SRI RAMACHANDRA

INSTITUTE OF HIGHER EDUCATION AND RESEARCH

(Category - I Deemed to be University) Porur, Chennai

SRI RAMACHANDRA FACULTY OF ENGINEERING AND TECHNOLOGY

Name : Shriram KP

Unique ID : E0219007

Year : 4th Year

Quarter : 1st quarter

Department : B.Tech CSE (Cys & IoT)

Faculty Name : Prof.Somasundaram

Academic year: 2022-2023

Research paper (1)

Title

Blockchain IoT (BIoT): A New Direction for Solving Internet of Things Security and Trust Issues

Author

Pascal Urien

Methodolgy

• Secure Communication, i.e. strong mutual authentication between end entities, privacy, and integrity for exchanged information;
• Secure Storage, required for secret values used by communication and enforced by tamper resistant devices such as secure elements;
• Node Integrity, which requires secure updates and secure boot. Physical technologies dealing with multi processors or logical technologies such as sandbox may effectively contribute to increase resistance to intrusion.

Advantage

The BIoT concept has four main benefits: publication/duplication of sensors data in public and distributed ledgers, time stamping by the blockchain infrastructure, data authentication, and non repudiation.
The architecture can secure over the air software updates both for GPU and radio SoC. Never less it is not able to avoid malicious updates performed by hackers who have physical access to devices. This feature implies the availability of secure download operations, typically associated to symmetric secret key stored and used in electronics chips.

Disadvantage

The encoding in the base 58 of the hash value of a file. Because a certificate is basically a signed hash, it is a way to compute a document certificate without a third trusted party. The transaction fee is computed from the transaction size, about 200 SATOSHIs per byte.
So having gas fees and maintainence fees and complexity of blockchain for simple Iot devices.

Research paper (2)

Title

IoT Data Security Via Blockchain Technology and Service-Centric Networking.

Author

1. Ali Mansour Al-madani
2. Dr. Ashok T. Gaikwad

Methodology

The IoT its became most commonly used and has some various applications such as smart city, banking, self-driving car, healthcare, smart home, and marketing. The implementation of IoT is increased as well as the Vulnerabilities increased. Those types of applications are important in our life and data must be private and secure. When the users using IoT without security techniques that mean their data and privacy will be in the attacker's hands. So that we are using Blockchain and SCN technology to avoid these threats.

Advantage

Based on the IoT security problems, this paper proposed a model for secure IoT data based on Blockchain; the model called service-centric networking (SCN). SCN provides communication by service names instead of addresses, and a decentralized network that allows the users of the network to communicate fast and data are reliable and secure. However, the identity of the users will be an encrypted format that is stored on their device backed by InterPlanetary File System (IPFS).

Disadvantage

Scalability is one of the biggest drawbacks of blockchain technology as it cannot be scaled due to the fixed size of the block for storing information. The block size is 1 MB due to which it can hold only a couple of transactions on a single block.

Research paper (3)

Title

Secure IoT Communication using Blockchain Technology

Author

1. Dinan Fakhri
2. Kusprasapta Mutijarsa

Methodology

IoT system using blockchain technology ,which replaces traditional MQTT protocol is replaced with a blockchain network and a smart contract. This smart contract functions as an intermediary for 2 IoT devices that are connected and used to store and retrieve data contained on the blockchain network. The smart refrigerator will store data on the blockchain network by using a smart contract, while the smart television will use the smart contract to get data that has been stored in the blockchain network.

Advantage

In the traditional security techniques they were three required; Integrity, Confidentiality, and Availability.
Integrity: the data will arrive in the receiver without modification by an unauthorized user.
Confidentiality: The data must be protected from unauthorized access.
Availability: When data required will be available for use. The limitation of traditional security technique centralized system, to overcome those limitations by using Blockchain technology, it provides a decentralized system.

Disadvantage

For verifying any transaction a lot of energy is used so it becomes a problem according to the survey it is considered that 0.3 percent of the world's electricity had been used by 2018 in the verification of transactions done using blockchain technology.

