Efficient and Robust Big Data IoT Security System Utilizing MultiFactor Authentication and Lightweight Cryptography

Vodnala Sathvika
Scholar, Department of MCA
Vaageswari College Of Engineering-Karimnagar

P.Sathish
Assistant professor, DepartmentOf MCA
Vaageswari College Of Engineering-Karimnagar

Dr.V.Bapuji
Professor&Head, DepartmentOf MCA
Vaageswari College Of Engineering-Karimnagar

ABSTRACT: The utilization of cloud computing solutions for IoT applications is becoming increasingly popular among businesses. Integrating IoT devices with cloud computing technology is one approach to managing the vast amount of data generated by these devices. However, businesses face challenges in ensuring the security of large data within the IoT-cloud architecture. To safeguard the big data system and address security concerns, we propose an IoT environment that is cloud-enabled and supported by multifactor authentication and lightweight cryptographic encryption methods. By integrating features from both public and private clouds, this hybrid setup aims to enhance the security of businesses' data. Our setup classifies Internet of Things devices as either sensitive or nonsensitive. Electronic devices that do not generate particularly sensitive data, such as home appliances, utilize the Advanced Encryption Standard (AES), whereas devices that do generate sensitive data, such as healthcare records, use the RC6 and Fiestel encryption techniques. Public and private clouds are used to store encrypted sensitive and nonsensitive data, respectively, to provide the highest level of security. Access to data stored in the cloud also utilizes multifactor authentication. Users input their registered credentials when logging in to access the data, and the Trusted Authority (TA) uses them to provide three layers of authentication: one for reading files, another for downloading files, and a third for downloading files from the hybrid cloud. Computing time, security strength, encryption time, and decryption time are some of the metrics used to evaluate the proposed cloud-IoT architecture, which is built using the NS3 network simulator.

Keywords – Big data, cloud computing, Internet of Things, multilevel authentication, lightweight cryptography.

1.INTRODUCTION

With the rise of wireless and mobile technologies and the proliferation of IoT applications, cloud computing and the IoT have assumed a more pivotal role. The objective of establishing device connection via the Internet of Things is to integrate low-power computing and storage devices [1, 2]. Securing user data saved in the cloud is of the utmost importance in cloud-integrated Internet of Things scenarios [3]. We propose a straightforward user authentication mechanism for cloud-IoT applications that makes use of smart cards that are secured by many factors [4]. +

