RESEARCH RELIABLE STORAGE WITH ENHANCED KEY FOR THE INDUSTRY LEADING IOT ENVIRONMENT

Mr. P. K. VenkateswarLal, M.Tech,(Ph.D) ,Associate professor, Department of Computer Science , Narayana Engineering College (Autonomous) Gudur**,**.SPSR Nellore, AP, India.
A.V.SaiHarshini, Student, I.DivyaBharathi, Student, B.Sunitha, UG Students, Department of ComputerScience, Narayana Engineering College (Autonomous) Gudur**,**.SPSR Nellore, AP, India.

Abstract

` Cognitive computing over big data brings more development opportunities for enterprises and organizations in industrial informatics and can make better decisions for them when they face data security . To satisfy the requirement of real-time data storage in the industrial Internet of Things (IoT), the remote unconstrained storage cloud is generally used to store the generated big data. However, the characteristic of semi-trust of the cloud service provider determines that the data owners will worry about whether the data stored in cloud computing is left or not .In this article, a secure storage auditing is proposed, which supports efficient key updates and can be well used in the cognitive industrial IoT environment. Moreover, the proposed basic auditing can also be extended to the support batch auditing that is suitable for the multiple end devices to audit their data blocks simultaneously in the practice. In addition, a hybrid data dynamics method is also proposed, which employs a hash table to store the data blocks and uses the linked list to locate the operated data block. Compared with previous methods, the data block location time in the proposed data dynamics can be reduced by 40%. The security analysis results is to demonstrate that the proposed scheme can be used to proved to be correct, and is secure under computational diffiehellman (CDH) and discrete logarithm (DL) assumptions.

Introduction

Industrial IoT is to integrate all kinds of sensors through wireless networks and use the technology of intelligent analysis to serve industrial productionM. L.-E. Lucas-Estanet.al.,J. Gonzalez(2019). Using industrial IoT to assist the production can improve manufacturing efficiency, reduce resource consumption and improve product quality. With the development of cognitive computing, the technology of industrial IoT is also moving towards the direction of intelligence that conforms to the definition in IoT. For instance, CR (Cognitive Radio) networks of industrial IoT can well address bandwidth issues and enable IoT devices to be performed with cognitive functionalities, such as dynamic spectrum accessing circumstantial perceiving, and self-learning L. Sun et.al., L. Wan, K Liu et.al., X. Wang (2019).

As the number of the end devices increased in industrial IoT, the amount of the data in the system will also be increased J. Shen, D. Liu et.al., X. Chen et.al., J. Li et.al., N. Kumar et.al., P. Vijayakumar, (2020). It is an urgent problem that how to manage and analyze the collected real-time data effectively. Cloud computing can provide end-users with unlimited computing capability and storage space F. Li et.al., K.-Y. Lam et.al., X. Li et.al., Z. Sheng et.al., J. Hua et.al., L. Wang (2019). Users only need to pay for the services they enjoy as a manner of pay-per-use without investing in local hardware. Through the cloud server's rapid analysis and processing of the data, the industries may adjust the decision-making of their product produced according to the response results, which will greatly maximize the utilization rate of resources and promote the transformation from traditional industry to intelligent industry. However, the CSP is honest but curious about the stored data. The CSP may destroy the data or delete the infrequently accessed data due to financial interests. If the data of industrial IoT in the cloud is stored completely, it will affect the production security of factories and make wrong decisions for industries. Hence, end-users in industrial IoT the requirements of integrity checking to their data stored in the cloud.

Literature survey

A.Balancing for reliable self-organizing industrial IoT networks:

The industry will interconnect and digitalize traditional industries to enable smart and adaptable factories that efficiently utilize resources and integrated with systems. A key enabler of the paradigm is the communicating infrastructure that will support the ubiquitous connectivity of CyberPhysical Production Systems. The integration of the wireless networks will facilitates the dynamic reconfiguration of the factories of the future, and the collections and managing of the large amounts of data. This vision requires the reliable and a low latency wireless links with a necessary bandwidth to support the data-intensive applications and the Spatio-temporal variations of the data resulting from the reconfiguration of Industrial IoT (Internet of Things) systems Z. Li et.al., B. Chang et.al., S. Wang et.al., A. Liu et.al., F. Zeng et.al.,G. Luo, (2018) To this aim, this paper proposes a load of balancing scheme that dynamically manages the wireless links based on their quality and the amount of the data to be transmitted by each of the node. The proposed scheme avoids the saturation of the channels, and significantly augments the reliability of the industrial wireless networks in the comparison with the existing solutions.

