in the Master of Computer Application at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District

ABSTRACT_ The Internet of Things (IoT) is the concept of connecting non-traditional computers and related sources through the internet. This entails embedding everyday computing and communication technology into physical objects. Security and confidentiality are two important concerns with the Internet of Things. The constraints in the memory, energy resources, and CPU of IoT devices threaten the important security specifications in IoT devices in the present security mechanisms available for IoT. Furthermore, centralised security systems are unsuitable for IoT due to a single point of failure. It is expensive to guard against attacks on centralised infrastructure. As a result, it is critical to decentralise the IoT security architecture in order to fulfil resource restrictions. Blockchain is a decentralised encryption scheme with numerous applications. The Traditional Blockchain ecosystem, on the other hand, is unsuitable for IoT applications due to its high processing complexity and inadequate scalability. As a result, we add a Sliding window protocol to standard blockchain to better suit applications in the IoT context. By altering the traditional blockchain and introducing a sliding window, past blocks in proof of work are used to shape the next hash block. SWBC results are analysed in real-time on a data stream generated by an IoT testbed (Smart Home). The results show that the suggested sliding window technique increases security while reducing memory overhead and consuming less resources.

1.INTRODUCTION

A distributed ledger called a blockchain is used to keep track of transactions between two or more parties. Blockchains, in contrast to relational database systems, are data structures in which new entries are added at the end of the ledger and do not have administrator permissions that permit data modification. Additionally, every other party needs to use a consensus algorithm to verify the addition of a new block to the chain. When compared to a relational database system, the blockchain has distributed control, making it difficult for hackers to alter the data. Social data sets are fundamentally intended for concentrated information capacity and blockchain are explicitly intended for decentralized information capacity. There are two distinct kinds of blockchains: I) permissioned and (ii) permissionless. A permissioned blockchain is a private blockchain which requires pre-confirmation of the members inside the organization who are expected to know one another while, a permissionless blockchain is a public blockchain [1]. Customary blockchain approach isn't suitablefor IoT with constant information streams because of their computationally perplexing Confirmation of-Work (PoW) [2]. As the computational time increments, blockchain security becomes infeasible to be utilized for IoT. The two significant difficulties engaged with applying blockchain to IoT conditions include: (i) scalability and computational complexity The computational intricacy relies upon trouble level and Merkle tree size. The Merkle tree is a tree in which the hash of a transaction data is labeled on every leaf node, and the cryptographic hash of the labels of its child nodes is labeled on every non-leaf node. Merkle tree develops with the quantity of exchanges made and, subsequently, expanding the time consumed for Confirmation of-Work, which is less good for an IoT organization. The limit on how many transactions a blockchain can process in a given amount of time is referred to as scalability. A well-known illustration of a blockchain is Bitcoin. Bitcoin blockchain is an installment framework that doesn't depend on a focal power to supply secure and control its cash. The size of a block in a Bitcoin blockchain is limited. A block is mined every ten minutes in Bitcoin, and the block size is limited to 1 MB. Strangely, the current writing [3] proposes blockchain as one of the information security and protection calculations that can be executed for IoT applications because of its dispersed engineering. In this paper, we propose a new blockchain engineering for IoT conditions, particularly with regards to brilliant home applications. The state of a smart home is monitored, analyzed, and reported on. Savvy homes use gadgets associated with IoT to computerize and screen in-home frameworks [4]. Savvy home can be considered as the littlest unit of a shrewd city. The security normalization of a brilliant home backings a shrewd city as well as the other way around. In a savvy home, the constant information streams are created by sensors which assist us with observing the ongoing status of the home, dissect energy utilization, and examine any mishaps inside a shrewd home. The frequency of data acquisition and the number of sensors used in a smart home determine the volume of data generated. Consequently, appropriate examining of sensor information is expected to create significant data which can be subsequently put away in the blockchain. The packet overhead, memory overhead, and computational overhead of a blockchain are determined by the volume of data stored therein. Our proposed sliding window blockchain architecture aims to reduce the memory overhead of IoT in a smart home environment and improve security in this context.

2.LITERATURE SURVEY

[1] T. M. F. Carames and P. F. Lamas, "A review on the use of blockchain for the Internet of Things," IEEE Access, vol. 6, pp. 32 979–33 001, May 2018

