International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
ISSN: 2457-0362
www.ijarst.in

SECURE STORAGE AUDITING WITH EFFICIENT KEY UPDATES FOR COGNITIVE INDUSTRIAL IOT ENVIRONMENT

Raja Rajeswari kalidindi, Eppili Sai Bhargav
Associate professor,
Department of MCA
rajeswari.kalidindi29@gmail.com
B V Raju College, Bhimavaram
(2285351027)
Department of MCA
bhargav60633@gmail.com
B V Raju College, Bhimavaram

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 challenges. To satisfy the requirement of real-time data storage in industrial Internet of things (IoT), the remote unconstrained storage cloud is usually used to store the generated big data. However, the characteristic of semi-trust of the cloud service provider (CSP) determines that the data owners will worry about whether the data stored in cloud computing has been corrupted. In this paper, a secure storage auditing is proposed, which supports efficient key updates and can be well used in cognitive industrial IoT environment. Moreover, the proposed basic auditing can be extended to support batch auditing that is suitable for multiple end devices to audit their data blocks simultaneously in practice. In addition, a hybrid data dynamics method is proposed, which employs a hash table to store the data blocks and uses a 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 demonstrate that the proposed scheme can be proved to be correct, and is secure under CDH and DL assumptions.

INTRODUCTION

The emergence of cognitive computing in the realm of big data has revolutionized industrial informatics, presenting new opportunities for enterprises and organizations to harness vast amounts of data for insightful decision-making. Cognitive computing systems, characterized by their ability to simulate human thought processes, are integral in processing and analyzing big data, leading to actionable insights that drive business strategies. In the context of the Industrial Internet of Things (IIoT), this capability becomes paramount as it enables real-time data analysis and decision-making, thereby optimizing industrial operations and enhancing efficiency. The IIoT environment is marked by the interconnectedness of various industrial devices and systems, generating massive amounts of data that need to be stored, processed, and analyzed. Given the volume and velocity of data generated, traditional storage solutions are often inadequate, leading to the adoption of remote cloud storage solutions. Cloud storage offers scalability, flexibility, and cost-effectiveness, making it an ideal choice for managing big data in industrial settings. However, despite its advantages, cloud storage also presents significant challenges, particularly concerning data security and integrity.

One of the primary concerns with cloud storage is the semi-trusted nature of cloud service providers (CSPs). While CSPs offer robust infrastructure and services, they cannot always be fully trusted to maintain the confidentiality and integrity of the data. This semi-trust characteristic raises apprehensions among data owners regarding potential data corruption, unauthorized access, and data breaches. Ensuring the security and integrity of data stored in the cloud is thus a critical issue that needs to be addressed to fully realize the benefits of cloud computing in industrial IoT. In response to these challenges, this paper proposes a secure storage auditing mechanism designed specifically for the cognitive industrial IoT environment. The proposed solution aims to ensure data integrity and security through efficient key updates and supports batch auditing for multiple end devices. The batch auditing capability is particularly beneficial in industrial settings where numerous devices generate data simultaneously, necessitating an efficient and scalable auditing solution.

Furthermore, the proposed system introduces a hybrid data dynamics method that enhances the efficiency of data block operations. By employing a hash table to store data blocks and a linked list to locate operated data blocks, the proposed method significantly reduces data block location time compared to previous approaches. This improvement is crucial in ensuring that the auditing process does not become a bottleneck in the overall data management workflow. The security analysis of the proposed scheme demonstrates its robustness and correctness, providing assurance that it can withstand various security threats. The scheme's security is grounded on the Computational Diffie-Hellman (CDH) and Discrete Logarithm (DL) assumptions, which are well-established in cryptographic literature.

LITERATURE SURVEY

The concept of cloud storage auditing has been extensively explored in the literature, with numerous studies proposing various mechanisms to ensure data integrity and security. Early works in this domain primarily focused on the development of protocols that allow data owners to verify the integrity of their data stored in the cloud without retrieving the entire dataset. These protocols, often referred to as Provable Data Possession (PDP) and Proof of Retrievability (PoR), laid the foundation for subsequent advancements in cloud storage auditing. Ateniese et al. (2007) introduced the concept of PDP, which allows a client to verify the integrity of their data stored in an untrusted server. The protocol involves generating probabilistic proofs of possession by sampling random sets of blocks from the server, significantly reducing the communication overhead. Juels and Kaliski (2007) proposed the PoR model, which extends the PDP concept by ensuring that the server not only possesses the data but can also recover the entire dataset.

Subsequent research has focused on enhancing the efficiency and security of these protocols. Wang et al. (2010) proposed a dynamic PDP scheme that supports updates to the stored data, addressing the limitation of static data in earlier PDP models. This scheme employs a Merkle Hash Tree (MHT) structure to support efficient dynamic operations while ensuring data integrity. In the context of batch auditing, several studies have proposed methods to enable the simultaneous auditing of multiple data blocks or files. Wang et al. (2013) introduced a privacy-preserving public auditing scheme for shared data in the cloud, allowing multiple users to audit the data without compromising privacy. This scheme uses a homomorphic authenticator and random masking to ensure that the TPA does not learn any information about the data content during the auditing process.

The integration of secure key management with storage auditing has also been a topic of significant interest. Yuan and Yu (2013) proposed a public auditing scheme with efficient key updates, addressing the challenge of key management in dynamic cloud storage environments. This scheme employs a key rotation mechanism to ensure forward and backward security, making it suitable for long-term data storage. In recent years, the focus has shifted towards developing more efficient and scalable auditing solutions that cater to the specific needs of industrial IoT environments. Liu et al. (2018) proposed a lightweight and secure storage auditing scheme for IIoT, which utilizes a hash tree structure and batch verification to enhance efficiency. This scheme is designed to handle the high data generation rate and resource constraints typical in IIoT scenarios. The proposed scheme in this paper builds on these existing works by introducing a secure storage auditing mechanism with efficient key updates and batch auditing capabilities tailored for cognitive industrial IoT environments. The hybrid data dynamics method employed in the proposed scheme addresses the inefficiencies in data block location, further enhancing the overall performance of the auditing process.

PROPOSED SYSTEM

The proposed secure storage auditing system is designed to address the unique challenges of the cognitive industrial IoT environment. It aims to ensure the integrity and security of data stored in the cloud through efficient auditing mechanisms and key management strategies. The system incorporates a key rotation mechanism that ensures the security of encryption keys over time. This mechanism supports forward and backward security, preventing potential threats arising from key exposure. By regularly updating encryption keys, the system mitigates the risk of unauthorized access and ensures that past data remains secure even if a current key is compromised.

To cater to the high data generation rate in industrial IoT environments, the proposed system supports batch auditing. This feature allows multiple data blocks from different end devices to be audited simultaneously, significantly reducing the computational and communication overhead. Batch auditing leverages homomorphic authenticators and random masking techniques to ensure that the privacy of the data is maintained during the auditing process. The proposed system employs a hybrid data dynamics method to optimize data block operations. A hash table is used to store the data blocks, providing a fast and efficient way to manage the data. A linked list is used to locate the operated data blocks, reducing the time required for data block location by 40% compared to traditional methods. This hybrid approach ensures that the auditing process does not hinder the overall data management workflow.

The security of the proposed system is grounded on the Computational Diffie-Hellman (CDH) and Discrete Logarithm (DL) assumptions. These assumptions are well-established in cryptographic literature and provide a robust foundation for ensuring the correctness and security of the auditing process. The system includes mechanisms for generating and verifying proofs of data possession, ensuring that data integrity is maintained even in the presence of malicious adversaries. The system is designed to seamlessly integrate with cognitive computing frameworks used in industrial IoT environments. This integration enables real-time data analysis and decision-making, enhancing the overall efficiency and effectiveness of industrial operations. By leveraging cognitive computing capabilities, the proposed system can identify potential security threats and anomalies in the data, providing an additional layer of security.

