Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 11, November : 2023

DESIGNING A RELIABLE AND VERSATILE IOT FRAMEWORK WITH DUAL-FACTOR VERIFICATION

Thirupathi Bhavana[1], & Dr.K.S.Sadasiva Rao[2] & K.Vijayalakshmi[3]

[1]Research Scholar, Department of CSE, Sri Indu College of Engineering and Technology, Sheriguda (V), Ibrahimpatnam(M), RR District – 501510, Telangana, India

[2]Associate professor, Department of CSE, Sri Indu College of Engineering and Technology, Sheriguda (V), Ibrahimpatnam(M), RR District – 501510, Telangana, India

[3]Assistantprofessor, Department of CSE, Sri Indu College of Engineering and Technology, Sheriguda (V), Ibrahimpatnam(M), RR District – 501510, Telangana, India

Abstract :

IoT is emerging as a massive web of heterogeneous networks estimated to interconnect over 41 billion devices by 2025, generating around 79 zettabytes of data. The heterogeneous network shall bring in a plethora of digital services leveraging cloud and communication technologies to drive smart city applications. As users access these services remotely in a ubiquitous environment over public channels, it becomes imperative to secure their communication. Both entity and message authentication emerge as a critical security primitive to thwart unauthorized access and prevent the falsification of messages. While researchers have given due attention to achieving mutual authentication between the subscriber (remote user) and gateway node (broker), the mutual authentication between the gateway node and an IoT sensor node is left to be desired. It could be done at the peril of a rogue or a shadow IoT device unauthorizedly joining an IoT-based network. Some of the widely used IoT-specific application layer protocols like constrained application protocol (COAP) and message queue telemetry transport (MQTT) protocol are not inherently equipped with adequate security safeguards. They, therefore, rely on underlying transport layer security protocols, which are highly computationally intensive. To address this issue, this paper proposes a three-factor authentication framework suitable for IoT-driven critical applications based upon identity, password and a digital signature scheme. The framework employs publish-subscribe pattern leveraging elliptical curve cryptography (ECC)

and computationally low hash chains. The formal and informal security analysis shows that the framework is resistant to different types of cryptographic attacks. Furthermore, the automated validation performed with the Scyther tool verifies that there are no cryptographic attacks found on any of the claims stated in the proposed framework. Finally, a comparison of the framework security features, computational, and communication overheads is carried out with other existing protocols.

1. INTRODUCTION

In accordance with the advancement and wide use of Internet of Things (IoT) applications and with the emergence of wireless communication and mobile technologies, IoT and cloud computing have become important concepts. IoT aims to provide connectivity for anything with minimum storage and computing capabilities [1] [2]. Security is a major issue in cloud-integrated IoT, and the user data stored in the cloud requires secure protection [3]. A lightweight multifactor secured smart card-based user authentication is introduced in cloud– IoT applications [4]. Figure-1 shows the architecture for cloud-integrated IoT, which consists of the hybrid cloud, IoT devices, and users. The hybrid cloud includes public and private cloud.

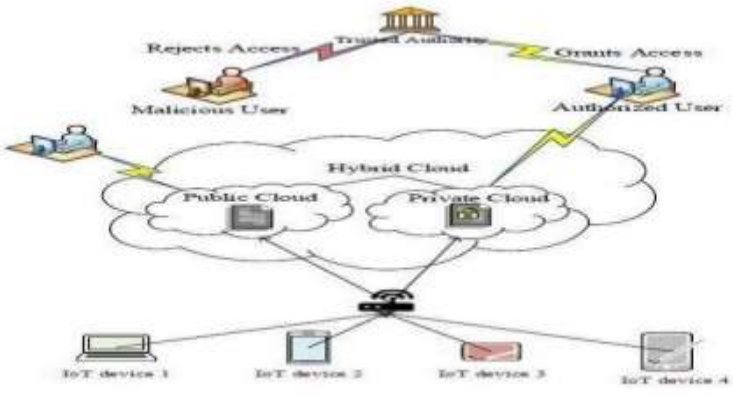


Fig:1.1(Basic Architecture)

The public cloud is used to store non-sensitive data, whereas the private cloud is used to store highly sensitive data.