In the last few years, we have witnessed the potential of Internet of Things to deliver exciting services across several sectors, from social media, business, intelligent transportation and smart cities to the industries [1], [2], [3]. IoT seamlessly interconnects heterogeneous devices with diverse functionalities in the human-centric and machine-centric networks to meet the evolving requirements of the earlier mentioned sectors. Nevertheless, the significant number of connected devices and massive data traffic become the bottleneck in meeting the required Quality-of-Services (QoS) due to the computational, storage, and bandwidth-constrained IoT devices. Mostrecently, the blockchain [4], [5], [6], [7], a paradigm shift, is transforming all the major application areas of IoT by enabling a decentralized environment with anonymous and trustful transactions. Combined with the blockchain technology, IoT systems benefit from the lower operational cost, decentralized resource management, robustness against threats and attacks, and so on. Therefore, the convergence of IoT and blockchain technology aims to overcome the significant challenges of realizing the IoT platform in the near future. Blockchain, a distributed append-only public ledger technology, was initially intended for the cryptocurrencies, e.g., Bitcoin1 . In 2008, Satoshi Nakamato [8] introduced the concept of blockchain that has attracted much attention over the past years as an emerging peer-to-peer (P2P) technology for distributed computing and decentralized data sharing. Due to the adoption of cryptography technology and without a centralized control actor or a centralized data storage, the blockchain can avoid the attacks that want to take control over the system. Later, in 2013, Ethereum, a transaction-based state-machine, was presented to program the blockchain technologies. Interestingly, due to its unique and attractive features such as: transactional privacy, security, the immutability of data, auditability, integrity, authorization, system transparency, and fault tolerance, blockchain is being applied in several sectors beyond the cryptocurrencies. Some of the areas are identity management [9], intelligent transportation [10], [11], [12], [13], [14], [15], supply-chain management, mobile-crowd sensing [16], agriculture [17], Industry 4.0 [18], [19], Internet of energy [20], [21], [18], [22], and security in mission critical systems [23]. As shown in Fig. 1, the blockchain structure is composed of a sequence of blocks, which are linked together by their hash values. In the blockchain network, a public ledger maintains the digitally signed transactions of the users in a P2P network. In general, a user has two keys: a public key for other users for the encryption and a private key to read an encrypted message, as shown in Fig. 2. From the blockchain perspective, the private key is used for signing the blockchain transaction and the public key represents the unique address. Asymmetric cryptography is used to decrypt the message encrypted by the corresponding public key. At the initial stage, a user signs a transaction using its private key and broadcasts it to its peers. Once the peers receive the signed transaction, they validate the transaction and disseminate it over the network. All the parties who are involved in the transactions mutually validate the transaction to meet a consensus agreement. Once a distributed consensus is reached, the special node, called as miners, includes the valid transaction into a timestamped block. The block, which is included by the miner, is broadcast back into the network. After validating the broadcast block, which contains the transaction, as well as hash-matching it with the previous block in the blockchain, the broadcast block is appended to the blockchain. Based on the data management and the type of applications, blockchain can classified either as private (permission) or public (permissionless). Both classes are decentralized and provide a certain level of immunity against faulty or malicious users for the ledger. The main differences between private and public blockchains lie in the execution of the consensus protocol, the maintenance of the ledger, and the authorization to join to the P2P network. Detailed examples of these classes are illustrated in [24]. In the context of IoT, blockchains can be classified based on authorization and authentication. As shown in Fig. 3, in a private blockchain, the centralized trusted authority that manages the authentication and authorization process selects the miners. On the other hand, in a public blockchain (in general, permissionless), there is no intervention of any thirdparty for the miner selection and joining for a new user to the blockchain network. Recently, there is a huge amount of investment from the industries [25], [26] as well as a significant interest from academia to solve major research challenges in blockchain technologies. For example, the consensus protocols are the major building blocks of the blockchain technologies, thus, the threats targeting the consensus protocols become a significant research issue in the blockchain. Furthermore, blockchain forks bring threats to the blockchain consensus protocols. Moreover, it is observed that the vulnerability is about 51% for a new blockchain [27]. At the same time, maintenance of several blockchains requires a significant amount of power consumption [28].

[2] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: challenges and solutions," arXiv preprint arXiv:1608.05187, August 2016.

The Internet of Things IoT is experiencing exponential growth in research and industry, but it still suffers from privacy and security vulnerabilities. Conventional security and privacy approaches tend to be inapplicable for IoT, mainly due to its decentralized topology and the resource-constraints of the majority of its devices. BlockChain BC that underpin the crypto-currency Bitcoin have been recently used to provide security and privacy in peer-to-peer networks with similar topologies to IoT. However, BCs are computationally expensive and involve high bandwidth overhead and delays, which are not suitable for IoT devices. This position paper proposes a new secure, private, and lightweight architecture for IoT, based on BC technology that eliminates the overhead of BC while maintaining most of its security and privacy benefits. The described method is investigated on a smart home application as a representative case study for broader IoT applications. The proposed architecture is hierarchical, and consists of smart homes, an overlay network and cloud storages coordinating data transactions with BC to provide privacy and security. Our design uses different types of BCs depending on where in the network hierarchy a transaction occurs, and uses distributed trust methods to ensure a decentralized topology. Qualitative evaluation of the architecture under common threat models highlights its effectiveness in providing security and privacy for IoT applications.

[3] L. Jiang, D. Y. Liu, and B. Yang, "Smart home research," in Proceedings of 2004 International Conference on Machine Learning and Cybernetics, vol. 2, August 2004, pp. 659–663.

Smart home is the integration of technology and services through home networking for a better quality of living. It uses different technologies to equip home parts for more intelligent monitoring and remote control and enabling them for influential harmonic interaction among them such that the everyday house works and activities are automated without user intervention or with the remote control of the user in an easier, more convenient, more efficient, safer, and less expensive way. In some cases, Integrating the home services as shown in fig. 1 [1] allows them to communicate with one another through the home controller, thereby enabling single button to control the various home systems according to preprogrammed scenarios or operating modes [2]. Smart homes have the potential to improve home comfort, convenience, security and energy management. Moreover it can be used for elder people and those with disabilities, providing safe and secure environments.

3.PROPOSED SYSTEM

In this paper author is describing concept to provide security to IOT devices using Blockchain technology as this technology supports decentralized data storage which means data will be stored at multiple nodes compare to centralized storage where data is stored at single centralized server. Decentralized data storage provides facility of receiving data from any available node and it has strong security where a single data store will verify hash value of all nodes. Verification of all nodes hash is computation intensive and its cannot be applied to IOT small devices due to memory, CPU and energy consumption restrictions.

To overcome from this problem author introduce Sliding window technique where the window size will be fixed and all Blockchain transaction hash values will be stored in window and if window size exceeded then old transaction blocks will be slided or removed and maintain only recent blocks due to this technique memory storage and data transfer overhead will be reduced.

