Architectures and Protocols for Internet of things based Ambient Assisted Living

Dr. Prescilla K.

Research group: Mr. Sarath Babu, Research Scholar, IIST,

Dr. B.S. Manoj, Professor, Dept. of Avionics, IIST, Thiruvananthapuram

INDIAN INSTITUTE OF SPACE SCIENCE AND TECHNOLOGY
THIRUVANANTHAPURAM, KERALA, INDIA 695547

January 27, 2020

Course of the presentation

Part I

Architectures and Protocols for Internet of things

Internet of Things

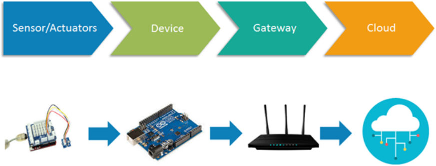
The concept of enabling Internet connectivity and associated services to non-traditional computers formed by integrating essential computing and communication capability to physical things for everyday usage.

Google Home Voice Controller

August Doorbell Cam

August Smart Lock

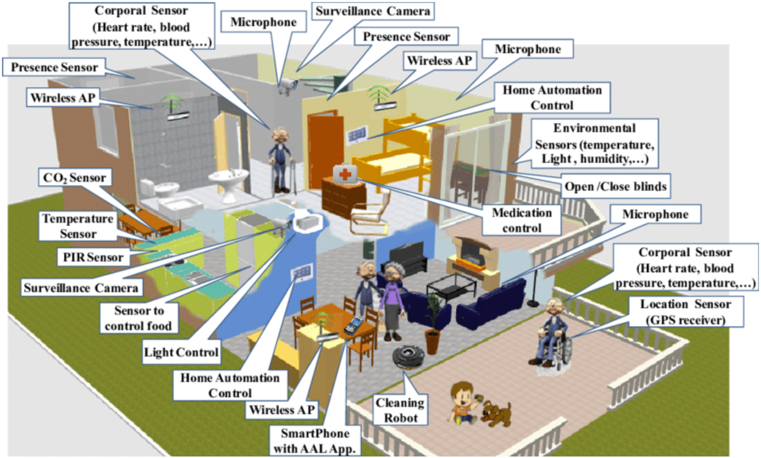
Footbot Air Quality Monitor



IoT Architecture

Ambient Assisted Living

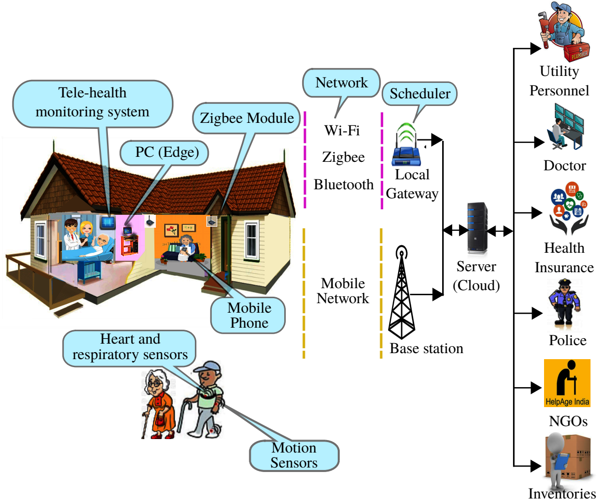
- AAL defines smart home environment for health care
  - Ambient environment cares for the inmates
  - Achieved through IoT



Ambient Assisted Living

- AAL provides personalized, time-sensitive, and context-aware intelligent services to achieve
  - Healthy elderly
  - Good care for people under palliative care who need continuous and time-sensitive health care.
  - Support differently-abled people
- Helps independent living and improves of the quality of life

Security of an AAL environment



A typical smart home system for assisted living

Constraints of IoT devices

- Limited memory
- Low processing capability
- Limited energy resources

Security constraints in IoT system

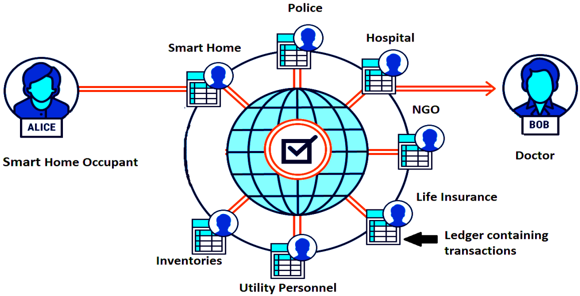
- Existing security frameworks cannot be applied due to the constraints in CPU, memory, and energy resources.
- Centralized security architectures are not suitable for IoT because they are subjected to **single point attacks**.