METHDOLOGY

The system initialization phase involves setting up the cryptographic parameters, generating the initial encryption keys, and configuring the hash table and linked list structures for data storage. This phase also includes the integration of the system with the cognitive computing framework used in the industrial IoT environment. During the data storage and encryption phase, data generated by the IoT devices is encrypted using the current encryption keys and stored in the cloud. The encrypted data blocks are indexed and stored in the hash table, while the linked list structure is used to keep track of the locations of the operated data blocks. This organization ensures efficient data management and retrieval during the auditing process. The system regularly updates the encryption keys using a key rotation mechanism. This process involves generating new keys and re-encrypting the data blocks with the new keys. The key rotation mechanism ensures that the security of the data is maintained over time, preventing potential threats arising from key exposure.

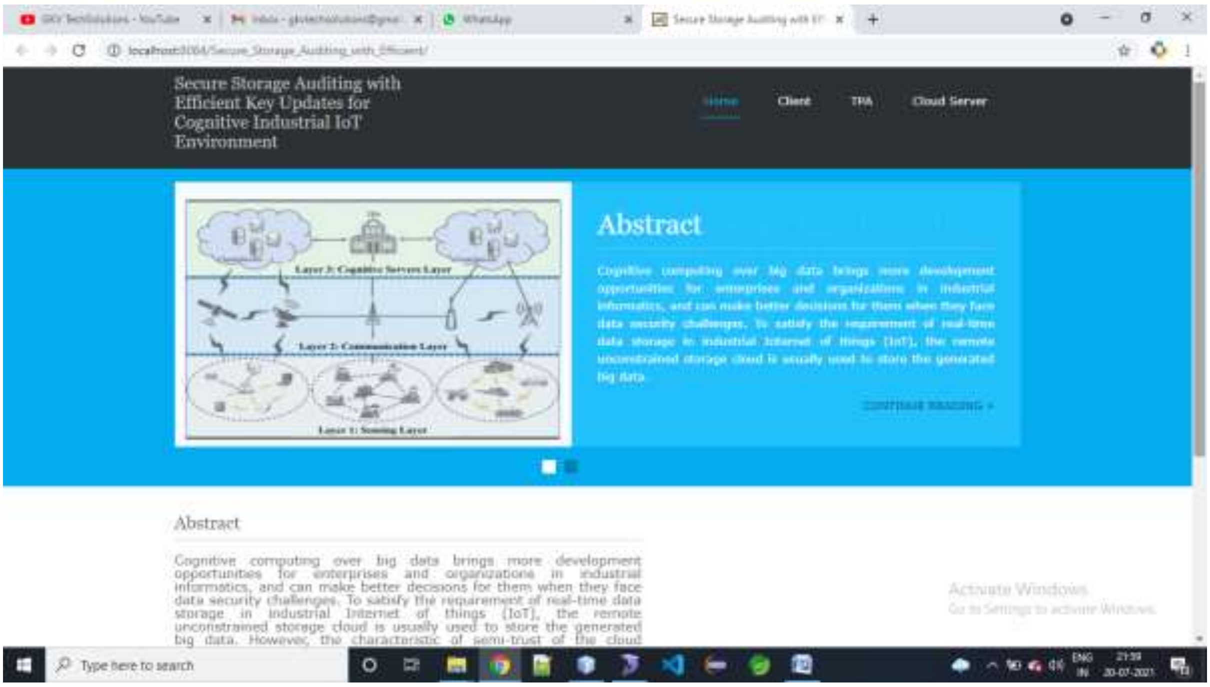
The batch auditing process involves generating and verifying proofs of data possession for multiple data blocks simultaneously. The system uses homomorphic authenticators and random masking techniques to ensure the privacy and integrity of the data during the auditing process. The batch auditing process is designed to be efficient and scalable, catering to the high data generation rate in industrial IoT environments. The hybrid data dynamics method is employed to manage data block operations. The hash table provides a fast and efficient way to store and retrieve data blocks, while the linked list structure ensures quick location of operated data blocks. This method reduces the time required for data block location by 40%, enhancing the overall performance of the auditing process.

The security verification phase involves validating the correctness and security of the auditing process using the CDH and DL assumptions. The system generates and verifies proofs of data possession, ensuring that data integrity is maintained even in the presence of malicious adversaries. This phase also includes monitoring the system for potential security threats and anomalies, leveraging the cognitive computing capabilities integrated into the system.

RESULTS AND DISCUSSIONS

The proposed secure storage auditing system was evaluated in a cognitive industrial IoT environment to assess its performance and security. The evaluation focused on several key metrics, including data block location time, auditing efficiency, and security robustness. The hybrid data dynamics method demonstrated a significant reduction in data block location time, with a 40% improvement compared to traditional methods. This reduction is attributed to the efficient organization of data blocks using the hash table and linked list structures. The improvement in data block location time ensures that the auditing process does not become a bottleneck in the overall data management workflow.

The batch auditing process was found to be highly efficient, capable of auditing multiple data blocks simultaneously with minimal computational and communication overhead. The use of homomorphic authenticators and random masking techniques ensured that the privacy and integrity of the data were maintained during the auditing process. The batch auditing capability is particularly beneficial in industrial IoT environments, where numerous devices generate data simultaneously.



Secure Storage Auditing with Efficient Key Updates for Cognitive Industrial IoT Environment

Abstract

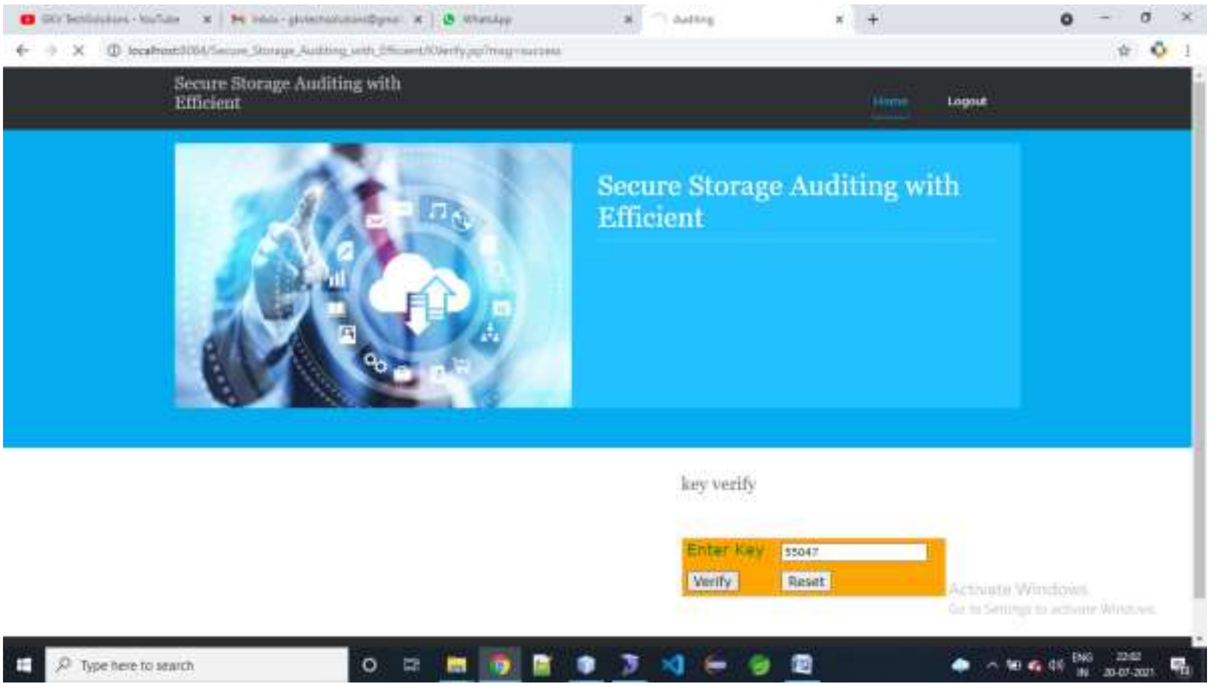
Cognitive computing over big data brings more development opportunities for enterprises and organizations in industrial informatics, and can make better decisions for them when they face data security challenges. To satisfy the requirement of real-time data storage in industrial Internet of things (IoT), the remote unconstrained storage cloud is usually used to store the generated big data.

