# “AI-empowered, blockchain and SDN-integrated security architecture for IoT network of cyber-physical systems”

Sohaib A. Latif a, Fang B. Xian Wen a, Celestine Iwendi b, Li-li F. Wang a,
Syed Muhammad Mohsin c, Zhaoyang Han d, Shahab S. Band e

**Professor: Park Jong Hyuk**

**Presented By: Than Than Swe**

**03 April 2023**

# Contents

# Abstract


- The Internet of things (IoT) is one of the most emerging technologies nowadays and it is one of the key enablers of an industrial cyber-physical system (CPSs).
- It has started to participate in almost every aspect of our social life, ranging from financial transactions to the healthcare system, communication to national security, battlefield to smart homes, and so on.
- However, the wide deployment of IoT suffers certain issues as well, such as interoperability, compatibility, heterogeneity, a large amount of data, processing of heterogeneous data etc.
- The researcher exploits the potential benefits of a blockchain system and integrates it with software-defined networking (SDN) while justifying energy and security issues.
- Distributed trust-based authentication mechanism makes blockchain even more adaptive for IoT devices with limited resources.
- The experimental results show that the proposed cluster structure-based routing protocol outperforms the state-of-the-art Ad-hoc On-demand Distance Vector (AODV), Destination-Sequenced Distance Vector (DSDV), Secure Mobile Sensor Network (SMSN), Energy efficient secured cluster-based distributed fault diagnosis (EESCFD), and Ad-hoc On-demand Multipath Distance Vector (AOMDV), in terms of energy consumption, network throughput, and packet latency.

# 1. Introduction

- Industrial automation leads to the concept of smart factories based on artificial intelligence (AI) and the internet of things (IoT).
- A huge number of sensors are deployed in the field for effective and efficient industrial automation and such a vast deployment leads to the issues of interoperability, heterogeneity among devices, processing and dealing of big data, storage of data, energy management, safety and security.
- Optimal energy utilization enhances the operation life of IoT and can be a viable solution in economic terms.
- In recent, fog and edge computing has presented a viable architecture to resolve the resource scarcity problem in IoT.
- Minimizing energy consumption without compromising network security or improving security without affecting energy consumption is an important consideration.
- The use of cluster structure and optimizing Proof-of-Work (PoW) prevents the entry of selfish nodes and enhances the security and energy optimization of IoT devices.

# 2. Literature Review

- Traditional distributed architectures, protocols, and techniques, especially those related to security and energy, are no longer sufficient in the current era of information technology in the field of IoT.
- Nowadays, Researchers and practitioners are attracted to the implementation of blockchain and SDN solutions to solve the current problems in the field of IoT space.

## DistBlockNet

- Blockchain technology is used by the DistBlockNet model to confirm and distribute flow rules tables between IoT devices.
- The design works on the fundamental principle of distributed features in a software-defined network (SDN) to generate security and comparability-based plan in IoT-based networks.
- In this architecture, threats are automatically isolated based on the updated flow rules tables using the blockchain technique.
- However, energy consumption and resource limitation of IoT devices is not considered to evaluate the performance of this architecture.

## Blockchain Security over SDN(BSS)

- Files are securely transferred using blockchain to SDN.
- The use of the Ethereum platform, as well as the integration of the OpenDaylight controller with the OpenStack controller, indicates safe file movement among SDN devices using P2P distributed architectures.
- The technique is purely based upon secure transmission and does not address the core issues of IoT devices i.e. Energy and resource limitations.

## Blockchain-based Architecture for smart city

- Blockchain-based architecture for a smart city is divided into core and edge networks for efficiency purposes.
- It utilizes a centralized distributed architecture for efficiency whereas PoW design is used for privacy and security purposes.
- The key evaluation parameters used in this approach are Delay, hash rate, and block.
- The hybrid approach discussed does not evaluate the performance of the network over key parameters of the IoT-based architecture which are energy and security issues.
- Two main problems in the discussed architecture are the effective implementation of edge nodes and the caching technique used by these nodes.