In extension author is saying to further save energy so I am adding concept of monitoring data in time interval and if sensor generate same random data within time interval then IOT will not process that data to store in Blockchain and this duplicate avoidance can further save energy.

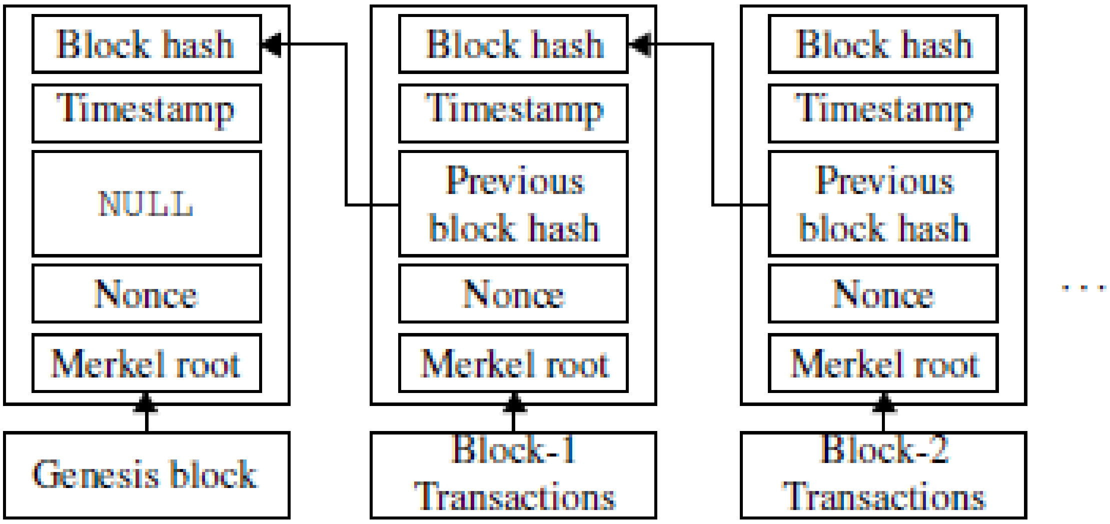
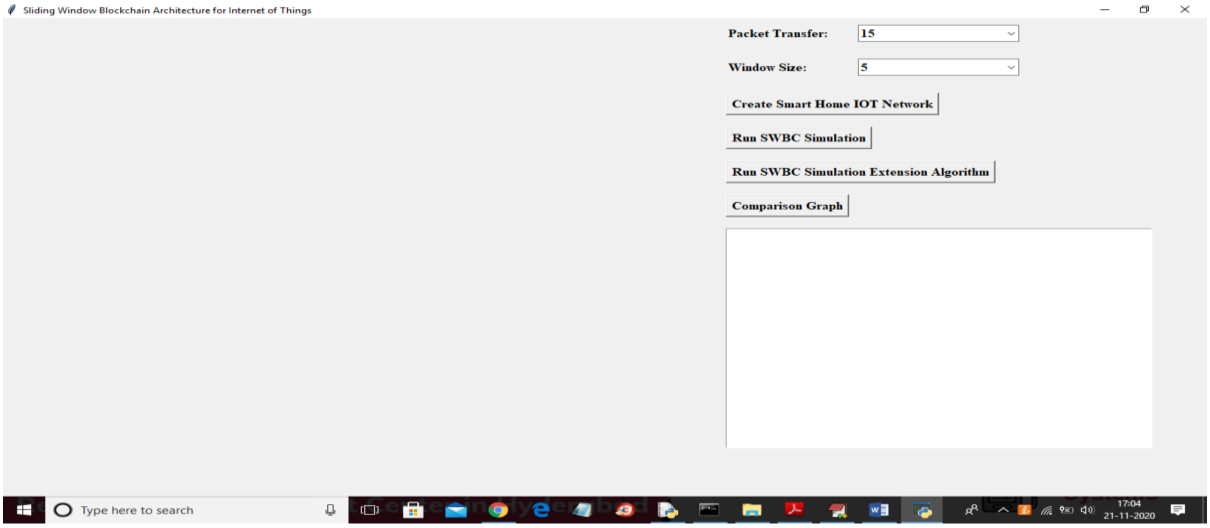


Figure 1: Blockchain architecture.