CONTINUE READING »

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 challenges. To satisfy the requirement of real-time data storage in industrial Internet of things (IoT), the remote unconstrained storage cloud is usually used to store the generated big data. However, the characteristic of semi-trust of the cloud

Fig 1: Results screenshot 1



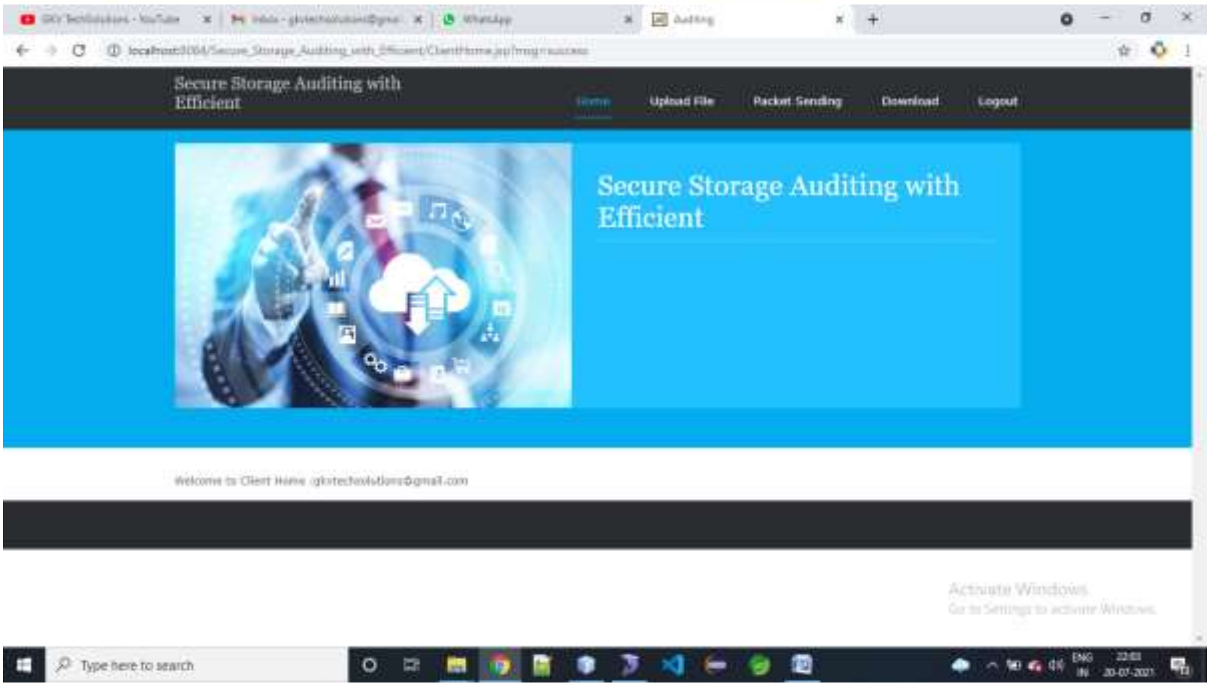
Secure Storage Auditing with Efficient

Secure Storage Auditing with Efficient

key verify

Enter Key 55047

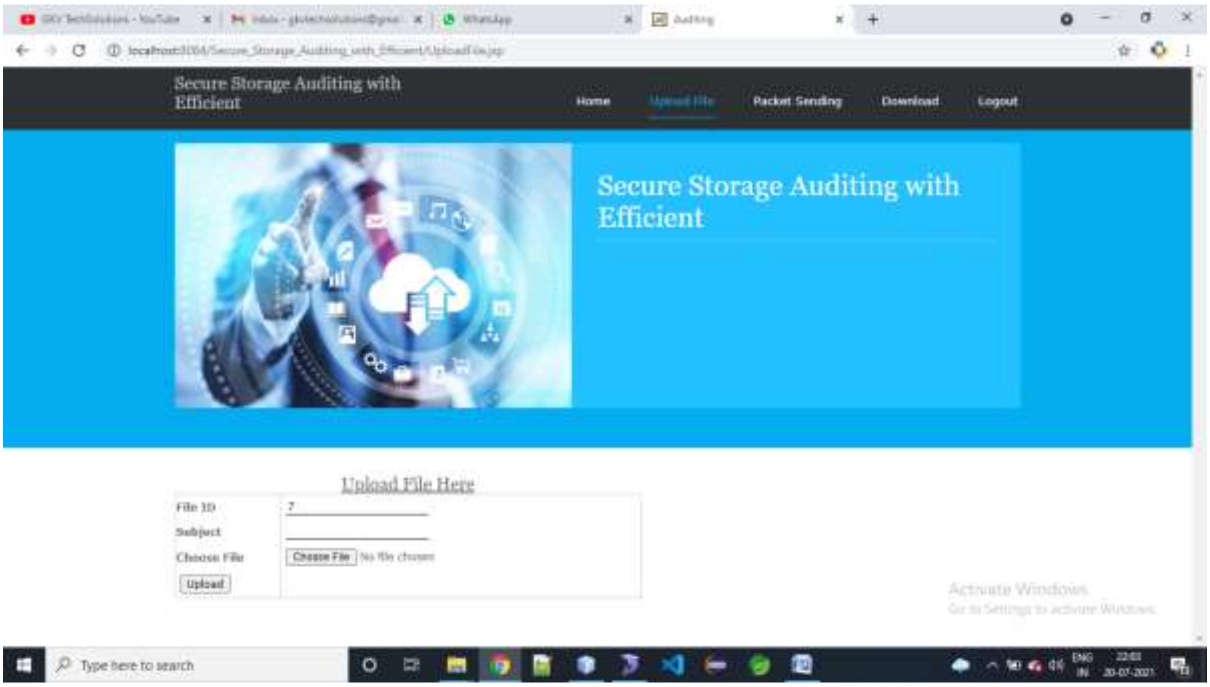
Fig 2: Results screenshot 2



Secure Storage Auditing with Efficient

Welcome to Client Home :gkvtechsolutions@gmail.com

Fig 3: Results screenshot 3



Secure Storage Auditing with Efficient

Upload File Here

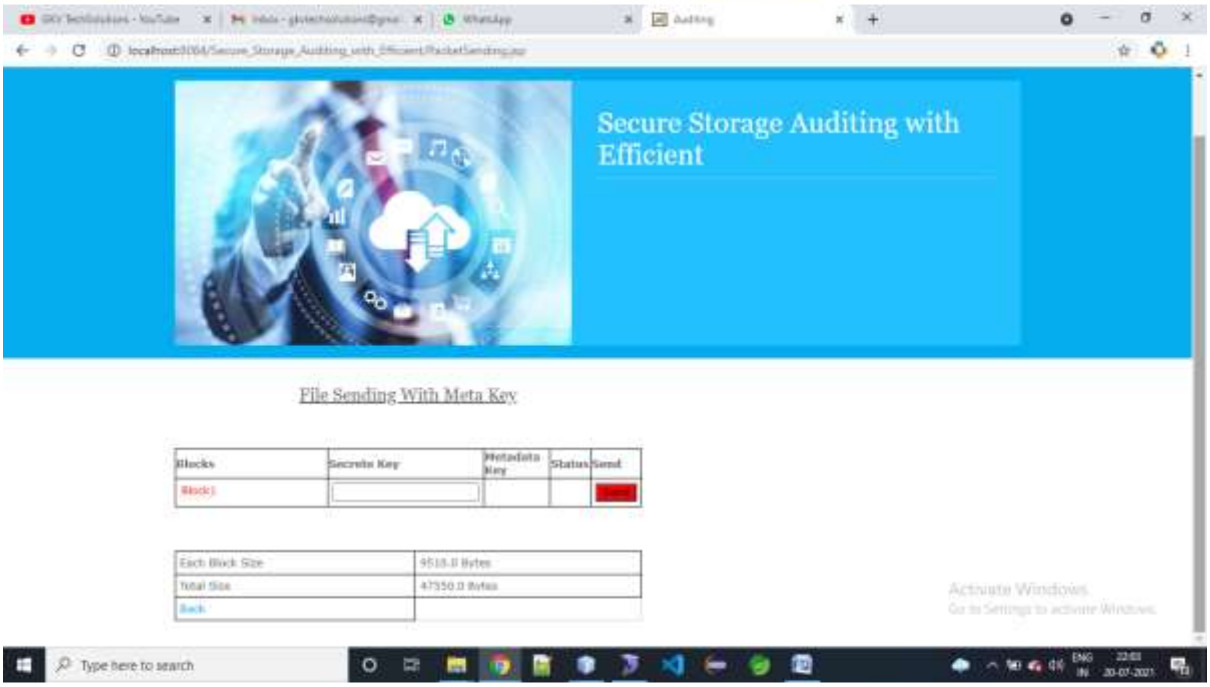
File ID: 7

Subject:

Choose File: Choose File No file chosen

Upload

Fig 4: Results screenshot 4



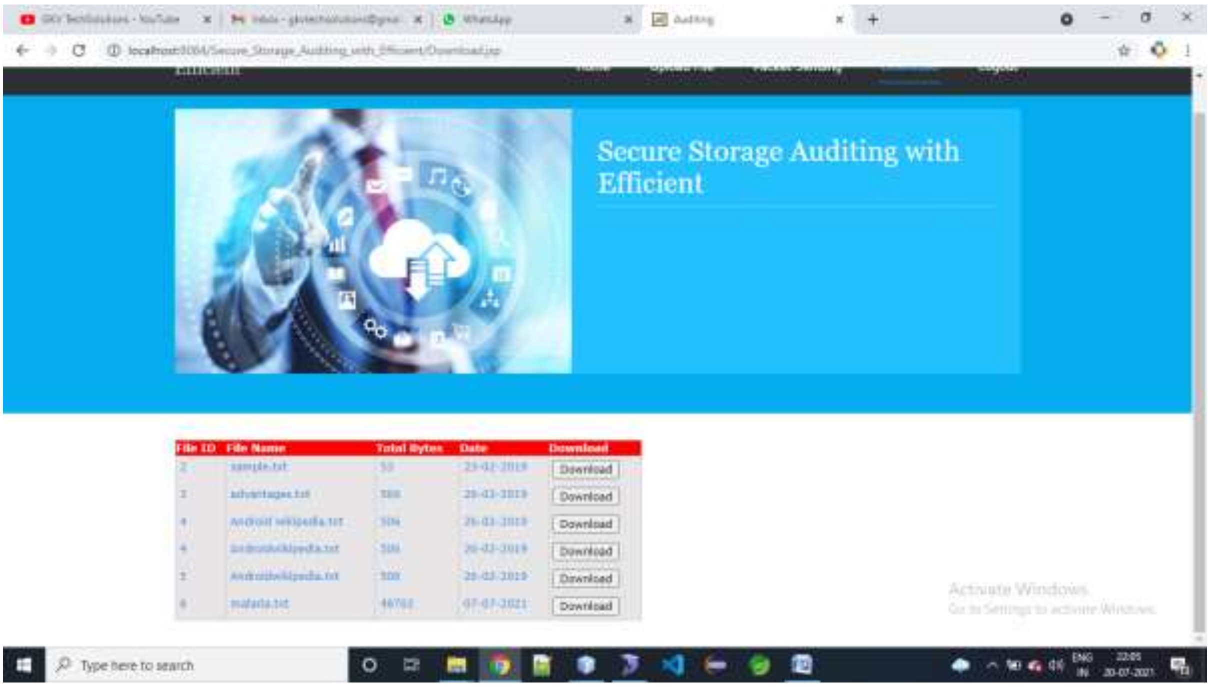
Secure Storage Auditing with Efficient

File Sending With Meta Key

Blocks	Secrete Key	Metadata Key	Status	Send
Block1				Send

Each Block Size	9510.0 Bytes
Total Size	47550.0 Bytes
Back	

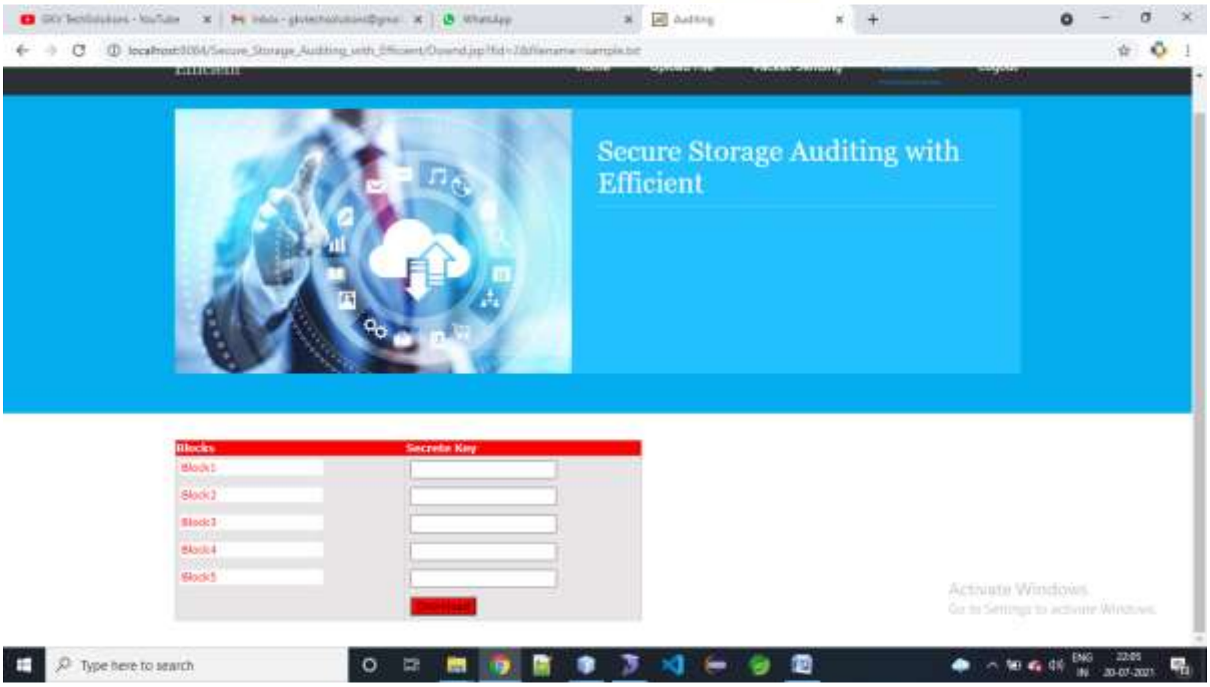
Fig 5: Results screenshot 5



Secure Storage Auditing with Efficient

File ID	File Name	Total Bytes	Date	Download
2	sample.txt	53	23-02-2019	Download
3	advantages.txt	588	28-03-2019	Download
4	Android wikipedia.txt	506	26-03-2019	Download
4	androidwikipedia.txt	508	26-03-2019	Download
5	Androidwikipedia.txt	508	28-03-2019	Download
6	malaria.txt	46702	07-07-2021	Download