# 3. Proposed System Model

- We implemented the IoT-supported blockchain and cluster structure of SDN for distributed network management of IoT.
- In Fig. 1, shows the high-level architecture of the proposed model.
- A blockchain is attached to each SDN controller for IoT communication. Analogous to Bitcoin's system, SDN controllers are connected in a P2P topology.
- **The proposed architecture has two key objectives:**

  (a) to improve communication security for IoT devices

  (b) to optimize their energy consumption to enhance their lifetime

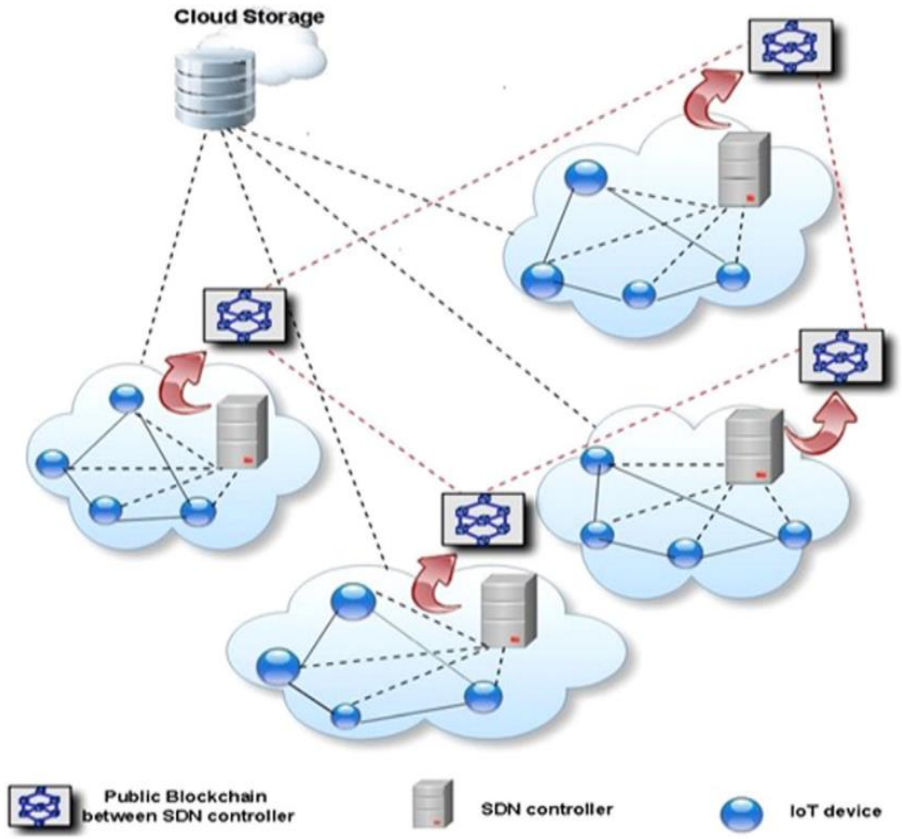


Fig 1: Cluster-based proposed model with blockchain-enabled SDN controller.

## 3.1 Data Transfer mechanism in SDN domain

- IoT devices in an SDN domain keep the private and public keys according to rules and policies defined by the SDN controller to carry out secure transactions in the blockchain.
- Whenever an IoT device intends to send data over the SDN domain; it signs in with a private key and publishes the message using its public key.
- The domain members consider the sender's public key and verify the validity of the block format message sent. The block is stored in a private blockchain, and the file is passed to the receiver if the sender node is allowed to share data.
- If data is to be sent to the device located in other SDN domains, after publishing its public key, the SDN controller sends a membership request to the controller of the destined device.
- On the successful completion of the registration and authentication process, the file is transferred to the recipient.

The following steps are to be followed for exchanging data files:

- Step 1: SDN controller in A1 signed the transaction using the private key and publishes it with the public key across the network
- Step 2: If the destined device is in the other SDN domain (A5 for the stated case), the file in the controller in A1 will send it the
- controller in A5
- Step 3: A block is added to the blockchain and broadcast in the SDN domain. The transaction is authenticated based on the public key
- Step 4: On receipt of the file, only the intended receiver can decode it