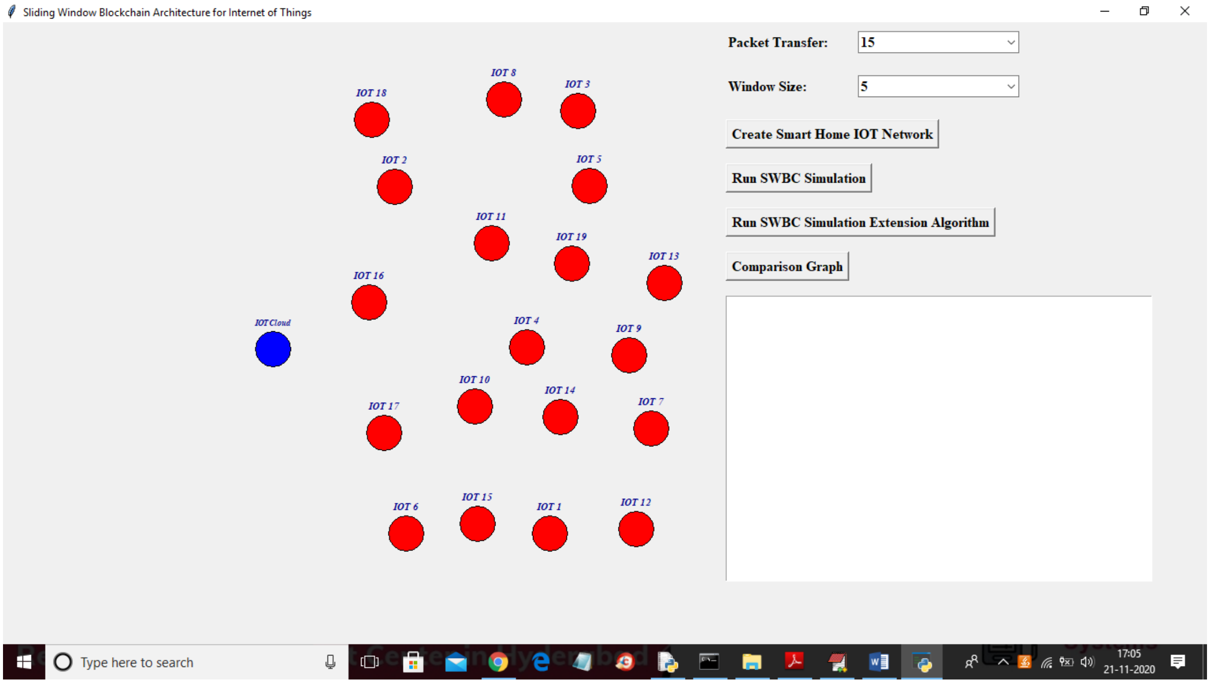
4.RESULTS AND DISCUSSION


Sliding Window Blockchain Architecture for Internet of Things

Packet Transfer: 15

Window Size: 5

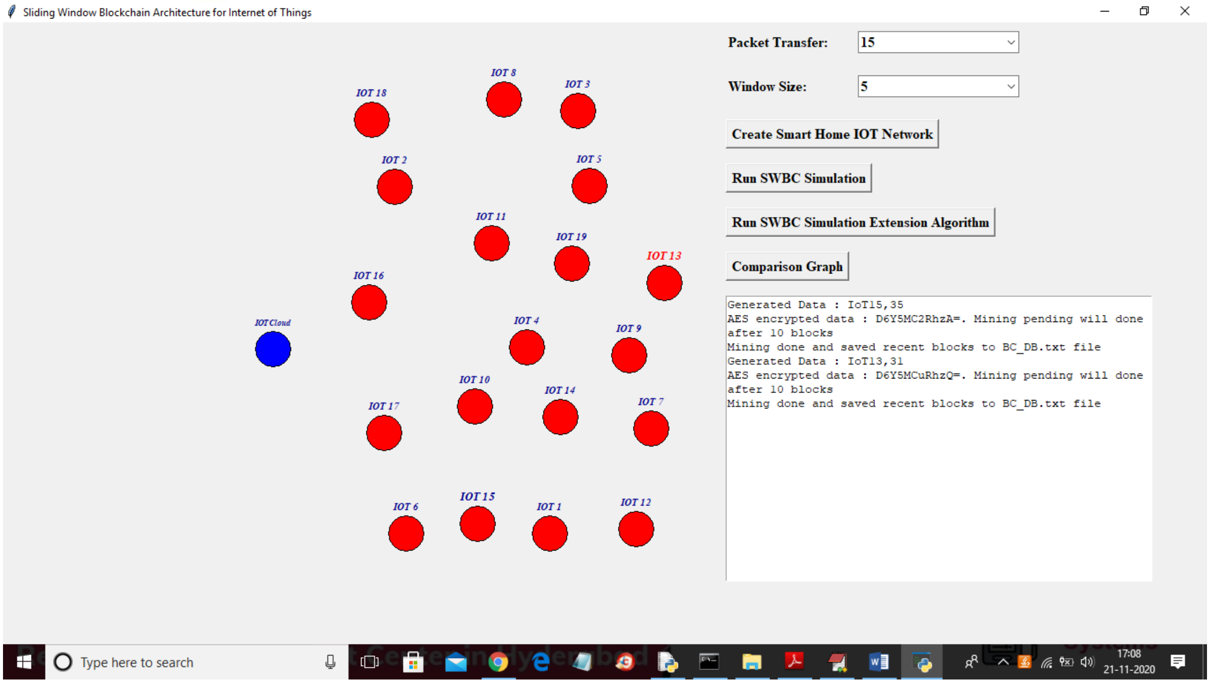
In above screen select number of packet transfer and then select window size as 5, 10 or 15 and then click on ‘Create Smart Home IOT Network’ button to get below screen


Sliding Window Blockchain Architecture for Internet of Things

Packet Transfer: 15

Window Size: 5

In above screen I selected number of packet transfer as 15 and window size is 5 and block chain can store data up to 5 blocks and if exceed then old block remove out and send to cloud for storage and new block will store in IOT memory. In above screen all red colour circles are home IOT and blue colour circle is the IOT cloud which will receive data from IOT upon IOT window full. Now click on ‘Run SWBC Simulation’ button to allow each circle to sense data randomly and while sensing circle label will change to red colour