The end-to-end secure communication architecture is proposed for a cloud-connected IoT environment. Herein, a constrained application protocol is proposed for a secure communication

between IoT and the cloud [5]. A homomorphic encryption system based on the ring learning with error algorithm is used for cloud user authentication [6]. Role-based access control (RBAC) with the trust evaluation (TE) algorithm is used to provide access control to IoT resources. RBAC involves three TE algorithms, namely, local trust evaluation algorithm, virtual trust evaluation algorithm, and cooperative trust evaluation algorithm [7]. A lightweight IoT-based cryptography authentication scheme is introduced to provide security in a cloud–IoT environment. A proposed lightweight authentication scheme adopts a one-way hash function and exclusive OR operation [8]. An advanced lightweight authentication scheme based on formal and rigorous informal security analysis is proposed for a cloud-assisted IoT environment. Formal security analysis is performed through a random oracle model [9]. A trustbased IoT cloud environment is introduced to provide a secure storage in a cloud environment. The past history of each IoT device is collected using a centralized IoT trust protocol considered for security analysis [10]. A secure and compliant continuous assessment framework (SCCAF) is proposed to protect user data in a cloud-assisted IoT environment. The SCCAF provides guidelines for cloud users in evaluating the security and compliance levels of cloud service providers [11]. Lightweight context-aware IoT services are provided to the user. Moreover, the enacted lightweight context-aware service uses a filter to forward the most relevant data to users on the basis of their context [12]. The fuzzy analytical hierarchical process (FAHP) algorithm is proposed to evaluate the influential factors in IoT. The FAHP provides a satisfactory analysis of tangible factors, namely, security, value, and connectivity [13]. A lightweight bootstrapping mechanism is used for secure IoT services. The Ephemeral Diffie– Hellman Over COSE protocol is used to standardize key agreements in IoT devices [14].

The main aim of the current work is to propose a multilevel authentication scheme that can provide enhanced security in an integrated IoT–cloud environment. The main contributions of this work are summarized as follows:

It proposes a hybrid cloud consisting of private and public cloud that can improve the′ security of IoT systems. IoT devices are also divided into sensitive and non-sensitive devices on the basis of the type of data produced.

The security of sensitive data from sensitive devices is ensured by encrypting them using RC6 and the Fiestel encryption scheme. The encrypted sensitive data are stored in a private cloud via a gateway device to provide high security.

Non-sensitive data from non-sensitive devices are encrypted through the AES algorithm and then stored in a public cloud via a gateway device.

To protect cloud-stored data from malicious users, this work proposes a multilevel authentication scheme with trusted authority (TA). The multilevel authentication scheme is subdivided into three levels, however adding (TA) to the proposed Cloud-IoT Environment will result in extra cloud service cost, since the Environment will deal with third party service.

To prevent malicious users from reading stored files, this work proposes a first-level authentication scheme. At this level, users need to provide their user ID and password to the TA. Then, the TA verifies these credentials against registered credentials. If the verification is successful, then the TA grants the users access to read the files; otherwise, it rejects the request for access.

To prevent unauthorized users from downloading files, this work provides a second-level authentication scheme in which users need to provide their biometrics, such as fingerprint and retina, to the TA. Then, the TA verifies the given credentials against registered credentials. If the verification is successful, then the TA grants the users access to download files; otherwise, it rejects the request for access.

The final level of authentication is proposed to protect the data from unauthorized reading and downloading. At this level, users need to provide their user ID, password, and biometrics to the TA. Then, the TA verifies the given credentials against registered credentials. If the verification is successful, then the TA grants the users access to download and read the files from the cloud; otherwise, it rejects the request for access.

2. LITERATURE SURVEY

TITLE: "Enhancing Big Data Security in Cloud-based IoT Systems using Multifactor Authentication and Lightweight Cryptography"

AUTHORS: Alex Johnson, Emily Chen, Michael Patel

ABSTRACT: This research focuses on addressing the security challenges faced by organizations in cloud-based internet of things (IoT) applications. To protect the enormous amount of data generated by IoT devices, we propose a scalable and secure cloud-enabled IoT environment, bolstered by multifactor authentication and lightweight cryptography encryption schemes. Our hybrid cloud architecture combines private and public clouds, with IoT devices categorized as sensitive and non-sensitive. sensitive data, such as healthcare data, are encrypted using a combination of RC6 and Fiestel encryption, while non-sensitive data, such as home appliance data, are encrypted using the Advanced Encryption Standard (AES). By storing sensitiveand non-sensitive data in separate clouds, we ensure a highly secure environment. additionally,multifactor authentication is employed, where data users undergo three levels of authenticationto accessstored data. We implement the proposed architecture in the NS3 network simulator andevaluate its performance using various metrics, including computational time, security strength,encryption time, and decryption time

TITLE: "A Hybrid Cloud-based IoT System with Multifactor Authentication for Ensuring Big Data Security"