Research paper (4)

Title

Task Offloading Strategy with Emergency Handling and Blockchain Security in SDN-Empowered and Fog-Assisted Healthcare loT

Author

1. Junyu Ren
2. Jinze Li
3. Huaxing Liu
4. Tuanfa Qin

Methodology

the typical application of wireless body area networks (WBANs) based smart healthcare has drawn wide attention from all sectors of society. To alleviate the pressing challenges, such as resource limitations, low-latency service provision, mass data processing, rigid security demands, and the lack of a central entity, the advanced solutions of fog computing, software-defined networking (SON) and blockchain are leveraged in this work. On the basis of these solutions, a task offloading strategy with a centralized low-latency, secure and reliable decision-making algorithm having powerful emergency handling capacity (LSROM-EH) is designed to facilitate the resource-constrained edge devices for task offloading.

Advantage

a blockchain sharing mechanism for the fog layer blockchain to tackle the inherent time-inefficiency problem of blockchain. Extensive simulation has been conducted to validate the efficiency and effectiveness of the proposed mechanisms, and numerical results show that the system performances, including efficiency, reliability, and security, are significantly improved, verifying the superiority of the scheme.

Disadvantage

Although authentication-based[35] approaches can be used to address security issues of the fog layer, they do not work well in cross-domain communication scenarios under the framework of SDN. Moreover, because of the curious nature of the fog nodes and the high-security sensitivity of human health data, great challenges have been posed on system security and data privacy, and how to ensure signaling and data integrity and prevent them from being tampered with should also be fully considered. Furthermore, the healthcare loT edge devices may be untrusted or malicious such that they may selfishly initiate false claims to obtain better services, and abuse network resources and ruin the system security by launching cyber-physical attacks; therefore, effective security measures should be designed to ensure the security of the entire system.

Research paper (5)

Title

Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network

Authors

1. SAURABH SINGH
2. A. S. M. SANWAR HOSEN
3. BYUNGUN YOON

Methodology

Different attacks on the blockchain network. We address the liveness attack, which delays the transaction confirmation time; double-spending attacks, which duplicate the transaction funds; 51% vulnerability attacks, where adversaries can exploit more than 50% in the consensus mechanism; and private Key security attacks, in which an attacker discovers a vulnerability in the elliptic curve digital signature used in encryption methods, privacy leakage, and self-mining

Advantages

the authors have thoroughly analyzed several attacks on blockchain and the security issues of blockchain with some real-world examples. Moreover, this paper discussed the various security issues, challenges, vulnerabilities, and attacks that impede the increased adoption of blockchain technology while exploring these challenges in a variety of aspects. We also explained other blockchain applications and benefits, and we discussed many related opportunities at the business level.

Disadvantage

Blockchain databases are stored on all the nodes of the network creates an issue with the storage, increasing number of transactions will require more storage.

Research paper (6)

Title

IoT System Accomplishment using BlockChain in Validating and Data Security with Cloud

Authors

1. J. Kingsleen Solomon Doss
2. Dr. S. Kamalakkannan (Associate Professor)

Methodology

A blockchain has been implemented to deter security risks such as data counterfeiting by utilizing intelligent meters. Zero-Knowledge Proof, an anonymity blockchain technology, has been implemented through block inquiry to prevent threats to security like personal information infringement. It was suggested that intelligent contracts would be used to avoid falsification of intelligent meter data and abuse of personal details.

Advantage

The smart contract acquires energy statistics transmitted from the smart meter and calls for the transaction to calculate the cost using a modern-day and month tax calculation technique. Once the block has been developed, you send the participant ID to the Mobius registry to retrieve or charge power fees, and the servant retrieves the blockchain tape records that fit the ID in the database and displays it in that person's application.

The electricity fed on and the amount of the charge paid can be checked via the block in the proposed system when the verifier or the new member knows only the user's tackle. It is how it will evaluate the user's power intake survey a question with private empirical abuses. The offender is at risk for a second offense, such as burglary, as the customer will tell that the residence is empty. In this article also advised you to secure the non-public information of the proposed system by utilizing a zero-know-how evidence to show that the details are correct in addition to supplying the checker with the details .