Therefore, the security architecture for IoT needs to be decentralized and designed to meet the limitations in resources.

Introduction to Blockchain

Blockchain

- Blockchain is a decentralized security architecture.

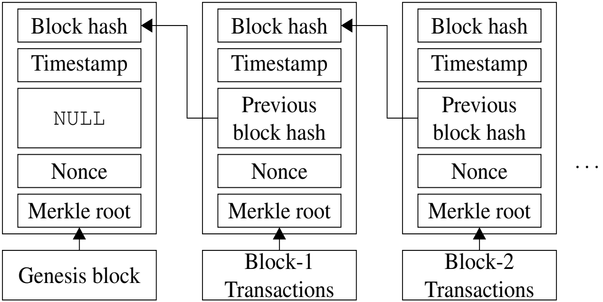


Blockchain architecture

Introduction to Blockchain

Blockchain

- A blockchain is a growing list of records, called blocks, that are linked using cryptographically generated hashes.
- Each block contains a cryptographic hash of the previous block, chaining the blocks together.



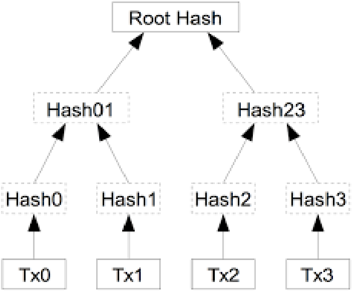
Blockchain

Introduction to Blockchain

Merkle tree

Merkle tree is a tree in which every leaf node is labeled with the hash of a transaction data and every non-leaf node is labeled with the cryptographic hash of the labels of its child nodes.

- Merkle tree grows with the number of transactions made



Merkle tree

Challenges in applying Blockchain to IoT

Computational complexity

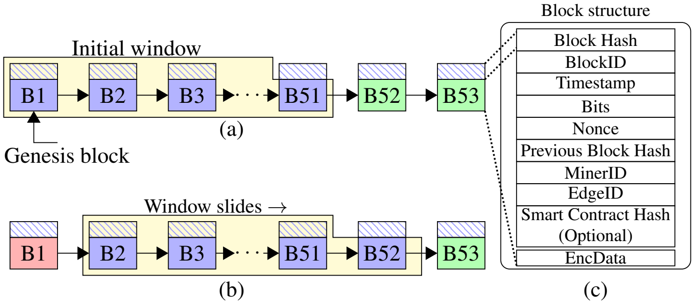
- Merkle tree
- Difficulty level -The difficulty level of mining is decided by the number of initial zeros of the hash value.

Scalability

- Number of transactions a blockchain can process within a specific time period.

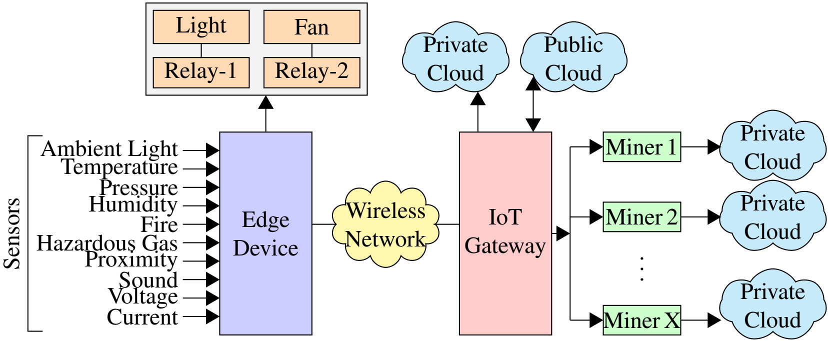
Proposed Sliding Window Blockchain

- The window consist of *n* recent blocks
- The window that slides through the blockchain for every block addition
- Window size increases from 1 to *n* and remains in the same size