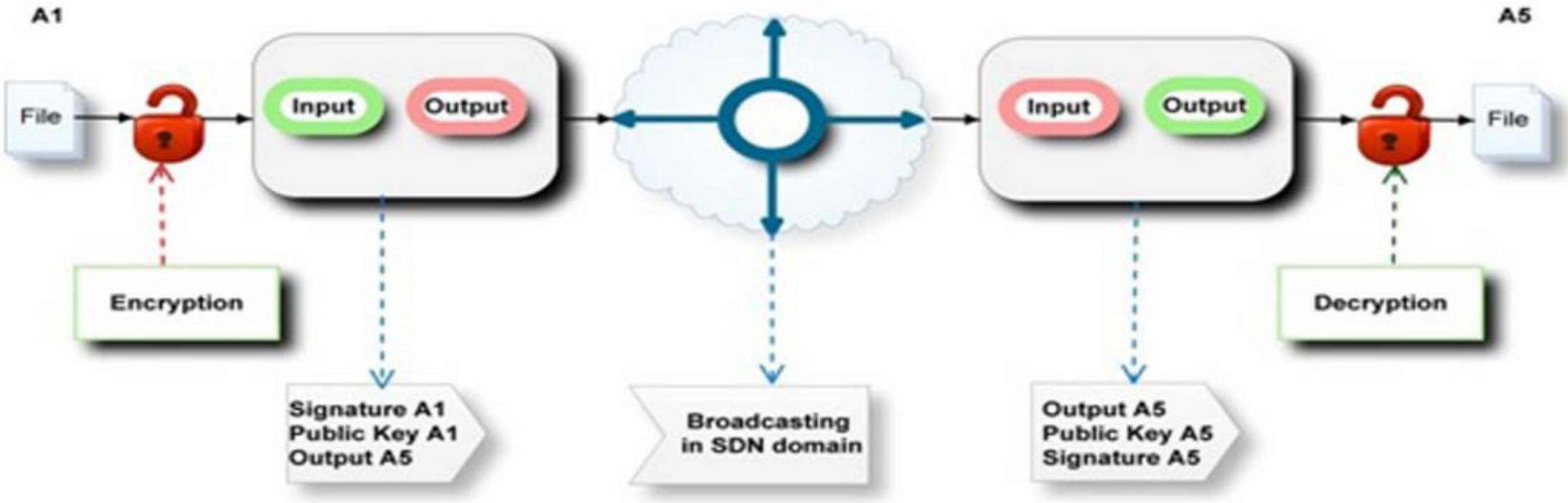


Fig 1: File transfer between two users A1 and A5 in SDN Domain.

## 3.2 Customizing blockchains to improve security and energy efficiency

- Proof-of-Work (PoW) is used in blockchain as a consensus algorithm when it commits to add new transactions into the ledger.
- PoW first aims to verify transactions and generate new blocks to the chain.
- With PoW, participants strive for each other to complete transactions on the network and get rewarded.
- The participant is known as a miner and the process is termed mining.
- Miners send digital tokens to each other in the network.
- A decentralized ledger gathers all the transactions into blocks.
- The complex and resource-hungry nature of the PoW algorithm does not suit resource-constrained IoT devices and becomes almost impractical.

- **The proposed model shown in Fig. 2 is SDN cluster-based IoT network aimed to reduce the proposed architecture's overhead associated with PoW.**