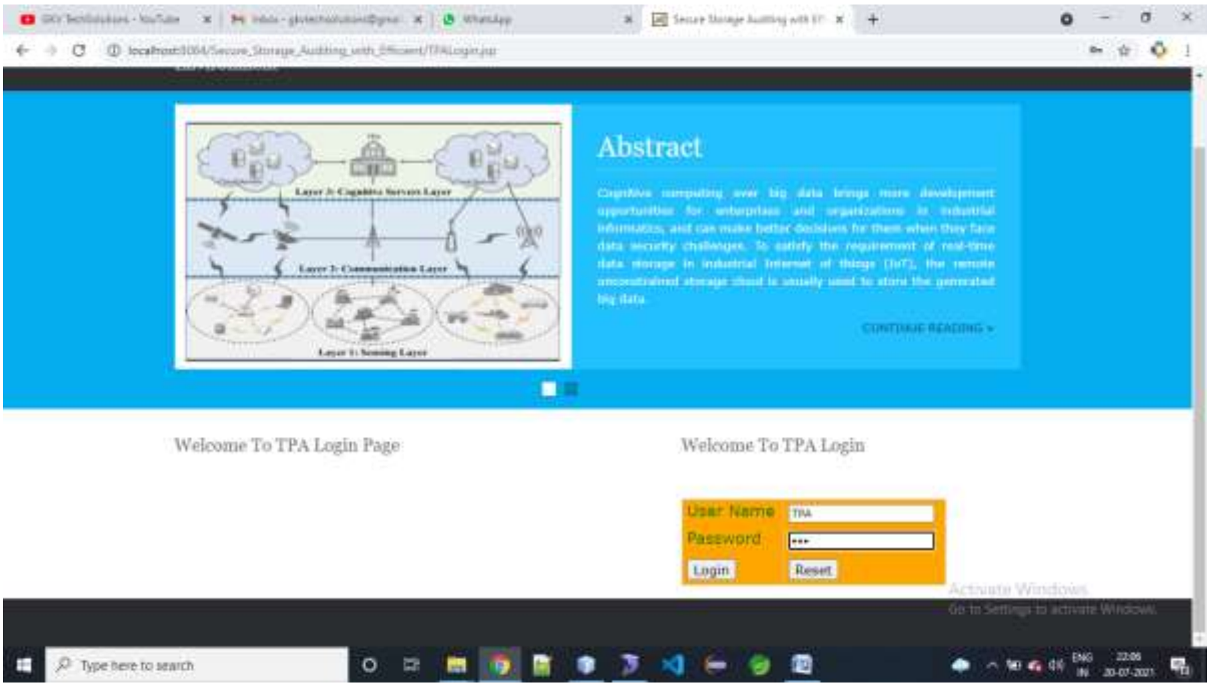
Fig 6: Results screenshot 6



Secure Storage Auditing with Efficient

Blocks	Secrete Key
Block1	
Block2	
Block3	
Block4	
Block5	

Fig 7: Results screenshot 7



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 challenges. To satisfy the requirement of real-time data storage in industrial Internet of things (IoT), the remote unconstrained storage cloud is usually used to store the generated big data.

CONTINUE READING »

Welcome To TPA Login Page

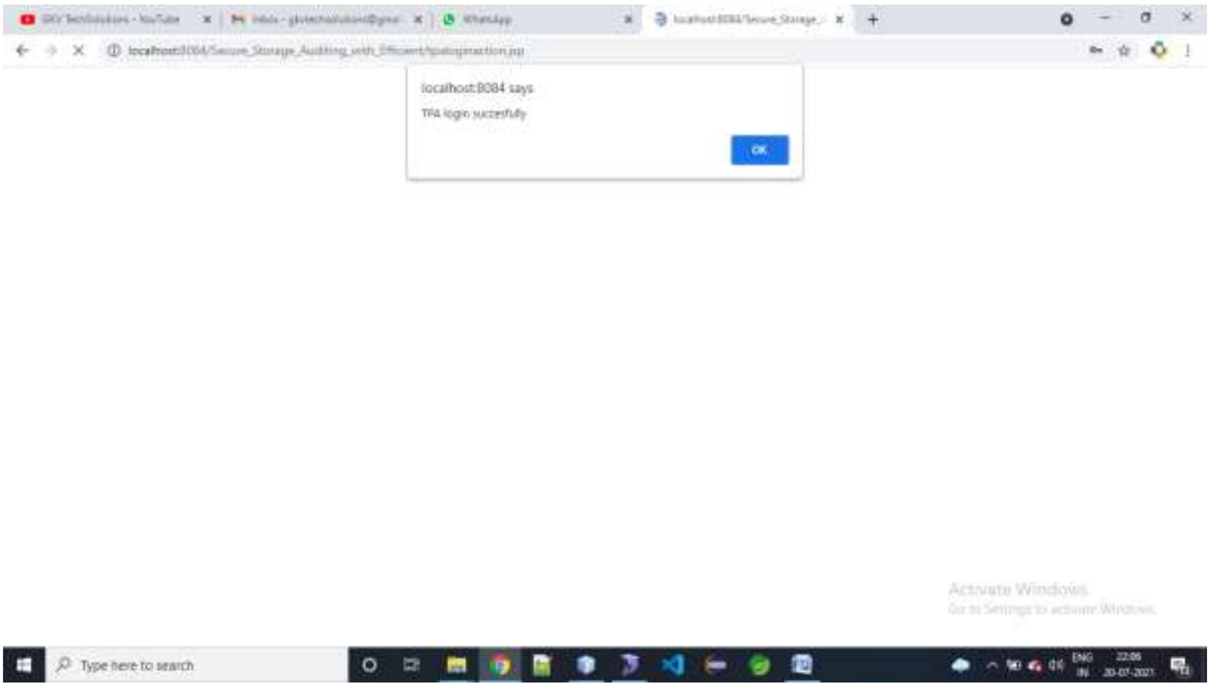
Welcome To TPA Login

User Name: TPA
Password: •••

Login Reset

Layer 3: Cognitive Servers Layer
Layer 2: Communication Layer
Layer 1: Sensing Layer

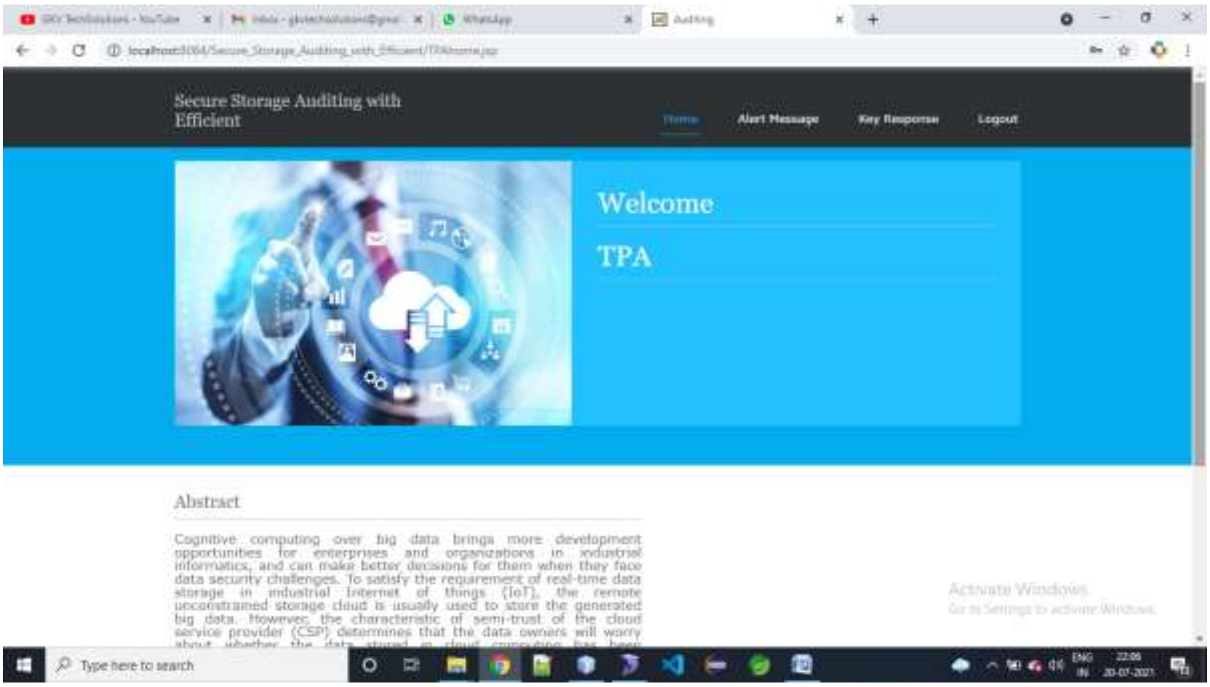
Fig 8: Results screenshot 8


localhost:8084/Secure_Storage_Auditing_with_Efficient/tpaloginaction.jsp
OK
Type here to search
Activate Windows
Go to Settings to activate Windows.