B.Cooperative-evolution based WPT resource allocation for large-scale cognitive industrial IoT:

The recently developed technique of the wireless power transfer (WPT) provides a way of promising to charge the wireless sensor networks (WSNs) of cognitive the industrial Internet of Things (IoT) deployed some areas that are difficult at sometimes for humans to access the issue. Previous work has been focused on the power allocation strategy at the wireless node level. However, the priority among different modes in the identical wireless node has not been taken into consideration, and different modes equipped with different types of batteries accomplish different tasks in an wireless node. Here we are using a strong approach for the security in IoT , L. Sun et.al., L. Wan et.al., K. Liu et.al., X. Wang(2019). Traditional WPT systems consist of a rechargeable WSN and a mobile charger, which are deployed for wirelessly charging wireless nodes. However, that the constructed WPT system consists of a rechargeable WSN and with adequate power, which can charge wireless nodes simultaneously. In today technology security is very important in the storage, and the critical path (CP) in the disjunctive graph is the core factor in determining the final maximum cost. Thus, we propose a new strategy that can identify the interacting variables based on the CP by exploiting the perturbation technique. Then, the decomposed components are evolved by adopting a evolutionary algorithm (CEA). The proposed is better in this method. Three state-of-the-art methods are tested and compared with CPCEA, and three scales of datasets are considered. The experimental results demonstrate the validity of CPCEA.

C.Advances and emerging challenges in cognitive internet-of-things:

The evolution of the Internet of Things (IoT) devices and their uses in new generation intelligent systems has generated a huge demand for wireless bandwidth. This bandwidth problem is further exacerbated by another characteristic of IoT applications, i.e., IoT devices are usually deployed in massive numbers, thus leading to an awkward scenario that many bandwidth devices are chasing after the very limited wireless bandwidth within a small geographic area .It is our responsibility that we need to fully study other critical issues such as standardization, privacy protection. In this paper, we investigate the structural frameworks and potential applications of cognitive IoT. We further discuss the functionalities and heterogeneity for cognitive IoT. Security and privacy issues involved in cognitive IoT are also identified. Finally, we present the key challenges and future direction of research on cognitiveradio-based IoT networks.

Existing Sytem

Privacy-preserving data outsourcing with integrity auditing for lightweight devices in cloud computing

- In 2007, a data storage checking scheme of PDP (Provable Data Possession) is proposed by Ateniese et al., which allows users to verify whether their data stored in an untrusted server is complete without retrieving it locally

- After that, Juels et al. defined a POR (proof of retrievability) model for data storage checking. It is worth noting that the POR allows users to check whether the data can be retrieved compared with the PDP. However, the classical two storage checking models of PDP and POR can only check the static data.

Drawbacks

- There are no Data Fragmentations to keep data secure.
- The data outsourced to a public cloud is not secured due to a lack of Cloud Security.

Proposed System

To reduce the computational cost of the user side, the computation of the partial key is delegated to the TPA. Moreover, the updated key is different in each round, which improves the non-foreseeability of the user's secret key. In addition, in the proposed scheme, the authenticator of the data blocks can be updated by the cloud without recomputing by data owners.

The proposed scheme can provide finegrained auditing. In other words, the proposed scheme in this paper not only supports the data block auditing but also supports the data sub-blocks auditing.

A new data index structure is designed that consists of a hash table and a linked list. In the proposed scheme, the hash table is used to store the data blocks, and the linked list is used to locate the data block. In this way, the efficiency of data dynamic operations can be highly improved.

Advantages

- The system proposes not to store the entire file at a single node. The methodology fragments the file and makes use of the cloud for replication.
- The data are distributed such that no node in a cloud holds more than a single block so that even a successful attack on the node leaks no significant information.