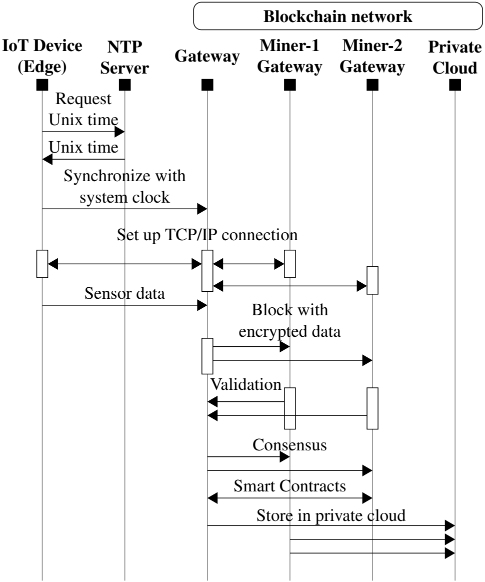


Sliding Window Blockchain architechture

Smart home testbed for studying SWBC



IoT-Blockchain Communication



Mining a block

Mining

Mining is the process of solving the blockchain Puzzle.

There are two main steps involved in puzzle solving

1. To find the hash of the block:

- SHA-256 algorithm is used
- Generates a 256 bit hash value for a block e.g., e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca 495991b7852b855.

Note

The sliding window has impact on the hash computation time with a computational complexity of $\mathcal{O}(n)$.

Mining a block

2. To reach the target with a specified difficulty level:

- The target is a 256-bit number. The target value consists of the difficulty.
  e.g., if the difficulty level is 3. The first three hexadecimal digits should be zeros. e.g., 000xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxx.
- Initially the hash of the block is compared with the target. If hash does not meet the target, nonce value (initial nonce value = 1) is incremented, and the hash of the block is recomputed.
- The process is repeated until the hash value meets the target. Since each block has different hash value to start with, the time at which the block reaches the target varies.

Performance analysis of SWBC on Raspberry Pi & PC

Table 1: Average time taken to add 30 blocks with a window size of 30.

Implementation	**Difficulty Level**	**Average block creation and addition time (Minutes)**
SWBC on Raspberry Pi	Level 4	30.75
	Level 5	529.98
	Random (1–5)	9.10
SWBC on PC	Level 4	4.061
	Level 5	66.2
	Random (1–5)	0.022

- A difficulty level $<= 4$ is preferred for IoT.
- A difficulty level $<= 5$ is preferred for PC.
- Random difficulty levels between 1–5 reduce the total computation time

Conclusion

- IoT devices face constraints on resources. Therefore, the standard security algorithms are not feasible for IoT.
- Proposed a sliding window blockchain that meets the requirements of a resource constrained IoT.
- SWBC reduces the memory overhead and limits the computational overhead.
- The security is increased by generating the block hash using the properties of n blocks in the sliding window.
- A false miner cannot mine a block unless he gets the previous $(n-1)$ blocks and the window size information.

Part II

Scope for ML/DL algorithms in IoT

Features of IoT big data

IoT big data features can be characterized through the "**6V**'s" features

1. **Volume**: massive/very large data
2. **Velocity**: high rate of data production
3. **Variety**: text, audio, video, and sensory data
4. **Veracity**: quality, consistency, and trustworthiness of the data
5. **Variability**: different rates of data flow
6. **Value**: information and insights that bring competitive advantage to organizations

Applications of IoT

1. Non time-critical applications
   - Inventory Management
   - Speech (or) voice recognition
   - Physiological and Psychological state detection
2. Time-critical applications
   - Autonomous driving
   - Environmental early warning (prediction of forest fires, hurricanes, landslides)
   - Driver/Elderly posture detection
   - Industrial IoT

Scope for ML/DL algorithms

Advantages of Deep Learning

1. Feature engineering is not required
2. Features not apparent to human view can be extracted easily by DL algorithms
3. Improves the accuracy of prediction model by using large amount of data.

Challenges in applying deep learning model for IoT

1. Lack of Large Dataset
2. Preprocessing
3. Secure and privacy preserving Deep Learning.
4. Challenges of 6V's

Conclusion

- DL and IoT have drawn the attention of researchers and commercial verticals in recent years
- DL and IoT have proven to make positive effect on our lives, cities, and all over the world
- However, not much research work has been carried out to meet the requirement of fast analytics in small scale platforms of IoT

Questions?

drprescilla.koshy@gmail.com

Thank you.