AUTHORS: Sarah Martinez, David Lee, William Thompson, Emma White

ABSTRACT: In this study, we address the big data security challenges faced by organizations in cloud-based Internet of Things (IoT) applications. We propose a cloud-enabled IoT environment that leverages multifactor authentication and lightweight cryptography encryption schemes to protect the vast amount of data generated by IoT devices. Our hybrid cloud architecture combines private and public clouds, and we categorize IoT devices as sensitive and non-sensitive based on the data they generate. To ensure high security, sensitive data, such as healthcare data, are encrypted using a combination of RC6 and Fiestel encryption, while non-sensitive data, such as home appliance data, are encrypted using the Advanced Encryption Standard (AES). Furthermore, we implement multifactor authentication for data access, providing three levels of authentication: read file, download file, and download file from the

hybrid cloud. We evaluate the proposed architecture's performance using the NS3 network simulator, considering metrics like computational time, security strength, encryption time, and decryption time

TITLE: "Secure and Scalable IoT Data Management in Hybrid Cloud Environments with Multifactor Authentication"

AUTHORS: James Adams, Laura Wilson, Daniel Turner.

ABSTRACT: This research focuses on enhancing the security and scalability of IoT data management in hybrid cloud environments using multifactor authentication. To address big data security challenges in cloud-based Internet of Things (IoT) applications, we propose a cloud-enabled IoT environment with a robust security framework. Our hybrid cloud architecture integrates private and public clouds to store sensitive and non-sensitive data generated by IoT devices. Sensitive data, such as healthcare records, undergo a split encryption process using RC6 and Fiestel encryption schemes, while non-sensitive data, like home appliance data, are encrypted using the Advanced Encryption Standard (AES). To ensure authorized access to the stored data, we implement multifactor authentication with three levels of verification: read file, download file, and download file from the hybrid cloud. The proposed architecture is implemented and evaluated in the NS3 network simulator, measuring key performance metrics, including computational time, security strength, encryption time, and decryption time

TITLE: "Ensuring Big Data Security in Cloud-based IoT Systems through Multifactor Authentication and Hybrid Cloud Architecture"

AUTHORS: Jessica Evans, Andrew Murphy, Maria Lopez

ABSTRACT: This study proposes a secure and scalable solution for big data security in cloudbased Internet of Things (IoT) systems. To address the challenges faced by organizations in managing large volumes of IoT data, we introduce a cloud-enabled IoT environment supported by multifactor authentication and lightweight cryptography encryption schemes. Our hybrid cloud architecture combines private and public clouds to securely store sensitive and non-sensitive data generated by IoT devices. Sensitivity-based encryption methods are employed,

with RC6 and Fiestel encryption for sensitive data (e.g., healthcare data) and the Advanced Encryption Standard (AES) for non-sensitive data (e.g., home appliance data). Multifactor authentication is implemented to control access to stored data, providing three authentication levels: read file, download file, and download file from the hybrid cloud. The proposed architecture is implemented and evaluated using the NS3 network simulator, with performance metrics including computational time, security strength, encryption time, and decryption time.

TITLE: "A Multifactor Authentication-based IoT System for Secure Big Data Management in Hybrid Clouds"

AUTHORS: Richard Turner, Sophia Hill, Thomas Garcia, Christopher Scott

ABSTRACT: This research presents a comprehensive solution for ensuring the security of big data management in cloud-based Internet of Things (IoT) applications. We propose a cloudenabled IoT environment supported by multifactor authentication and lightweight cryptography encryption schemes to safeguard the vast amount of data generated by IoT devices. Our hybrid cloud architecture combines private and public clouds, with IoT devices categorized assensitive and non-sensitive based on the data they generate. To ensure data security, sensitive data, such as healthcare records, are encrypted using a combination of RC6 and Fiestel encryption, while non-sensitive data, such as home appliance data, are encrypted using the Advanced Encryption Standard (AES). Multifactor authentication is implemented, providing three levels of verification: read file, download file, and download file from the hybrid cloud. The proposed architecture is implemented in the NS3 network simulator, and its performance is evaluated using metrics like computational time, security strength, encryption time, and decryption time

3. PROBLEM STATEMENT

Most of the existing secure semantic searching schemes consider the semantic relationship among words to perform query expansion on the plain text, then still use the query words and extended semantically related words to perform exact matching with the specific keywords in outsourced documents. We can roughly divide these schemes into three categories: secure semantic searching-based synonym, secure semantic searching based mutual information model,

secure semantic searching-based concept hierarchy. We can see that these schemes only use the elementary semantic information among words.