Sliding Window Blockchain Architecture for Internet of Things

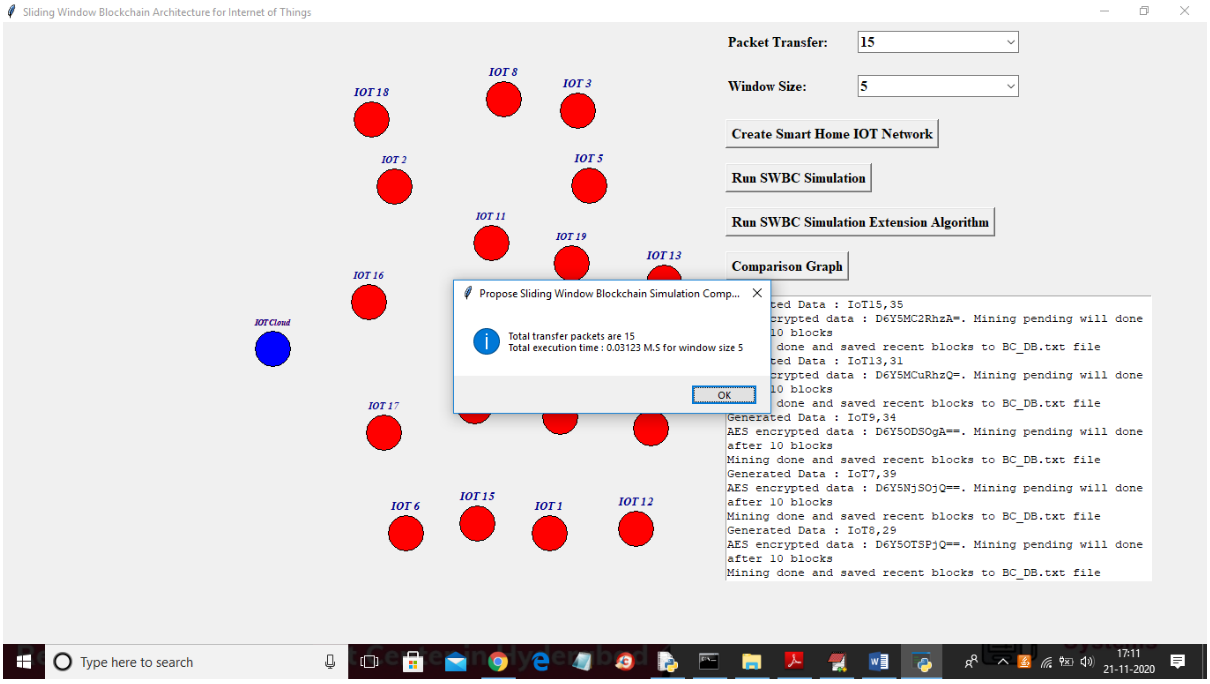
Packet Transfer: 15

Window Size: 5

```
Generated Data : IoT15,35
AES encrypted data : D6Y5MC2RhzA=. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : IoT13,31
AES encrypted data : D6Y5MCuRhzQ=. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
```

17:08
21-11-2020

In above screen IOT13 label is sensing data and its label colour change to red colour and this simulation will run for 15 packets transfer and for each transfer sensor will be chosen randomly. In text area we can see which IOT is sensing data and its sense value separated by comma symbol. In next line displaying AES encrypted data and then displaying mining is done or not and after simulation will get below screen



Sliding Window Blockchain Architecture for Internet of Things

Packet Transfer: 15

Window Size: 5

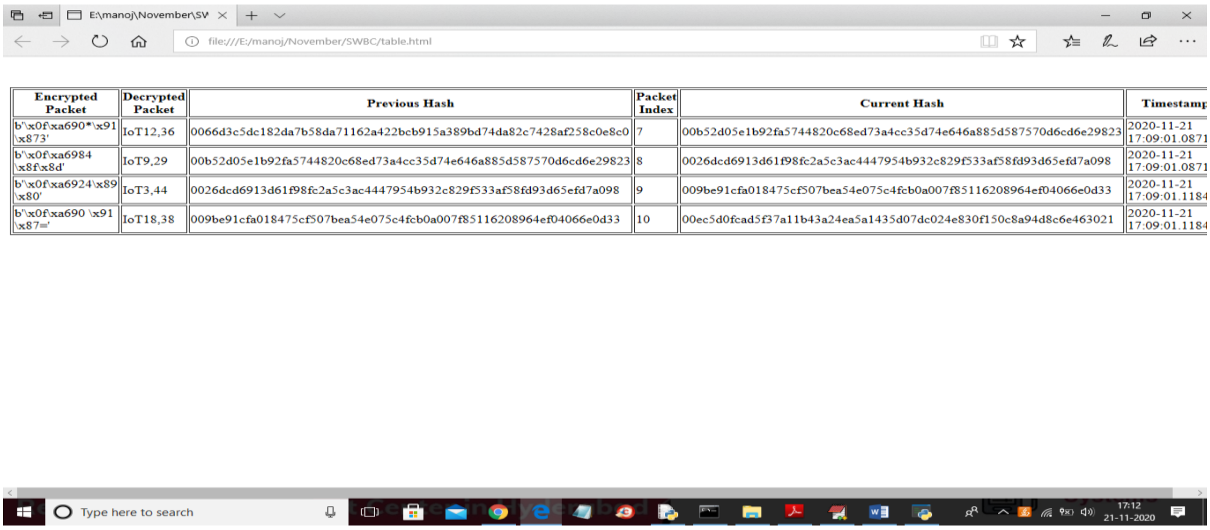
Propose Sliding Window Blockchain Simulation Comp...