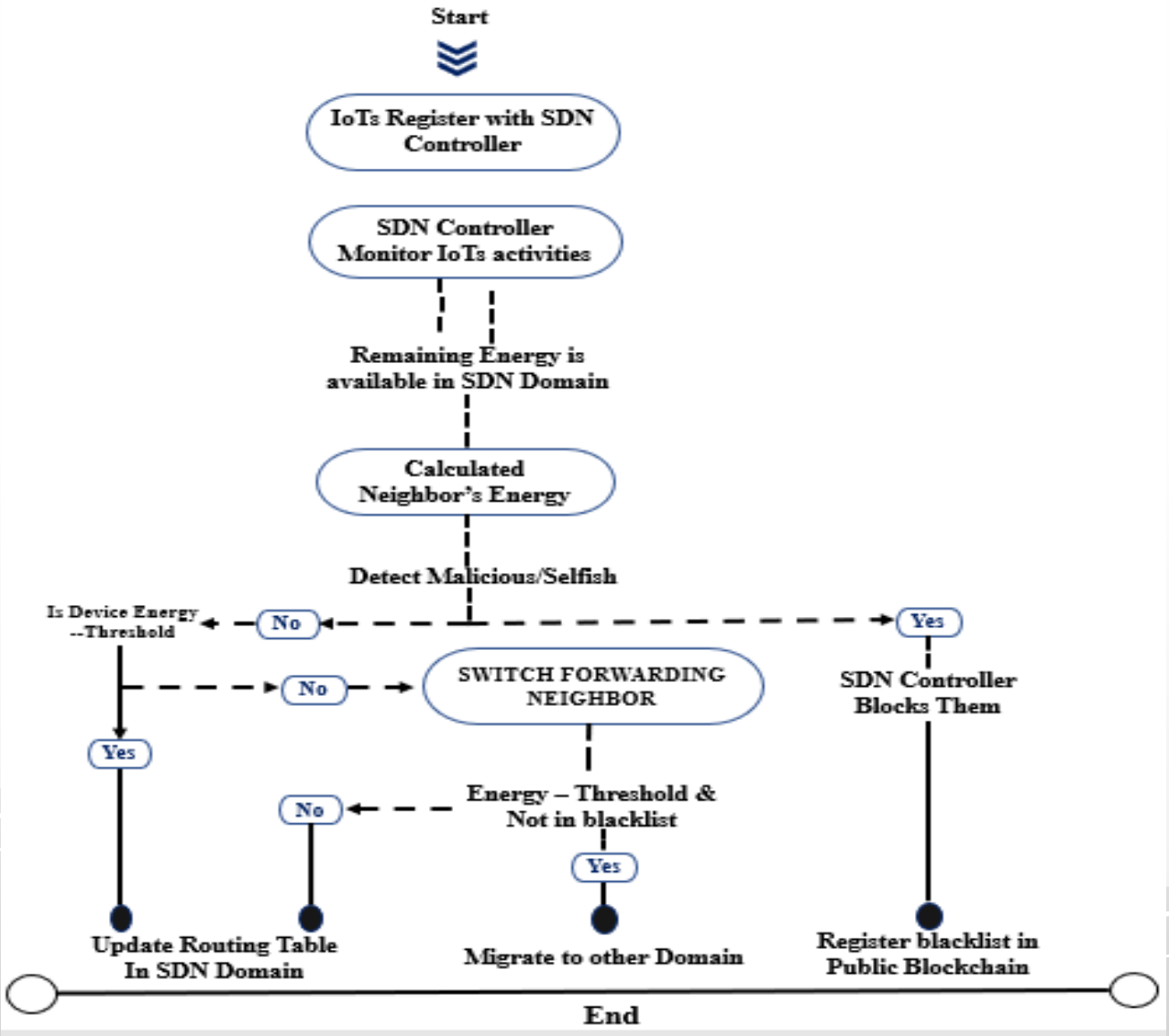


Fig 2: Flow mechanism of secure and energy efficient proposed model.

- The distribution trust base authentication mechanism resolves the PoW complexity issue.
- To be more precise, blocks are inserted into chains without the need for PoW consensus, reducing the initial PoW's overhead to zero.
- When you create a block, the SDN controller creates its hash.
- The controller recalculates the hash whenever the data changes.
- Linking the hash of the block to each other builds a chain and this whole process ensures the security of the network.
- The proposed architecture applies to diverse IoT devices, which generate and share data, perform transactions, and perceive smart contract features. It is pertinent to have a secure and energy-efficient mechanism to prevent unauthorized access in each SDN domain.
- Since the SDN controller acts as a cluster head in each domain, the controller grants permission to avail the network services by IoT devices.
- It prevents the selfish or malicious node from becoming part of the SDN domain.
- Once, the malicious joins the network, it compromises the network security and causes it to deplete the device's energy abruptly.
- The proposed architecture model enables IoT devices to migrate on a need basis and communicate in different domains.
- The network will protect and detect compromising nodes by combining public and private blockchains with peer-to-peer communication.
- The SDN controller monitors the IoT devices in this area of responsibility and detects selfish parties and prohibits them from registering in other SDN domains.

# 4. Experiments and results

- In this section, a description of the experimental setup is provided followed by performance evaluation and analysis.
- The performance of the proposed model is evaluated against state-of-the-art AODV, DSDV, SMSN, EESCFD, and AOMD, in terms of energy consumption, network throughput, and packet latency.

## 4.2 Performance Evaluation

- The proposed model revolves around the cluster structure to the security features in SDN with public and private blockchains while considering the resource limitations of IoT.
- The responsibility for authentication and validation of IoT devices rests with the SDN controller.
- The proposed model is flexible enough to accept changes in the cluster structure.
- The overhead of the proposed architecture is compared with the fundamental blockchain Flow Base Configuration (FBC) having PoW and hashing methods.
- The proposed model uses the cluster-based approach, it is also evaluated against two energy-aware clustering algorithms, i.e, Secure Mobile Sensor Network(SMSN) and Energy Efficient Secured Clustered-Based Distributed Fault Diagnosis Protocol (EESCFD).