The public key which is stored in the blockchain except saving genuine logs in the blockchain and the individual documents are preserved in the application store by way of the evidence Validation protocol. Unless the proof is jointly done using a shared key in the blockchains using the zero knowledge evidence process, it is understood that the details are used to prevent the encryption of data.

Disadvantage

Because the data obtained by the smart meter are scattered across a variety of human beings across the blockchain, the malicious attacker may evaluate a person's sample lifestyles by looking at the period the energy usage, so the attacker the take the time to consume limited electricity. Therefore, if the data obtained by the clever meter are automatically exposed by the blockchains, this can thus breach the consumer's privacy and harm the user's properties.

Research paper (7)

Title

A New IoT Trust Model Based on TLS-SE and TLSIM Secure Elements: a Blockchain Use Case.

Author

Pascal Urien

Methodology

A major security issue is PSK protection against eavesdropping, in order to avoid device cloning or illegitimate use. We present two secure elements TLSIM used on client side, and TLS-SE used on server side, which enforce PSK security. TLS-IM is a smartcard associated with TLS1.3 client running in laptop. TLS-SE is a standalone TLS1.3 server running in a secure element, which embeds an application computing signature for blockchain transaction. TLS-SE has a SIM form factor, and is plugged in a hardware module working with a Wi-Fi SoC, providing TCP/IP connectivity.

Advantage

Many blockchain systems work with the SECP256k1 elliptic curve for transaction signing. The TLS-SE secure element embeds an application, which delivers cryptographic services, such as key generation or ECDSA signature over the SECP256k1 curve. Commands are encoded by ASCII lines, ended by CrLf characters. A command comprises a first character that identifies the procedure to be executed (g=generate key, s=sign, p=get public key, r=get private key), a key index encoded by two hexadecimal digits, and an optional payload expressed in hexadecimal. The response is ERROR CrLf in case of issues, or a set of hexadecimal data ended by the CrLf sequence in case of success.

Disadvantage

First (HMAC) is required to verify the PSK binder included in the ClientHello message, second is used to compute the handshake secret from the Diffie-Hellman exchange over elliptic curve. The demonstration shows (see figure 3) the TLS-IM integration, in the open stack wolfSSL, thanks to the implementation of 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC) 978-1-7281-9794-4/21/$31.00 ©2021 IEEE 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC) | 978-1-7281-9794-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/CCNC49032.2021.9369485 Authorized licensed use limited to: Univ of Calif Santa Barbara. Downloaded on June 22,2021 at 05:29:45 UTC from IEEE Xplore. Restrictions apply. dedicated callback functions, which perform the verification of PSK binder and the computing of the handshake secret.

So the it consumes more time than traditional iot system.

Research paper (8)

Title

BSS: Blockchain Enabled Security System for Internet of Things Applications

Authors

1. Lokendra Vishwakarma
2. Debasis Das

Methodology

The conventional security protocols are not suitable for IoT applications due to the high computation and storage demand. Therefore, we proposed a blockchain-enabled secure storage and communication scheme for IoT applications, called BSS. The scheme ensures identification, authentication, and data integrity. Our scheme uses the security advantages of blockchain and helps to create safe zones (trust batch) where authenticated objects interconnect securely and do communication. A secure and robust trust mechanism is employed to build these batches, where each device has to authenticate itself before joining the trust batch. The obtained results satisfy the IoT security requirements with 60% reduced computation, storage and communication cost compared with state-of-the-art schemes. BSS also withstands various cyberattacks such as impersonation, message replay, man-in-the-middle, and botnet attacks.

Advantage

The BSS constitute two elements, candidate (IoT devices) and controller. It has two phases, i.e., authentication and batch creation (ABC), and candidate to candidate communication (CCC). A controller must authenticate all the candidates who want to join the trust batch and want to interact with each other. All the controllers synchronize to maintain the consistency of blockchain. In the ABC phase, any device who wants to join the trust batch has to send the join request to the controller. The controller generates a signed token and sends it to the requesting device along with its public key (Assuming all the controllers have a public-private key pair). After receiving the response from the controller, the candidate retrieves the secret information and saves it for future communication. The controller creates the batch and generates the genesis block. The algorithm 1 describes the authentication and batch creation process. The association of the candidate device to the trust batch is governed by the smart contract defined in the algorithm 2. At the blockchain level, the uniqueness of the devices is verified by the smart contracts. If any of the conditions is not satisfied, then the device candidate can not be linked with the trust batch

Disadvantage

The performance of the scheme is measured as computational cost, energy consumption, and storage and communication cost. The measuring unit of computational cost is milliseconds and represented as Tct.