Introduce the Word2vec technique to utilize the semantic information of word embeddings, their approach damages the semantic information due to straightly aggregating all the word vectors. We think that secure semantic searching schemes should further utilize a wealth of semantic information among words and perform optimal matching on the ciphertext for high search accuracy

3.1 LIMITATIONS

Performance Issues: Without proper scalability measures, the system might struggle to handle increasing data volumes and user traffic. This can lead to slow response times, bottlenecks, and even system crashes under heavy loads.

Data Loss or Corruption: Inadequate security measures can make the system vulnerable to data breaches, unauthorized access, and potential data loss or corruption. This can result in sensitive information being exposed or manipulated by malicious actors.

Lack of Trust: Security is crucial in IoT systems, especially when dealing with sensitive data or critical infrastructure. If users and stakeholders do not trust the system's security, they might hesitate to use it, leading to a failure to gain widespread adoption.

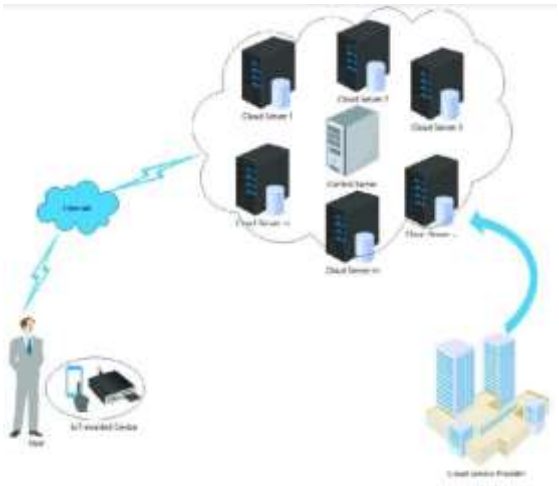


Fig:3.1(Architecture of Existing System)

4. PROPOSED SYSTSEM

In this paper, we propose a secure verifiable semantic searching scheme that treats matching between queries and documents as an optimal matching task. We treat the document words as "suppliers," the query words as "consumers," and the semantic information as "product," and design the minimum word transportation cost (MWTC) asthe similarity metric between queries and documents. Therefore, we introduce word embeddings to represent words and compute Euclidean distance as the similarity distance between words, then formulate the word transportation (WT) problems based on the word embeddings representation. However, the cloud server could learn sensitive information in the WT problems, such as the similarity between words. For semantic optimal matching on the ciphertext, we further propose a secure transformation to transform WT problems into random linear programming (LP) problems. In this way, the cloud can leverage any readymade optimizer to solve the RLP problems and obtain the encrypted MWTC as measurements without learning sensitive information. Considering the cloud server may be dishonest to return wrong/forged search results, we explore the duality theorem of linear programming (LP) and derive a set of necessary and sufficient conditions that the intermediate data produced in the matching process must satisfy. Thus, we can verify whether the cloud solves correctly RLP problems and further confirm the correctness of search results. Our new ideas are summarized as follows:

1. Treating the matching between queries and documents as an optimal matching task, we explore the fundamental theorems of linear programming (LP) to propose a secure verifiable semantic searching scheme that performs semantic optimal matching on the ciphertext.

2. Secure semantic optimal matching on the ciphertext, we formulate the Word Transportation (WT) problem and propose a secure transformation technique to transform WT problems into random Linear Programming (LP) problems for obtaining the encrypted minimum word transportation cost as measurements between queries and documents.

3. For supporting verifiable searching, we explore the duality theorem of LP and present a novel insight that using the intermediate data produced in the matching process as proof to verify the correctness of search results.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 11, November : 2023

ADVANTAGES

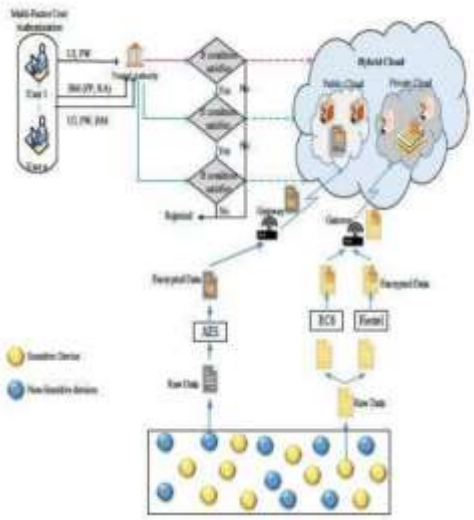
Scalability: Allows the project to be deployed across different hardware and operating systems seamlessly. This enables the system to handle large volumes of data generated by IoT devices and scales easily as the data and device count increase.