## 4.2.1 Throughput

- The amount of data transferred successfully from the source to the destination is termed throughput.
- It can be linked with the total number of transactions carried out in the network.
- A significant amount of throughput difference can be observed from the figure.
- The main reason for this improvement is the utilization of cluster structure.
- Throughput has also been improved because of reduced overhead which was originated by PoW in FBC.

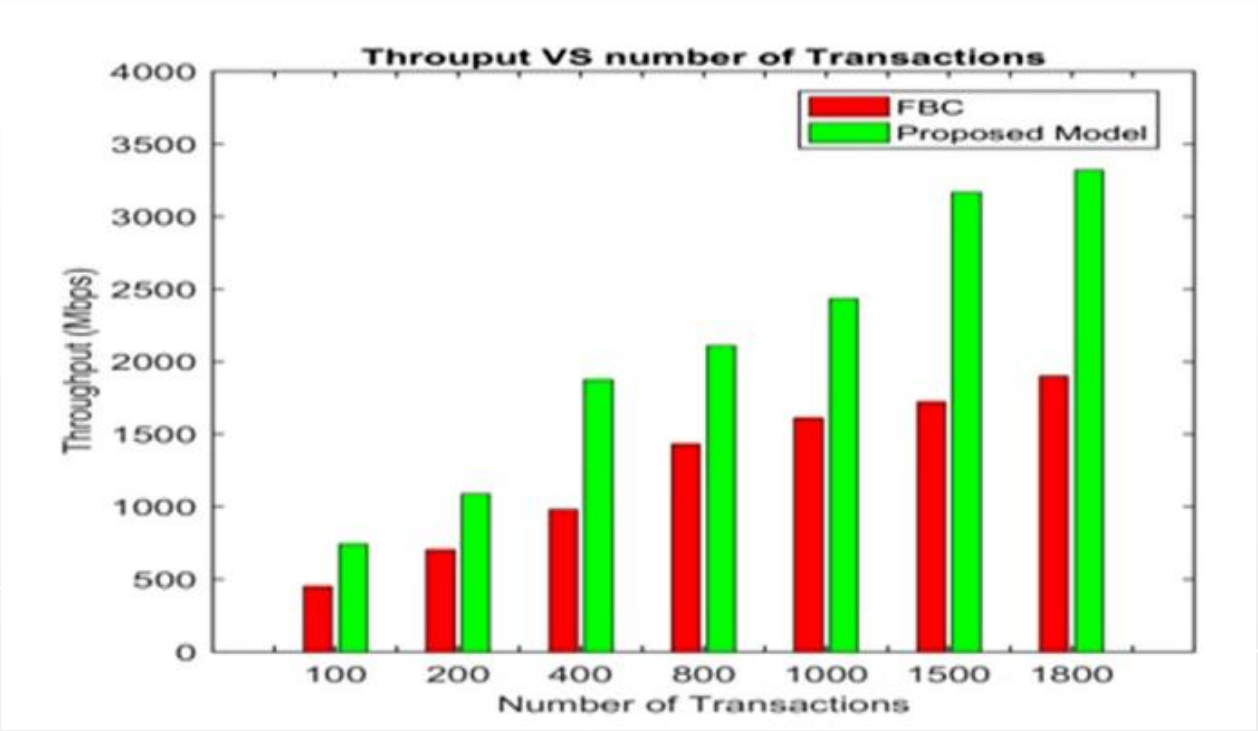


Fig 3: Throughput comparison of the proposed model with FBC.

# 4.2.2 End-to-end delay

- End-to-end is a term that refers to the process from beginning to end Delay, also known as latency, is the time it takes for a packet to pass from its source to its destination.
- It is the combination of processing time $\mathbf{T_{proc}}$ , transmission time $\mathbf{T_{trans}}$, and queuing time $\mathbf{T_{queue}}$ i.e. shown in Eq. (1).

$$Delay = T_{proc} + T_{trans} + T_{queue}$$

- The distance between the source and destination, the number of packets in the output buffer, and the processing speed of nodes all influence the delay.
- For the sake of the evaluation, we set the traffic type as cluster-based routing (CBR) with varying numbers of packets and packet size to 500 to 4000 and 1000 to 3500 bytes respectively.
- The proposed model observes low delay, and it is not affected by the amount of traffic in each cluster.
- The delay value increases from 0.5 to 1.6 nanoseconds with increasing the packet size.
- This is because buffer capacity reduces with an increase in packet size, which ultimately increases delay.