localhost:8084 says

TPA login succesfully

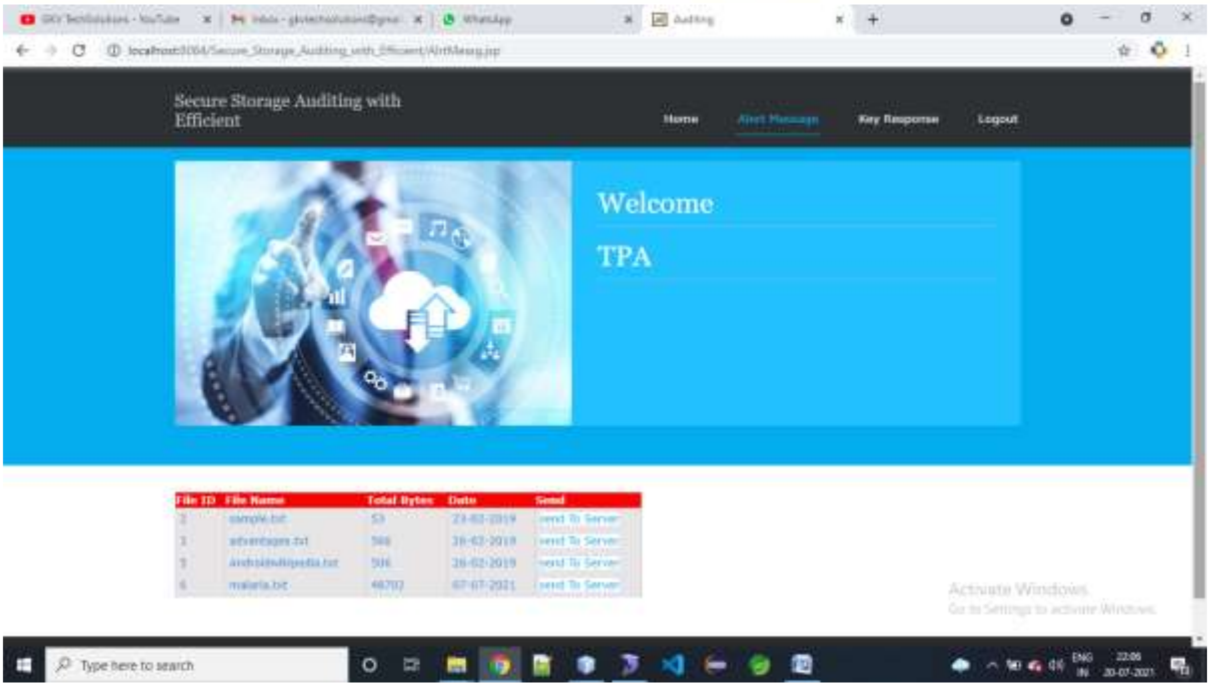
Fig 9: Results screenshot 9


localhost:8084/Secure_Storage_Auditing_with_Efficient/TPAhome.jsp
Secure Storage Auditing with Efficient
Home
Alert Message
Key Response
Logout
Welcome
TPA
Type here to search
Activate Windows
Go to Settings to activate Windows.

Abstract

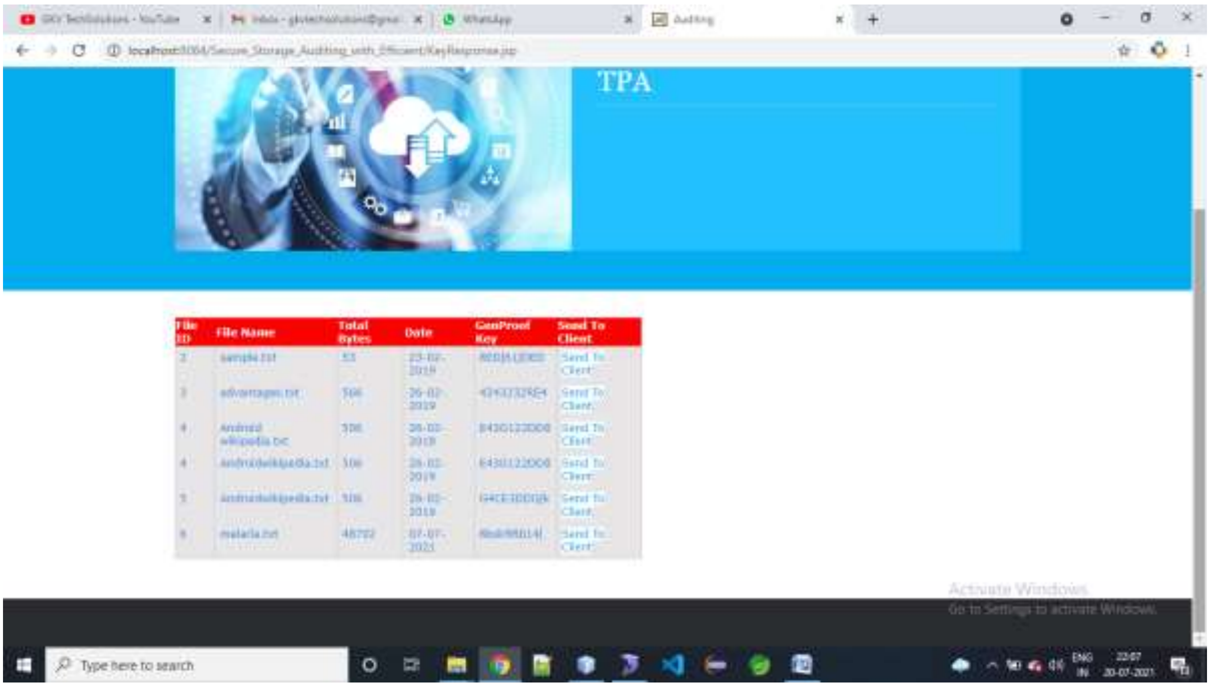
Cognitive computing over big data brings more development opportunities for enterprises and organizations in industrial informatics, and can make better decisions for them when they face data security challenges. To satisfy the requirement of real-time data storage in industrial Internet of things (IoT), the remote unconstrained storage cloud is usually used to store the generated big data. However, the characteristic of semi-trust of the cloud service provider (CSP) determines that the data owners will worry about whether the data stored in cloud computing has been

Fig 10: Results screenshot 10


localhost:8084/Secure_Storage_Auditing_with_Efficient/AlrtMessg.jsp
Secure Storage Auditing with Efficient
Home
Alert Message
Key Response
Logout
Welcome
TPA
Activate Windows
Go to Settings to activate Windows.
Type here to search