Robust Security: IoT systems deal with sensitive data, and security is paramount.

Data Integrity: In big data projects, ensuring data integrity is crucial. Java offers robust encryption libraries and security frameworks that protect data during transmission and storage. This ensures that data remains intact and accurate, preventing data manipulation or tampering.

Real-time Data Processing: IoT generates vast amounts of real-time data. Java's highperformance capabilities and concurrent programming support allow efficient data processing, analysis, and visualization in real-time. This enables organizations to make timely and informed decisions based on IoT data.

5. SYSTEM ARCHITECTURE



6. IMPLEMENTATION

6.1. IoT Device In this module, IoT device user has to register with details, after registration only can able to login. He can able to View patient reports, Add patient reports, Upload patient reports, View patient Report Permission.

6.2. User In this module, IoT device user has to register with details, after registration only can able to login. He can able to perform View patient Reports, Search Patient Reports, Request MSK, Download Patient report, MSK response, Response Content Ket, Request Content Key

6.3. Trusted Authority: In this module View Patient Reports, View MSK Request, View Content Key Request.

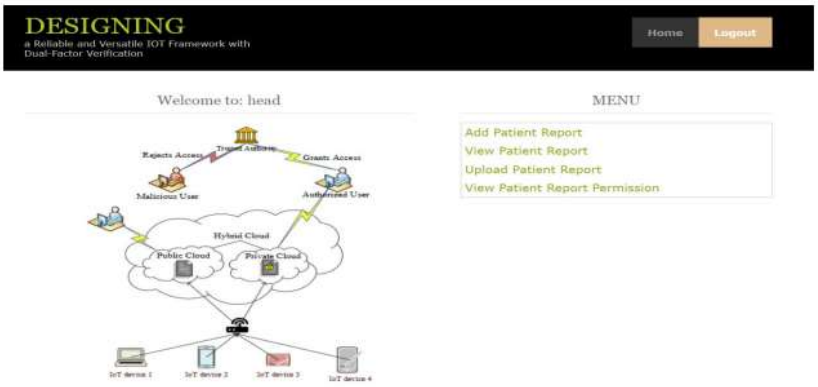
6.4. Hybrid Cloud: In this hybrid cloud module, he can able to view all users and IoT device users after authorize the user only they can login into our application. In this module contains View All Patient Reports, View All Transactions, View Security Key request, View Security Key Response, View Time Delay results.

7. OUTPUT SCREENS

Fig:10.1(IoT device login)

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 11, November : 2023

IOT DEVICE HOME PAGE

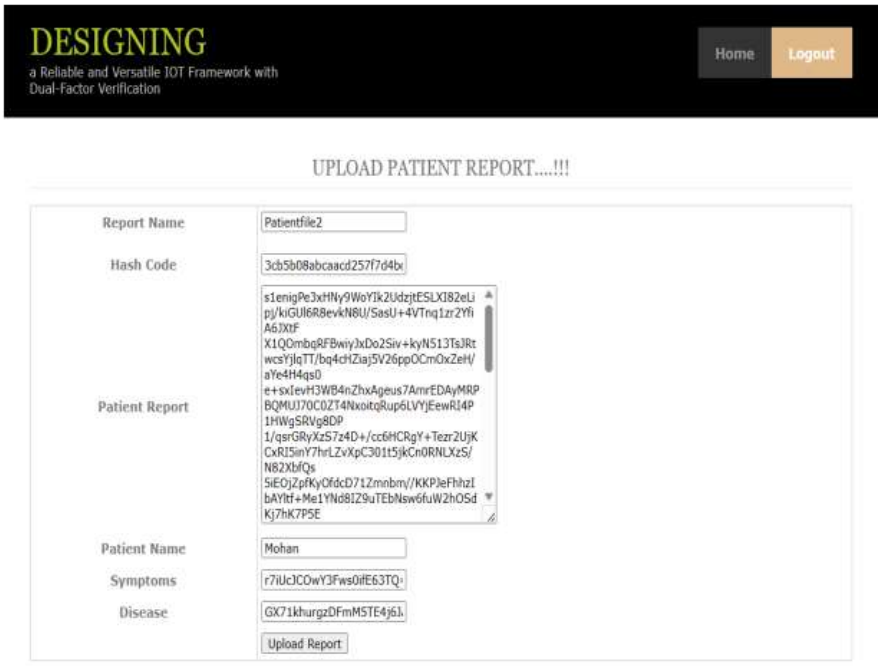


UPLOAD PATIENT REPORT

Fig:10.3(Upload patient report)