Modules

a.Data Owner Module

In this module, the data owner uploads their data to the cloud server. For the security purpose, the data owner encrypts the data file's blocks and then store in the cloud. The data owner can check the replication of the file's blocks over the Corresponding cloud server. The Data owner can have capable of manipulating the encrypted data file's blocks and the data owner can check the cloud data as well as the replication of the specific file's blocks and also he can create a remote user concerning registered cloud servers. The data owner also checks data integrity proof on which the block is modified by the attacker.

b.Cloud server Module

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data file blocks and store them in the cloud for sharing with Remote Users. To access the shared data file's blocks, data consumers download encrypted data file blocks of their interest from the cloud and then decrypt them.

c.End-User

In this module, the remote user logs in by using his user name and password. After he will request the secrete key of the required file blocks from cloud servers, and get the secrete key. After getting secrete key he is trying to download the file's blocks by entering the file's block name and secrete key from thecloud server.

d.Data Encryption and Decryption

All the legal users in the system can freely query any interested encrypted and decrypted data. Upon receiving the data from the server, the user runs the decryption algorithm Decrypt to decrypt the ciphertext by using its secret keys from different Users. Only the attributes the user possesses satisfy the access structure defined in the ciphertext CT, the user can get the content key.

Conclusion

In this paper, we propose a secure storage auditing scheme with efficient key updates for the cognitive industrial IoT environment. Moreover, the proposed auditing in this paper can be extended

to support batch auditing, which highly improves the efficiency of multiple user data auditing. Note that the data index in this paper is composed of a hash table and a liked index list, which reduces the time cost of the data dynamics by 40% compared with previous schemes. In addition, the security analysis shows that the proposed scheme is proved to be correct and secure. The final analysis indicates that the proposed one can be performed with low computational cost, which is suitable for the lightweight end devices in cognitive industrial IoT.

References

1. M. L.-E. Lucas-Estan and J. Gonzalez, (2019) ,“Load balancing for reliable self-organizing industrial IoT networks," IEEE Transactions on Industrial Informatics, vol. 15, no. 9, pp. 5052–5063.
2. J. Wan, S. Tang, Q. Hua, L. Di, and J. Lloret, (2019) ,"Context-aware cloud robotics for material handling in the cognitive industrial internet of things," IEEE Internet of Things Journal, vol. 15, no. 4, pp. 2272–2281.
3. L. Sun, L. Wan, K. Liu, and X. Wang,(2019), “Cooperative-evolution based WPT resource allocation for large-scale cognitive industrial IoT," IEEE Transactions on Industrial Informatics .
4. J. Shen, C. Wang, J.-F. Lai, Y. Xiang, and P. Li, (2019), “Cate: Cloud-aided trustworthiness evaluation scheme for incompletely predictable vehicular ad hoc networks,” IEEE Transactions on Vehicular Technology.
5. T. Zhou, J. Shen, X. Li, C. Wang, and J. Shen, (2018), “Quantum cryptography for the future internet and the security analysis,” Security and Communication Networks.
6. H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y . Huang, Y. Chen, and J. Liu, (2017), “Dynamichash-table based public auditing for secure cloud storage,” IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 701 – 714.
7. Penchalaiah P, Rajasekar P et al, "An Efficient Multi-User Hierarchical Authenticated Encryption Using Simultaneous Congruence for Highly Secure Data", International Journal of Future Generation Communication and Networking (WoS), ISSN: 2233-7857(Print); 2207-9645(Online), NADIA, (2020), Vol. 13, No. 2, pp. 1-10
8. D. Liu, J. Shen, Y. Chen, C. Wang, T. Zhou, and A. Wang, "Privacy-preserving data outsourcing with integrity auditing for lightweight devices in cloud computing," in Proceedings of the International Conference on Applied Cryptography and Network Security, 2019, p. 223–239.
9. P.Rajasekar, H Mangalam, "Design and implementation of power and area optimized AES architecture on FPGA for IoT application", Circuit World, ISSN 0305-6120 Vol. 47 No. 2, pp. 153-163 https://doi.org/10.1108/CW-04-2019-0039
10. J. Shen, D. Liu, X. Chen, J. Li, N. Kumar, and P. Vijayakumar, (2020), "Secure real-time traffic data aggregation with batch verification for the vehicular cloud in events,” IEEE Transactions on Vehicular Technology, vol. 69, no. 1, pp. 807–817.
11. Z. Li, B. Chang, S. Wang, A. Liu, F. Zeng, and G. Luo, (2018), “Dynamic compressive wideband spectrum sensing based on channel energy reconstruction in cognitive internet of things,” IEEE Transactions on Industrial Informatics, vol. 14, no. 6, pp. 2598–2607.
12. F. Li, K.-Y. Lam, X. Li, Z. Sheng, J. Hua, and L. Wang, (2019), “Advances and emerging challenges in cognitive internet-of-things,” IEEE Transactions on Industrial Informatics.