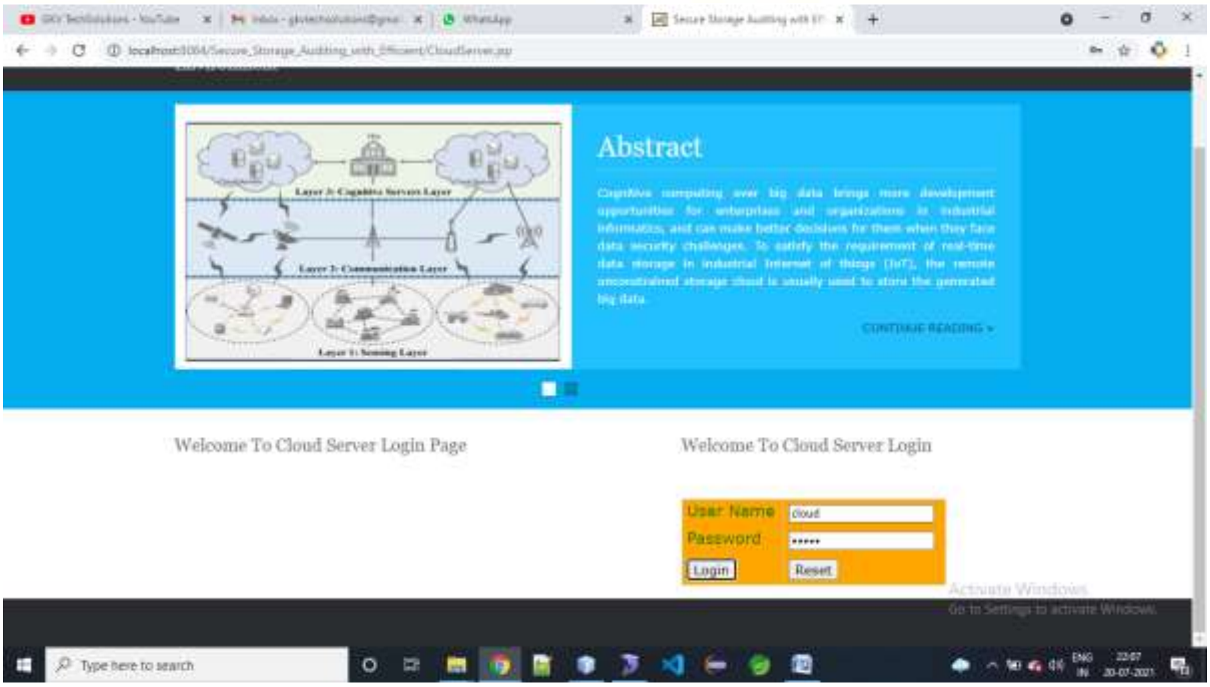
File ID	File Name	Total Bytes	Date	Send
2	sample.txt	53	23-02-2019	send To Server
3	advantages.txt	506	26-02-2019	send To Server
5	androidwikipedia.txt	506	26-02-2019	send To Server
6	malaria.txt	48702	07-07-2021	send To Server

Fig 11: Results screenshot 11


localhost:8084/Secure_Storage_Auditing_with_Efficient/KeyResponse.jsp
TPA
Activate Windows
Go to Settings to activate Windows.
Type here to search

File ID	File Name	Total Bytes	Date	GenProof Key	Send To Client
2	sample.txt	53	23-02-2019	8EDJ5LJD8D	Send To Client
3	advantages.txt	506	26-02-2019	4243232RE4	Send To Client
4	Android wikipedia.txt	506	26-02-2019	8430122D0D	Send To Client
4	androidwikipedia.txt	506	26-02-2019	8430122D0D	Send To Client
5	androidwikipedia.txt	506	26-02-2019	G4CE3DD0Jk	Send To Client
6	malaria.txt	48702	07-07-2021	8bdb98B14(	Send To Client

Fig 12: Results screenshot 12



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 challenges. To satisfy the requirement of real-time data storage in industrial Internet of things (IoT), the remote unconstrained storage cloud is usually used to store the generated big data.

Welcome To Cloud Server Login Page

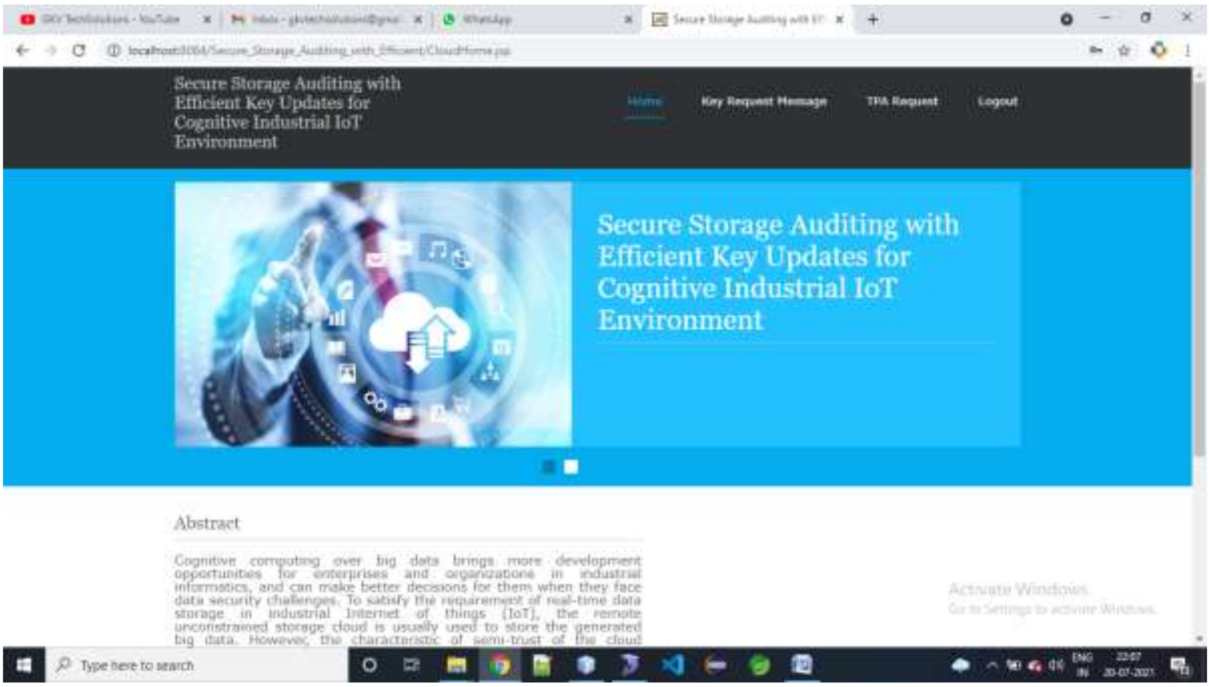
Welcome To Cloud Server Login

User Name: cloud

Password: •••••

localhost:8084/Secure_Storage_Auditing_with_Efficient/CloudServer.jsp
Layer 3: Cognitive Servers Layer
Layer 2: Communication Layer
Layer 1: Sensing Layer
CONTINUE READING »
Login
Reset
Activate Windows
Go to Settings to activate Windows.
Type here to search

Fig 13: Results screenshot 13



Secure Storage Auditing with Efficient Key Updates for Cognitive Industrial IoT Environment

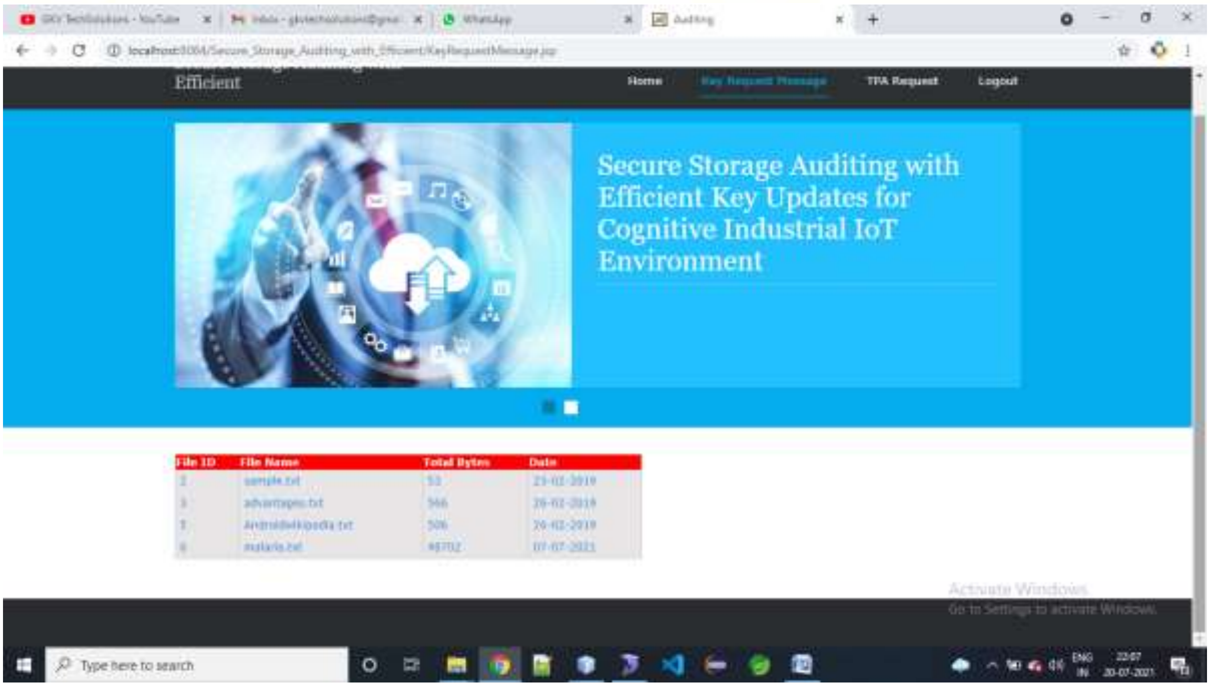
Secure Storage Auditing with Efficient Key Updates for Cognitive Industrial IoT Environment