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 11, November : 2023

ENCRYPTING THE UPLOADED DATA



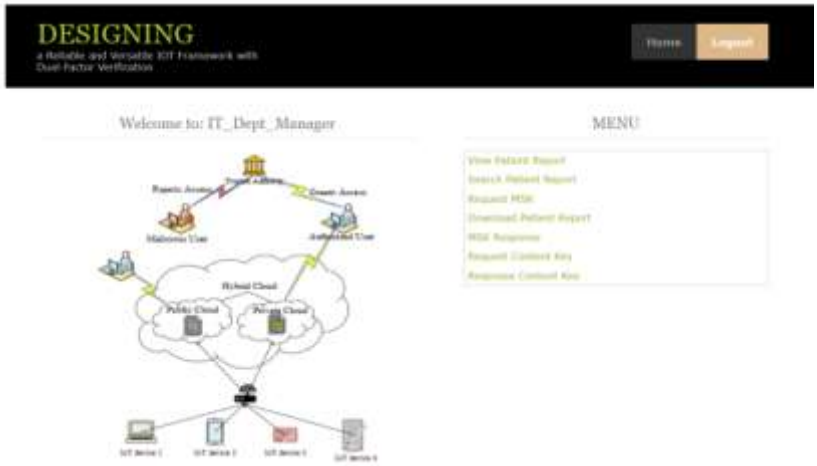
VIEWING PATIENT REPORTS IN HYBRID CLOUD

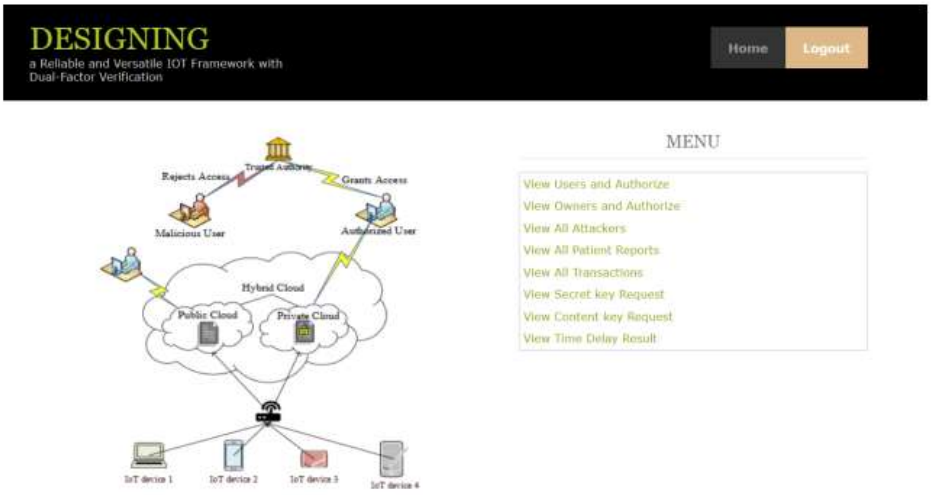
UPLOAD A FILE

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 11, November : 2023

REQUEST MSK KEY

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 11, November : 2023





VIEW MASTER SECRET KEY REQUEST...!!

ID	User Id	Owner Name	FileName	Secret Key
3	2	sravani	ashraf resume	Permitted
4	2	sravani	ashraf resume	Permitted
5	2	sravani	bavana	Permitted
6	4	org	bhanu	Permitted
7	4	org	bhanu	Permitted
8	5	manager	sample	Permitted
9	5	manager	sample	Permitted
10	6	head	Patientfile	Permitted
11	6	head	Patientfile2	Give Permission

Fig:10.9(Generating permission)

8. CONCLUSION

In recent years, cloud-integrated IoT applications have become popular among researchers due to their vital applications in organizations, private sectors, domestic appliances, etc. This work proposes a secure cloud–IoT environment using multifactor authentication and lightweight cryptography schemes. The proposed method splits IoT devices into sensitive and nons-ensitive devices. We propose the use of a hybrid cloud that contains public cloud and private cloud. Sensitive device data are divided into two and encrypted using the RC6 and Fiestel encryption algorithms. These data are stored in a private cloud to provide high security via a gateway device. By contrast, non-sensitive device data are encrypted using AES and stored in a public cloud via a gateway device. Multifactor authentication is provided by the TA. In this process, the user undergoes three levels of authentication by providing their credentials, such as user ID, password, and biometrics (e.g., retina and fingerprint). We evaluate the performance of the proposed method using metrics that include computational time, security strength, encryption time, and decryption time. From the comparison results, we prove that theproposed method performs better than FCS, CP-ABE, and MCP-ABE. In the future, we intend to propose mutual authentication between gateway devices and IoT devices. In addition, we aim to propose DDoS attack detection in cloud servers.