Total transfer packets are 15
Total execution time : 0.03123 M.S for window size 5

```
ted Data : IoT15,35
crypted data : D6Y5MC2RhzA=. Mining pending will done
10 blocks
 done and saved recent blocks to BC_DB.txt file
ted Data : IoT13,31
crypted data : D6Y5MCuRhzQ=. Mining pending will done
10 blocks
 done and saved recent blocks to BC_DB.txt file
Generated Data : IoT9,34
AES encrypted data : D6Y5ODSOgA==. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : IoT7,39
AES encrypted data : D6Y5NjSOjQ==. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : IoT8,29
AES encrypted data : D6Y5OTSPjQ==. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
```

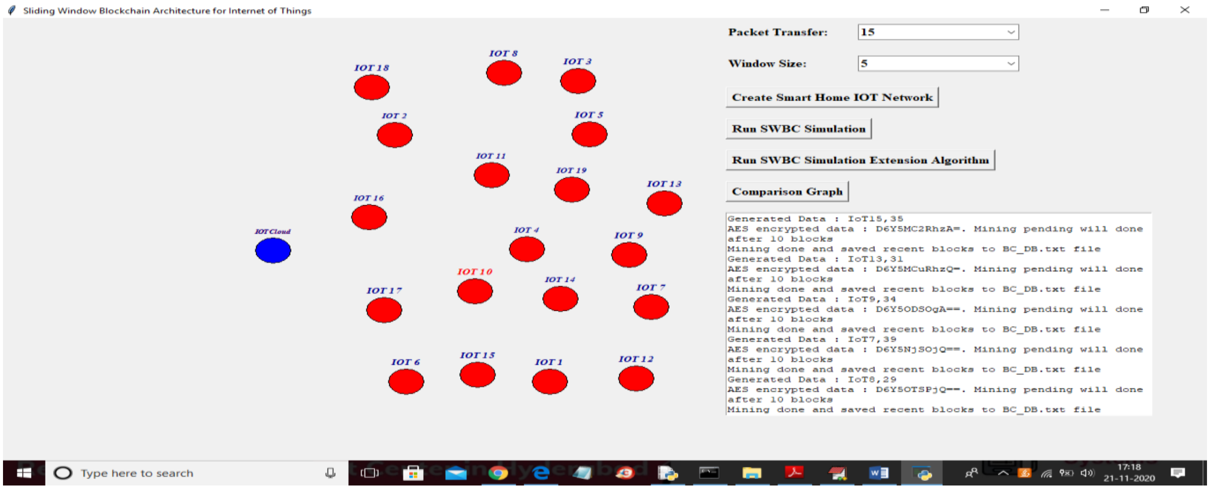
17:11
21-11-2020

In above screen after sending packets we will get above dialog box with total packets sense and send and it will display how much time it took to process that window size 5 and displaying total sense and send packets as 15. In below screen we can see latest recent blocks store at IOT memory



Encrypted Packet	Decrypted Packet	Previous Hash	Packet Index	Current Hash	Timestamp
b'\x0f\xa690*\x91 \x873'	IoT12,36	0066d3c5dc182da7b58da71162a422bcb915a389bd74da82c7428af258c0e8c0	7	00b52d05e1b92fa5744820c68ed73a4cc35d74e646a885d587570d6cd6e29823	2020-11-21 17:09:01.0871
b'\x0f\xa6984 \x8f\x8d'	IoT9,29	00b52d05e1b92fa5744820c68ed73a4cc35d74e646a885d587570d6cd6e29823	8	0026dcd6913d61f98fc2a5c3ac4447954b932c829f533af58fd93d65efd7a098	2020-11-21 17:09:01.0871
b'\x0f\xa6924\x89 \x80'	IoT3,44	0026dcd6913d61f98fc2a5c3ac4447954b932c829f533af58fd93d65efd7a098	9	009be91cfa018475cf507bea54e075c4fcb0a007f85116208964ef04066e0d33	2020-11-21 17:09:01.1184
b'\x0f\xa690 \x91 \x87='	IoT18,38	009be91cfa018475cf507bea54e075c4fcb0a007f85116208964ef04066e0d33	10	00ec5d0fcad5f37a11b43a24ea5a1435d07dc024e830f150c8a94d8c6e463021	2020-11-21 17:09:01.1184

In above screen as our window size was 5 and first block is empty for genesis and latest 4 records of IOT are displaying and in above screen in first column showing encrypted data then in second column decrypted data and then showing previous hash value and then block chain index value and then current hash value with time. In above screen we can see that block chain verify previous and current hash value. In above screen we can see current hash of first row is matched with previous hash of second row. In above screen with propose work we sense and store 15 packets and sometime IOT sensor will sense same data as temperature will not change for some intervals and if we send same data again and again then it waste processing time and increase overhead. We can avoid this overhead by monitoring data and If same data generate again then we will not process in extension work. Now click on 'Run SWBC Simulation Extension Algorithm' button to avoid duplicate processing