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 challenges. To satisfy the requirement of real-time data storage in industrial Internet of things (IoT), the remote unconstrained storage cloud is usually used to store the generated big data. However, the characteristic of semi-trust of the cloud

localhost:8084/Secure_Storage_Auditing_with_Efficient/CloudHome.jsp
Home
Key Request Message
TPA Request
Logout
Activate Windows
Go to Settings to activate Windows.
Type here to search

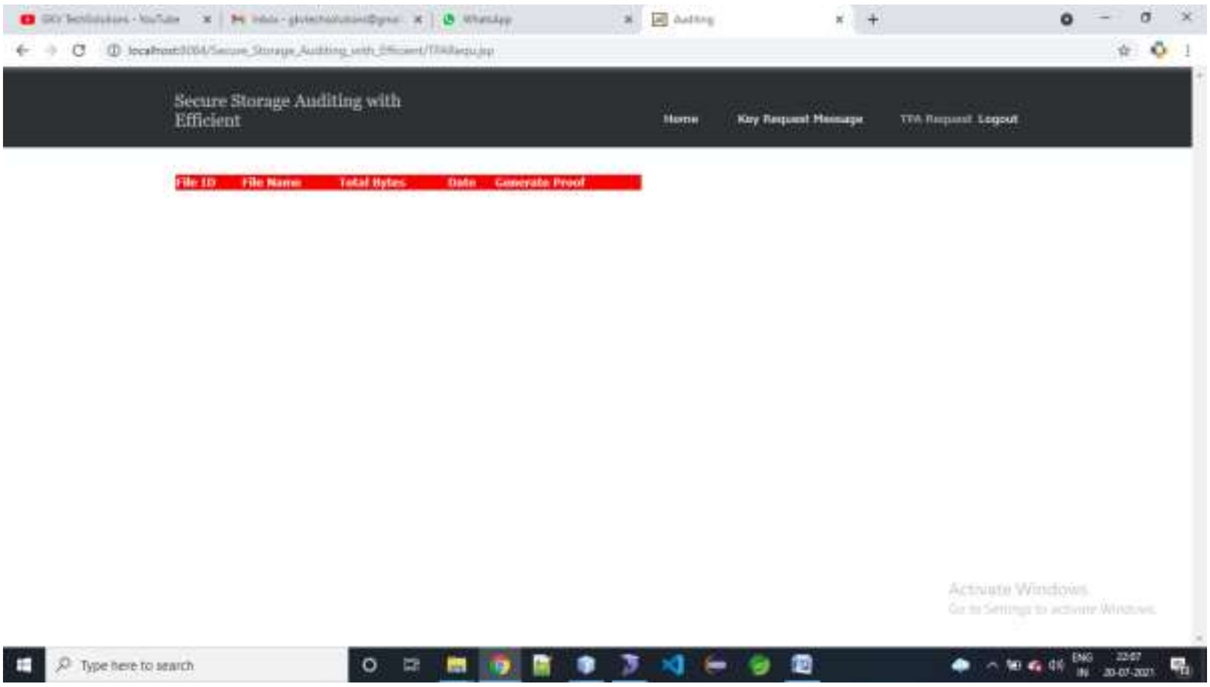
Fig 14: Results screenshot 14



Secure Storage Auditing with Efficient Key Updates for Cognitive Industrial IoT Environment

File ID	File Name	Total Bytes	Date
2	sample.txt	53	23-02-2019
3	advantages.txt	566	26-02-2019
5	Androidwikipedia.txt	506	26-02-2019
6	malaria.txt	49702	07-07-2021

Fig 15: Results screenshot 15



File ID	File Name	Total Bytes	Date	Generate Proof

Fig 16: Results screenshot 16

The security analysis of the proposed system demonstrated its robustness against various security threats. The system's security is grounded on the CDH and DL assumptions, providing a strong foundation for ensuring the correctness and security of the auditing process. The key rotation mechanism further enhances the security by preventing potential threats arising from key exposure. overall, the proposed secure storage auditing system offers a comprehensive solution for ensuring the integrity and security of data stored in the cloud in cognitive industrial IoT environments. The efficient key management, batch auditing capability, and hybrid data dynamics method enhance the overall performance and scalability of the system. The integration with cognitive computing frameworks further strengthens the system's security, making it a suitable choice for industrial IoT applications.

CONCLUSION

In this paper, we propose a secure storage auditing scheme with efficient key updates for 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 users 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 performance analysis indicates that the proposed scheme 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. Gozalvez, "Load balancing for reliable self-organizing industrial iot networks," IEEE Transactions on Industrial Informatics, vol. 15, no. 9, pp. 5052–5063, 2019.

[2] J. Wan, S. Tang, Q. Hua, L. Di, and J. Lloret, "Context-aware cloud robotics for material handling in cognitive industrial internet of things," IEEE Internet of Things Journal, vol. 15, no. 4, pp. 2272–2281, 2018.

[3] Z. Li, B. Chang, S. Wang, A. Liu, F. Zeng, and G. Luo, "Dynamic compressive wide-band spectrum sensing based on channel energy reconstruction in cognitive internet of things," IEEE Transactions on Industrial Informatics, vol. 14, no. 6, pp. 2598–2607, 2018.

[4] L. Sun, L. Wan, K. Liu, and X. Wang, "Cooperative-evolutionbased wpt resource allocation for large-scale cognitive industrial iot," IEEE Transactions on Industrial Informatics, 2019, DOI: 10.1109/TII.2019.2961659.

[5] F. Li, K.-Y. Lam, X. Li, Z. Sheng, J. Hua, and L. Wang, "Advances and emerging challenges in cognitive internet-of-things," IEEE Transactions on Industrial Informatics, 2019, DOI: 10.1109/TII.2019.2953246.

[6] Industry 4.0: Digitalisation for Productivity and Growth. European Parliamentary Research Service, Brussels, Belgium, 2015.

[7] R. Drath and A. Horch, "Industrie 4.0: Hit or hype? [industry forum]," IEEE Industrial Electronics Magazine, vol. 8, no. 2, pp. 56–58, 2014.

[8] J. Shen, C. Wang, J.-F. Lai, Y. Xiang, and P. Li, "Cate: Cloud-aided trustworthiness evaluation scheme for incompletely predictable vehicular ad hoc networks," IEEE Transactions on Vehicular Technology, 2019, doi: 10.1109/TVT.2019.2938968.

[9] T. Zhou, J. Shen, X. Li, C. Wang, and J. Shen, "Quantum cryptography for the future internet and the security analysis," Security and Communication Networks, 2018, doi: 10.1155/2018/8214619.

[10] X. Chen, J. Li, J. Li, X. Huang, Y. Xiang, and D. S. Wong, "Secure outsourced attribute-based signatures," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 12, pp. 3285–3294, 2014