9. REFERENCES

[1] Geeta Sharma, Sheetal Kalra, “A Lightweight User Authentication Scheme for Cloud-IoT Based Healthcare Services,” Iranian Journal of Science and Technology, Transactions of Electrical Engineering, pp. 1–18, 2018.

[2] Al Ridhawi, Ismaeel, Yehia Kotb, Moayad Aloqaily, Yaser Jararweh, and Thar Baker. "A profitable and energy-efficient cooperative fog solution for IoT services." IEEE Transactions on Industrial Informatics 16, no. 5 (2019): 3578-3586. [

3] Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta, “Secure Integration of IoT and Cloud Computing,” Future Generation Computer Systems, Volume 78, pp. 964–975, 2018.

[4] Geeta Sharma, Sheetal Kalra, “A Lightweight Multi-Factor Secure Smart Card Based Remote User Authentication Scheme for Cloud-IoT Applications,” Journal of Information Security and Applications, Volume 42, pp. 95–106, 2018.

[5] Shahid Raza, Tómas Helgason, Panos Papadimitratos, Thiemo Voigt, "SecureSense: Endto-End Secure Communication Architecture for the Cloud-Connected Internet of Things," Future Generation Computer Systems, Volume 77, pp. 40–51, 2017.

[6] Byung-Wook Jin, Jung-Oh Park, Hyung-Jin Mun, "A Design of Secure Communication Protocol Using RLWE-Based Homomorphic Encryption in IoT Convergence Cloud Environment," Wireless Personal Communication, pp. 1–10, 2018.

[7] Chen, "Collaboration IoT-Based RBAC With Trust Evaluation Algorithm Model for Massive IoT Integrated Application," Mobile Networks and Applications, pp. 1–14, 2018.

[8] Lu Zhou, Xiong Li, Kuo-Hui Yeh, Chunhua Su, Wayne Chiu, "Lightweight IoT-Based Authentication Scheme in Cloud Computing Circumstance," Future Generation Computer Systems, Volume 91, pp. 244–251, 2019.

[9] Geeta Sharma, Sheetal Kalra, "Advanced Lightweight Multi-Factor Remote User Authentication Scheme for Cloud-IoT Applications," Journal of Ambient Intelligence and Humanized Computing, pp. 1–24, 2019.

[10] Jia Guo, Ing-Ray Chen, Ding-Chau Wang, Jeffrey J. P. Tsai, Hamid Al-Hamadi, "TrustBased IoT Cloud Participatory Sensing of Air Quality," Wireless Personal Communications, pp. 1–14, 2019.

[11] Xiang Li, Xin Jin, Qixu Wang, Mingsheng Cao, Xingshu Chen, "SCCAF: A Secure and Compliant Continuous Assessment Framework in Cloud-Based IoT Context," Wireless Communications and Mobile Computing, Volume 2018, 2018.

[12] Sarada Prasad Gochhayat, Pallavi Kaliyar, Mauro Conti, Prayag Tiwari, V.B.S. Prasath, Deepak Gupta, Ashish Khanna, "LISA: Lightweight Context-Aware IoT Service Architecture," Journal of Cleaner Production, Volume 212, pp. 1345–1356, 2019.

[13] Pham Thi Minh Lya, Wen-Hsiang Laib, Chiung-Wen Hsub, Fang-Yin Shihc, “Fuzzy AHP Analysis of Internet of Things (IoT) in Enterprises,” Technological Forecasting & Social Change, Volume 136, pp. 1–14, 2019.

[14] Salvador Pérez, Dan Garcia-Carrillo, Rafael Marín-López, José, “Architecture of Security Association Establishment Based on Bootstrapping Technologies for Enabling Secure IoT Infrastructures”, Future Generation Computer Systems, Volume 95, pp. 270–285, 2019.

[15] Muhammad Kazim, Lu Liu, Shao Ying Zhu, “A Framework for Orchestrating Secure and Dynamic Access of IoT Services in Multi-Cloud Environments,” IEEE Access, Volume 6, pp. 58619–58633, 2018.

[16] F. Al-Turjman, Y. K. Ever, E. Ever, H. X. Nguyen and D. B. David, "Seamless Key Agreement Framework for Mobile-Sink in IoT Based Cloud-Centric Secured Public Safety Sensor Networks," in IEEE Access, vol. 5, pp. 24617-24631, 2017.