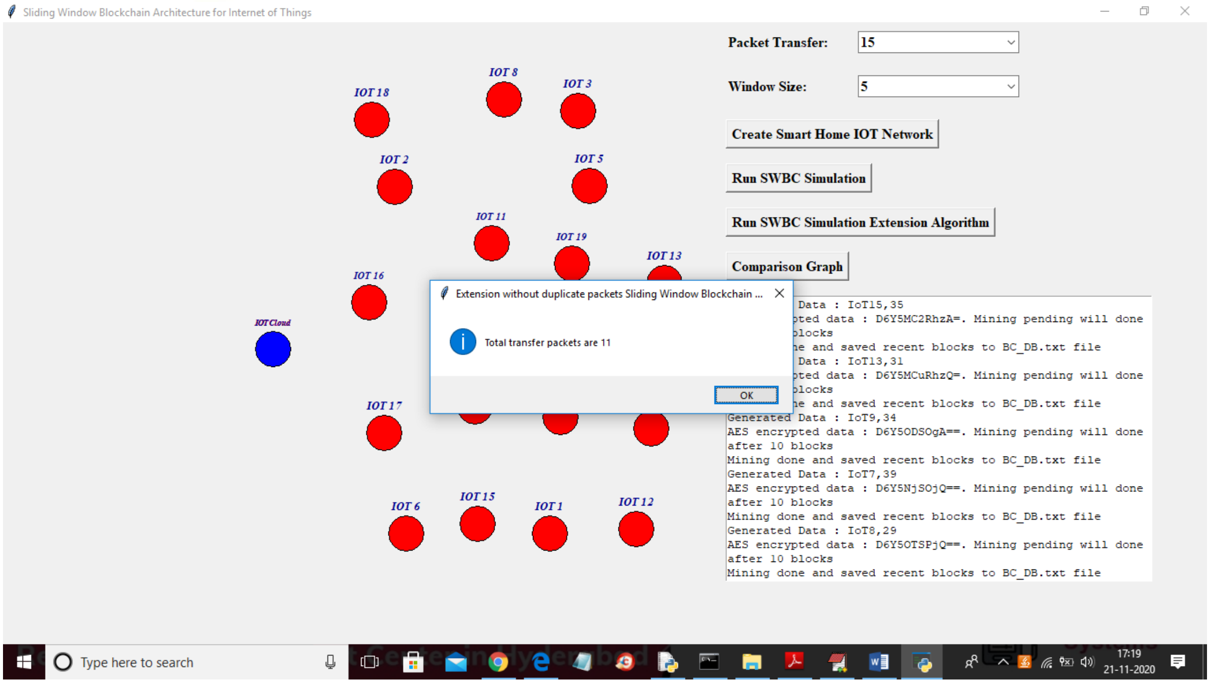


Packet Transfer: 15

Window Size: 5

```
Generated Data : IoT15,35
AES encrypted data : D6Y5MC2RhzA=. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : IoT13,31
AES encrypted data : D6Y5MCuRhzQ=. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : IoT9,34
AES encrypted data : D6Y5ODSOgA==. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : IoT7,39
AES encrypted data : D6Y5NjSOjQ==. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : IoT8,29
AES encrypted data : D6Y5OTSPjQ==. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
```

In above screen also IOT start sensing and sending packets and in above screen IOT10 is changed to red colour which means its sensing and sending data and after all 15 packets transfer will get below screen


Sliding Window Blockchain Architecture for Internet of Things
IOT 18
IOT 8
IOT 3
IOT 2
IOT 5
IOT 11
IOT 19
IOT 13
IOT 16
IOT Cloud
IOT 17
IOT 6
IOT 15
IOT 1
IOT 12
Create Smart Home IOT Network
Run SWBC Simulation
Run SWBC Simulation Extension Algorithm
Comparison Graph
Extension without duplicate packets Sliding Window Blockchain ...
OK
Type here to search
17:19
21-11-2020

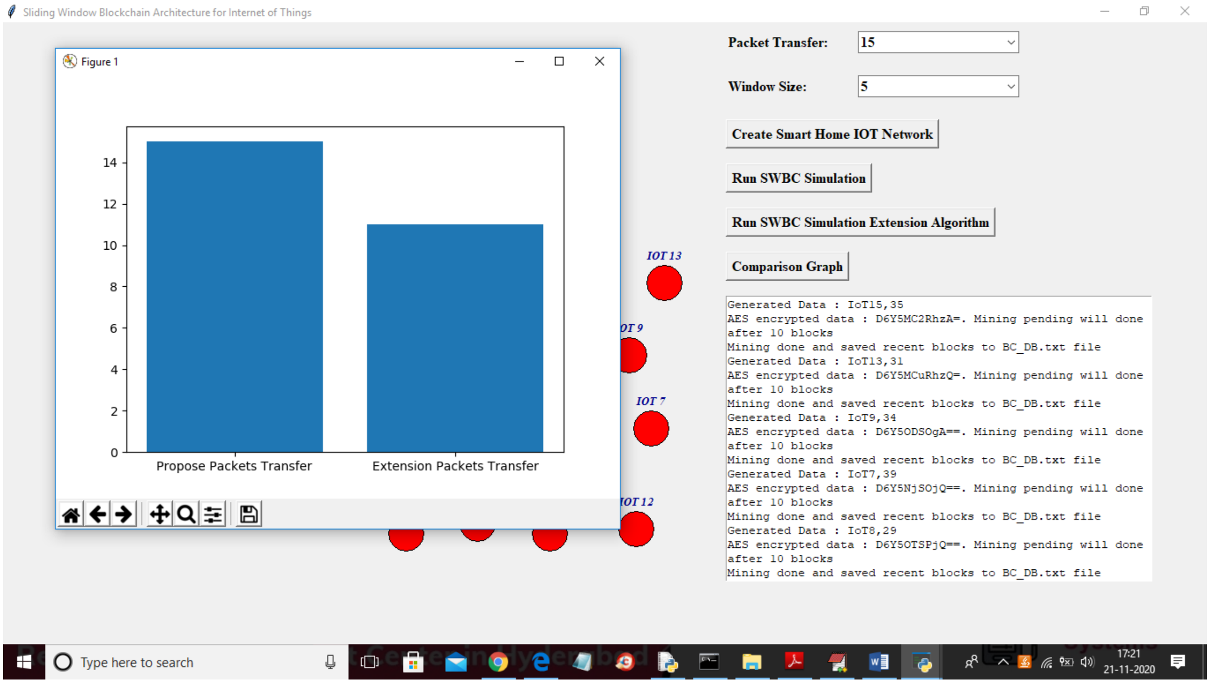
Packet Transfer: 15

Window Size: 5

Total transfer packets are 11

```
 Data : IoT15,35
pted data : D6Y5MC2RhzA=. Mining pending will done
blocks
ne and saved recent blocks to BC_DB.txt file
 Data : IoT13,31
pted data : D6Y5MCuRhzQ=. Mining pending will done
blocks
ne and saved recent blocks to BC_DB.txt file
Generated Data : IoT9,34
AES encrypted data : D6Y5ODSOgA==. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : IoT7,39
AES encrypted data : D6Y5NjSOjQ==. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : IoT8,29
AES encrypted data : D6Y5OTSPjQ==. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
```