So the computational cost is higher which is biggest disadvantage of this model.

Research paper (9)

Title

Healthcare Domain in IoT with Blockchain Based Security- A Researcher's Perspectives

Author

1. A.Yogeshwar Research Scholar
2. S. Kamalakkannan Associate Professor

Methodology

One of the key development in security is created by Blockchain (BC) technology which can exchange the data in secure manner. In many existing studies can be improved by enabling BC technology in the healthcare system. The main scope of BC technology has to convey effectively exchanging information between patient and other medical service parties based on some of the advantages such as authentication, immutability, decentralized storage, interoperability, distributed ledger, trustworthy and provides opportunity in a reliable manner and increase in productive. This paper presents challenges and problems for BC based IoT healthcare and provide with the security requirements of such domains due to traditional security measures. The aim of this paper is simply investigate how Blockchain will improve the healthcare environment within the IoT context. It also amalgamates the potential of blockchain technology as a promising security measure, highlights potential challenges in the healthcare domain, and provides an analysis of different blockchain based security solutions.

Advantage

A comprehensive analysis of basic security requirements of healthcare systems is one of the main contributions of this paper. In comparison to monotonic accessible state-of-the-art surveys, this paper offers an integrative research addressing security standards as well as challenges and open problems based on loopholes in current solutions, patients' information sharing and privacy promise concerning blockchain add-on in healthcare. It also filters out the exploding patterns in the region to include a baseline for several other researchers. It emphasizes that, in addition to other security solutions, blockchain might be able to get a scalable solution and decentralized to meet the increasing needs of the smart healthcare industry.

Disadvantage

Healthcare domain in IoT has higher safety with better quality which has minimize the cost of services and reduced time based on the increased user experience with constant medical care. The sensitivity of the data is the very essential parameter in Healthcare domain in IoT. Hence large quantity of information are generated which may consumes lot of power and obstructs the network. There are several challenges can occur in healthcare when the use of small sensors due to limiting the memory usage, limited power supply, limited network capacity and computer specifications.

Research paper (10)

Title

POSTER: Blockchain-based Key Management Protocol for Resource-Constrained IoT Devices

Author

1. Ahmed Alrehaili
2. Aabid Mir

Methodology

The proposed system has been designed for light-weight IoT devices with additional security measures provided by deploying difficulty parameters. This paper examines the hash mining procedure along with the application of proposed solution implemented in java programming language. Also the paper examines deploying different hashing algorithms in the proposed solution and compares their processing time. The higher difficulty parameters combined with faster hashing algorithms provides the most suitable solution for IoT devices with less computational power and memory requirements.

Advantage

The two critical components of a basic security process, authentication and authorization are required to deliver these benefits. Existing security measures and network architectures seem to be ineffective against the future generation networks and devices. Some of the serious challenges encountered by the existing networks are heterogeneity of the IoT devices, scalability and sensors operating in the open environment [1]. These challenges, if not addressed, can result in roadblocks towards a secure IoT infrastructure. This paper presents an attempt to resolve the balance between openness of the IoT network and the security of IoT devices using blockchain technology.

Disadvantage

Selecting a suitable hashing algorithm is a critical task which affects various parameters of a given network such as number of connected devices, memory size, bandwidth, security, etc . Therefore, the proposed system has to consider different factors to avoid encountering obstacles to end users. Comparison of elapsed time of mining 100 blocks. Comparison of elapsed time of mining 8000 blocks. especially when working with low memory and low power IoT devices

There is a trade-off between the size of output of a hashing algorithm and security. For blockchains related to IoT environments, a smaller hash size is suitable for its storage memory. Nevertheless, these smaller hashes are easier to be calculated and breached. Therefore, hashing algorithms with smaller output sizes should be accompanied by a larger difficulty parameter to compensate for the reduced time complexity