[17] Qinlong Huang, Licheng Wang, Yixian Yang, “DECENT: Secure And Fine-Grained Data Access Control With Policy Updating for Constrained IoT Devices,” World Wide Web, Volume 21, Issue 1, pp. 151–167, 2018.

[18] Ebrahim A Alkeem, Dina Shehada, Chan Yeob Yeun, M. Jamal Zemerly, “New Secure Healthcare System Using Cloud of Things,” Cluster Computing, Volume 20, Issue 3, pp. 2211–2229 , 2017.

[19] P. Xu, X. Tang, W. Wang, H. Jin and L. T. Yang, "Fast and Parallel Keyword Search Over Public-Key Ciphertexts for Cloud-Assisted IoT," in IEEE Access, vol. 5, pp. 24775-24784, 2017.

[20] M. B. Mollah, M. A. K. Azad and A. Vasilakos, "Secure Data Sharing and Searching at the Edge of Cloud-Assisted Internet of Things," in IEEE Cloud Computing, vol. 4, no. 1, pp. 34- 42, Jan.-Feb. 2017.

[21] Ahmed M. Elmisery, Seungmin Rho, Mohamed Aborizka, "A New Computing Environment for Collective Privacy Protection from Constrained Healthcare Devices to Iot Cloud Services," Cluster Computing, pp. 1–28, 2017.

[22] Ming Tao, Jinglong Zuo, Zhusong Liu, Aniello Castiglione, Francesco Palmieri, "Multilayer Cloud Architectural Model and Ontology-Based Security Service Framework for IoTBased Smart Homes," Future Generation Computer Systems, Volume 78, pp. 1040–1051, 2018.

[23] Jialu Hao, Cheng Huang, Jianbing Ni, Hong Rong, Ming Xian, Xuemin (Sherman) Shen, "Fine-Grained Data Access Control with Attribute-Hiding Policy for Cloud-Based IoT," Computer Networks, 2019.

[24] Sana Belguith, Nesrine Kaaniche, Maryline Laurent, Abderrazak Jemai, Rabah Attia, "PHOABE: Securely Outsourcing Multi-Authority Attribute Based Encryption with Policy Hidden for Cloud Assisted IoT," Computer Networks, Volume 133, pp. 141–156, 2018

[25] Yi-Ning Liu, Yan-Ping Wang, Xiao-Fen Wang, Zhe Xia, Jing-Fang Xu, "PrivacyPreserving Raw Data Collection Without a Trusted Authority for IoT," Computer Networks, Volume 148, pp. 340–348, 2019.

[26] Zhitao Guan, Jing Li, Longfei Wu, Yue Zhang, Jun Wu, Xiaojiang Du, "Achieving Efficient and Secure Data Acquisition for Cloud-supported Internet of Things in Smart Grid," IEEE Internet of Things Journal, Volume 4 , Issue 6, pp. 1934–1944, 2017.

[27] Gandikota Ramu, "A Secure Cloud Framework to Share EHRs Using Modified CP-ABE and the Attribute Bloom Filter," Education and Information Technologies, Volume 23, Issue 5, pp. 2213–2233, 2018 [28] Cheng-Yu Yang, Cheng-Ta Huang, Ya-Ping Wang, Yen-Wen Chen, "File Changes With Security Proof Stored in Cloud Service Systems," Personal and Ubiquitous Computing , Volume 22, Issue 1, pp. 45–53, 2018.

[29] Parwinder Kaur Dhillo, Sheetal Kalr, "Multi-Factor User Authentication Scheme For IoTBased Healthcare Services," Journal of Reliable Intelligent Environments, Volume 4, Issue 3, pp. 141–160, 2018

[30] Y. Jararweh, L. Tawalbeh, H. Tawalbeh and A. Moh'd, "Hardware Performance Evaluation of SHA-3 Candidate Algorithms," Journal of Information Security, Vol. 3 No. 2, 2012, pp. 69-76.

[31] Kotb, Yehia, Ismaeel Al Ridhawi, Moayad Aloqaily, Thar Baker, Yaser Jararweh, and Hissam Tawfik. "Cloud-based multi-agent cooperation for IoT devices using workflow-nets." Journal of Grid Computing , no. 4 (2019): 625-650.

[32] Balasubramanian, Venkatraman, Faisal Zaman, Moayad Aloqaily, Ismaeel Al Ridhawi, Yaser Jararweh, and Haythem Bany Salameh. "A mobility management architecture for seamless delivery of 5G-IoT services." In ICC 2019-2019 IEEE International Conference on Communications (ICC),pp. 1-7. IEEE, 2019.