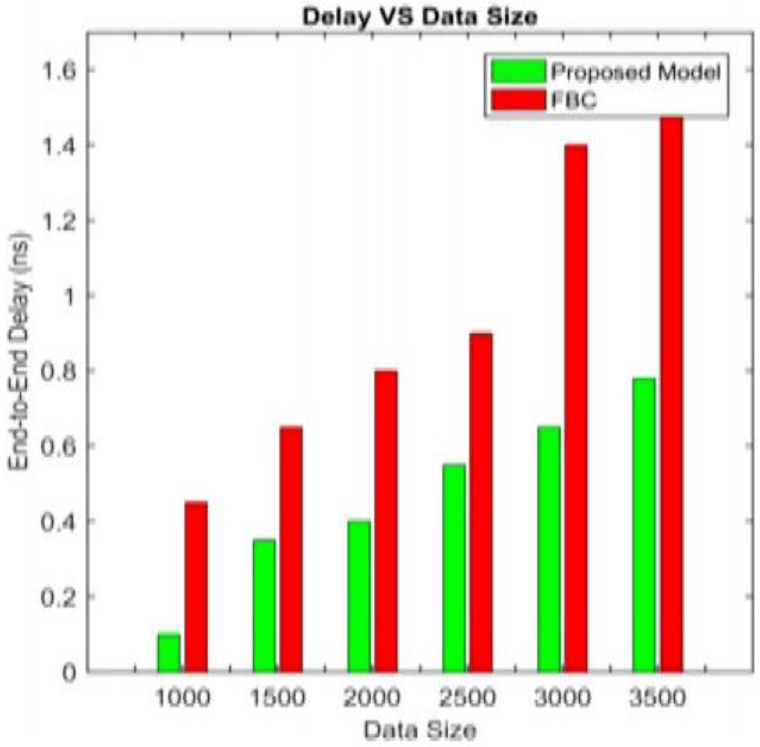


Fig 4. Delay comparison of the proposed model with FBC with various sizes of the data file.

## 4.2.3 Energy consumption

- Energy consumed in SDN based IoT network is the sum of energy consumed by each IoT device and SDN controller.
- The total energy consumption can be computed with the help of Eq. (2). Notations and their description is given in Table 1 of this study.

$$E_{tot} = N_{trans} * T_{trans} + [(N_{cont} * E_{cont}) + (N_{iot} * E_{iot})]$$

- The above equation dictates that the more and larger the number of packets sent, and high the degree of connectivity, the higher will be the energy consumption.
- The proposed protocol uses an energy-efficient technique in which routing tables are modified via the SDN controller based on the energy profiles of nodes in each SDN domain. This may mean that the protocol is suitable for use in the proposed IoT system architecture.

| Notation | Description |
|---|---|
| $E_{tot}$ | Total Energy Consumption |
| $N_{trans}$ | No. of Transactions |
| $T_{trans}$ | Transaction Time |
| $N_{cont}$ | No. of SDN Controllers |
| $E_{cont}$ | Energy consumed by each SDN Controller |
| $N_{iot}$ | No. of IoT devices |
| $E_{iot}$ | Energy consumed by each IoT devices |

**Table 1 : Notations and their description**

# 5. Conclusion and future work

- Next-generation industrial cyber-physical systems (CPSs) require artificial intelligence (AI) empowered solutions to overcome the issues of heterogeneity of devices, big data generated by the sensors, data streaming, processing of heterogeneous unstructured data and data security.
- The increasing trend of smart and intelligent services triggers the avalanche in the IoT network and their related services.
- To provide secure and efficient services, there is an urgent need to manage the computing and energy scarcity problem of IoT.
- By exploiting the power of AI, we have proposed architecture for IoT networks to enhance security and improve energy efficiency.
- We integrated the two emerging AI-based technologies namely, blockchain and SDN, and leverage their potential benefits in terms of efficient data analysis, data security and efficient energy management.
- The resource-hungry component of PoW is eliminated to tailor the blockchain for IoT capabilities.
- This method saves a large amount of energy, boosts data transfer rates, and reduces latency.
- Extensive testing has shown that the proposed model outperforms both the basic blockchain approach and current routing protocols.
- This study will in the IoT domain, we hope to develop a high-level P4 architecture with blockchain support in the future.

# *Thank You*