In above screen with extension work from 15 packets we process only 11 packets and 4 duplicate packets avoided and this 4 packets energy consumption will be saved. Now click on ‘Comparison Graph’ button to get below graph


Sliding Window Blockchain Architecture for Internet of Things
Figure 1
14
12
10
8
6
4
2
0
Propose Packets Transfer
Extension Packets Transfer
IOT 13
OT 9
IOT 7
OT 12
Create Smart Home IOT Network
Run SWBC Simulation
Run SWBC Simulation Extension Algorithm
Comparison Graph
Type here to search
17:21
21-11-2020

Packet Transfer: 15

Window Size: 5

```
Generated Data : IoT15,35
AES encrypted data : D6Y5MC2RhzA=. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : IoT13,31
AES encrypted data : D6Y5MCuRhzQ=. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : IoT9,34
AES encrypted data : D6Y5ODSOgA==. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : IoT7,39
AES encrypted data : D6Y5NjSOjQ==. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
Generated Data : IoT8,29
AES encrypted data : D6Y5OTSPjQ==. Mining pending will done
after 10 blocks
Mining done and saved recent blocks to BC_DB.txt file
```

In above graph x-axis represents algorithm name and y-axis represents number of packets transfer and with extension work application process only 11 packets and can save energy of 4 packets.

5. CONCLUSION

IoT devices have resource limits such as computational capability, energy sources, and memory. As a result, typical security techniques are impractical for IoT. We presented a sliding window blockchain that, by minimising memory cost and restricting computing overhead, satisfies the needs of a resource-constrained IoT network. We discovered the following from the experimental results: (i) The computing time of PoW increases exponentially with difficulty. (ii) As the number of miners in the group grows, so does the overall block addition time. (iii) As the window size increases, so does the hash computation time. (iv) Choosing a random difficulty for each block in a blockchain minimises total block addition time.

REFERENCES

[1] S. Kulkarni, “The beauty of the blockchain,” Open Source for You, vol. 06, pp. 22–24, June 2018.

[2] T. M. F. Carames and P. F. Lamas, “A review on the use of blockchain for the Internet of Things,” IEEE Access, vol. 6, pp. 32 979–33 001, May 2018.

[3] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: challenges and solutions,” arXiv preprint arXiv:1608.05187, August 2016.

[4] IoT Agenda, “Smart home or building,” April 2018. [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/ smart-home-or-building

[5] L. Jiang, D. Y. Liu, and B. Yang, “Smart home research,” in Proceedings of 2004 International Conference on Machine Learning and Cybernetics, vol. 2, August 2004, pp. 659–663.

[6] theinstitute.ieee.org, “Towards a definition of the Internet of Things (IoT),” May 2015. [Online]. Available: https://iot.ieee.org/images/files/pdf/IEEE IoT Towards Definition Internet of Things Revision1 27MAY15.pdf

[7] J. Wan, X. Gu, L. Chen, and J. Wang, “Internet of Things for ambient assisted living: Challenges and future opportunities,” in International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), October 2017, pp. 354–357.

[8] D. Abbasinezhad-Mood, A. Ostad-Sharif, and M. Nikooghadam, “Novel anonymous key establishment protocol for isolated smart meters,” IEEE Transactions on Industrial Electronics, vol. 67, no. 4, pp. 2844–2851, April 2020.

[9] S. K. Das, D. J. Cook, A. Battacharya, E. O. Heierman, and T. Y. Lin, “The role of prediction algorithms in the MavHome smart home architecture,” IEEE Wireless

Communications, vol. 9, no. 6, pp. 77–84, December 2002.

[10] C. Qu, M. Tao, J. Zhang, X. Hong, and R. Yuan, “Blockchain based credibility verification method for IoT entities,” Security and Communication Networks, vol. 2018, pp. 1–11, June 2018.

[11] C. Lee, L. Zappaterra, K. Choi, and H. A. Choi, “Securing smart home: Technologies, security challenges, and security requirements,” in IEEE Conference on Communications and Network Security, October 2014, pp. 67–72.

[12] P. Treleaven, R. G. Brown, and D. Yang, “Blockchain technology in finance,” Computer, vol. 50, no. 9, pp. 14–17, September 2017. [13] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamar´ıa, “To blockchain or not to blockchain: That is the question,” IT Professional, vol. 20, no. 2, pp. 62–74, March 2018

AUTHOR PROFILES

Ms. M. ANITHA completed her Master of Computer Applications and Masters of Technology. Currently working as an Assistant professor in the Department of Masters of Computer Applications in the SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. Her area of interest includes Machine Learning with Python and DBMS.

Mr. CH. SATYANARAYANA REDDY Completed his Bachelor of Computer Applications at Acharya Nagarjuna University. He completed his Master Computer Applications at Acharya Nagarjuna University. Currently working as an Assistant professor in the Department of Computer Applications SRK Institute of Technology, Enikepadu, Vijayawada, NTR(DT). His areas of interest include Networks, Machine Learning & Artificial Intelligence.

Ms. SHAIK RAMEEJA is an MCA student in the Department of Computer Applications at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. She has a Completed Degree in B.Sc.(computers) from Sir C R Reddy Degree College for Women Eluru. Her areas of interest are DBMS, Java Script, and Machine Learning with Python.