Leveraging Blockchain Technology for IoT Security Enhancement

Shikhar Mahajan
0801CS171077

Research Paper :

Name : A Study on Leveraging Blockchain Technology for IoT Security Enhancement

Publisher : IEEE

Published in : 2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA)

Internet of Things

IoT is the interconnection of physical devices, forming a network of smart things that communicate and exchange data with one another to reduce human exertions, improve efficiency of systems and overall economic benefits.

The basic components of IoT system includes,

- the IoT devices to collect data (for example, sensors, antenna, and microcontroller),
- IoT hub or gateway to collate and transfer data,
- the user interface or back-end systems.

Substantial challenges related to security and privacy for interconnected IoT devices, applications and networks

1. **Lack of Standardization**: The use of several different standards for development and deployment of IoT applications, leads to incompatibility and unexpected incidents.
2. **Device Identification**: IoT devices need to have secure identities and ownership, which are currently not provided
3. **Data Sharing**: The interconnected IoT devices share a large amount of data with each other that require proper authorization and authentication mechanisms for secure data interchange. To preserve privacy, there should be a proper user consent mechanism to keep the right of individuals to share their information. For example, in healthcare IoT using the patients' data without their permission.

Continued..

4. **Centralization in IoT**: The current IoT infrastructure relies on a centralized mechanism that leads to dissemination of information to Trusted Third Party (TTP) by relying on their security and privacy-preservation mechanisms.IoT networks are integrated with a platform that leads to a single point of vulnerability.
5. **Anonymity and Access Control**: Privacy-preservation can only be achieved with proper embedding of data and user anonymity with access control only by authenticated parties.

Blockchain Innovation

- A blockchain is a list of records, called blocks, which are cryptographically linked together, forming a chain of blocks. Blockchain technology is considered as a vigorous and robust solution for cybersecurity and privacy preservation in various technological scenarios, especially in IoT.
- The privacy preservation in blockchain can be guaranteed by keeping the transactions anonymous.
- There is no single point of failure. If a security breach occurs at one device or node, the system rejects its activities.

Blockchain-based solutions for IoT applications

- **Supply chain**: In supply chain IoT, achieving transparency is the key issue. Blockchain-based solution can provide visibility, optimization, petition
- **Energy Management and Smart Grid:** With the integration of blockchain and IoT in the energy industry, there has been a tremendous increase in the efficiency of smart grids and energy distribution, along with the monitoring and control of dissemination of resources.
- **Healthcare:** One of the blockchain-based IoT solutions in healthcare is the self or remote monitoring of patient's data through wearables or other smart devices.

Shortcomings of IoT		Blockchain Solutions
High costs	- Increased cost with scalability and addition of new IoT devices - Need for large servers and networking equipment - Maintenance and infrastructure cost	- No third party needed - Autonomous and distributed storage - Non-central and dispersed control guarantees robustness and scalability
Single point of failure	- Possibility of bottleneck - One malicious node can disrupt the entire network - IoT small devices are susceptible to DDoS attacks, data theft and remote hijacking.	- Interlocked devices - Data breach on/from one device, that device is thrown out of Blockchain - Utilizing resources of all participating nodes and eliminating one-to-many and many-to one traffic flows
Susceptibility to manipulation	- Mismanagement of data - Manipulation of findings in a particular direction	- Trackability - Immutability: data once entered or once a transaction is occurred, cannot be altered or deleted
Downtime & Unavailability	- Since, current infrastructure of IoT is mostly dependent on cloud, hence possibility of servers down or cooling	- Transactions are on a number of devices to hold identical information - A faulty node can join in or leave the system anytime
Unsecure Communication	- Communication is through third party or cloud	- Leverage smart contracts for secure communication - Message exchanges between occurs same as financial transaction in bitcoin
Privacy Breach	- Personally identifiable information (PII) can be exposed, for example, through profiling	- Anonymity of personal data by cryptographic linkage of nodes - Confidentiality is maintained similar to securing identity and balance information in bitcoin
Authentication	- Relies on trusted third party (TTP)	- Cryptographically signed transactions - Verification of digital signatures - Trust building

Conclusions

- Centralized models are expensive and problematic to manage when employed to heterogeneous scenarios like IoT, hence leading to the adoption and effectiveness of a blockchain-based decentralized approach.
- A captivating characteristic of blockchain is that the personal data can only be viewed with permission from the individual. The cryptographic technique is used to store proof of identity hence, breaking it is almost impossible, providing a strong privacy protection mechanism.

Thank You!!