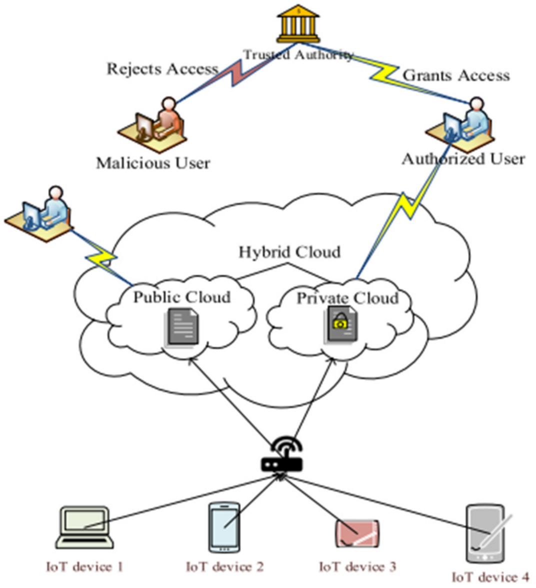


Figure.1: Cloud-Integrated IoT Architecture

The cloud-integrated IoT architecture shown in Figure 1 consists of end users, Internet of Things (IoT) devices, and a hybrid cloud. The hybrid cloud combines elements of both public and private clouds. Public clouds are better suited to storing less sensitive data, whilst private clouds are better suited for storing more sensitive data. It is advised that in an IoT setting that is connected to the cloud, an end-to-end secure communication architecture be used. Presented in this research [5] is a restricted application protocol for secure cloud-to-IoT communication. Cloud user authentication makes use of a ring learning with error–based homomorphic encryption scheme [6]. When the trust evaluation (TE) method is used with role-based access control (RBAC), it becomes much simpler to implement access control on resources inside the Internet of Things (IoT). Remote branch authentication and authorization (RBAC) makes use of three different types of trust evaluation algorithms (TE): virtual, cooperative, and local [7]. To provide an authentication method based on lightweight IoT cryptography to ensure security inside an IoT and hybrid cloud environment. One lightweight authentication solution uses a one-way hash function and an exclusive OR operation [8]. Following extensive formal and informal security research, it is advised to use a sophisticated lightweight authentication mechanism with cloud support in an Internet of Things (IoT) setting. Formal security analysis may make use of a random oracle model [9]. The introduction of a trust-based cloud ecosystem for the IoT enables secure cloud storage. Security analysis considers historical data collected from all IoT devices using a centralized trust mechanism [10]. To ensure the security of user data in an IoT context that utilizes the cloud, we recommend implementing a secure and compliant continuous assessment framework (SCCAF). The SCCAF provides criteria that cloud customers may utilize to evaluate the security and compliance levels of cloud service providers [11]. Internet of Things services that are both lightweight and context aware are made available to users. Moreover, the deployed lightweight context-aware service employs a filter to provide users with the data that is most relevant to their current situation [12]. The fuzzy analytical hierarchical process (FAHP) approach is suggested for evaluating key IoT variables. When it comes to evaluating concrete attributes, FAHP excels in determining value, connectedness, and security [13]. Using a lightweight bootstrapping strategy ensures that IoT services are safe. The Ephemeral Diffie-Hellman Over COSE protocol is useful for standardizing important agreements in IoT devices [14].

2.LITERATURE REVIEW

Geeta Sharma and Sheetal Kalra propose that with the ongoing revolution of cloud computing and the Internet of Things (IoT), remote patient monitoring has become feasible. These networking paradigms are widely used to provide healthcare services and real-time patient monitoring. Sensors, either wearable or embedded within a patient's body, transmit patient data to remote medical centers. Medical professionals can access this data stored in the cloud from anywhere across the globe. Since the sensitive data of patients is sent over insecure cloud-IoT networks, secure user authentication is of utmost importance. An efficient user authentication scheme ensures that only legitimate users can access data and services. This paper proposes a secure and efficient user authentication scheme for remote patient monitoring. The proposed scheme is robust, lightweight, and secure against multiple security attacks. Furthermore, the scheme has low computational overhead. A formal verification using the AVISPA tool confirms the security of the proposed scheme.

Moayad Aloqaily, Yaser Jararweh, and Thar Baker discuss the concept of fog-to-fog communication, which has been introduced to deliver services to clients with minimal reliance on the cloud through resource and capability sharing of cooperative fogs. Current solutions assume full cooperation among the fogs to deliver simple and composite services. Realistically, each fog might belong to a different network operator or service provider and thus will not participate in any form of collaboration unless self-monetary profit is incurred. In this paper, they introduce a fog collaboration approach for simple and complex multimedia service delivery to cloud subscribers while achieving shared profit gains for the cooperating fogs. The proposed work dynamically creates short-term service-level agreements (SLAs) offered to cloud subscribers for service delivery while maximizing user satisfaction and fog profit gains. The solution provides a learning mechanism that relies on online and offline simulation results to build guaranteed workflows for new service requests. The configuration parameters of the short-term SLAs are obtained using a modified tabu-based search mechanism that uses previous solutions when selecting new optimal choices. Performance evaluation results demonstrate significant gains in terms of service delivery success rate, service quality,reduced power consumption for fog and cloud data centers, and increased fog profits.

Kostas E. Psannis, Byung-Gyu Kim, and Brij Gupta explain that fog-to-fog communication has been introduced to deliver services to clients with minimal reliance on the cloud through resource and capability sharing of cooperative fogs. Current solutions assume full cooperation among the fogs to deliver simple and composite services. Realistically, each fog might belong to a different network operator or service provider and thus will not participate in any form of collaboration unless self-monetary profit is incurred. In this paper, they introduce a fog collaboration approach for simple and complex multimedia service delivery to cloud subscribers while achieving shared profit gains for the cooperating fogs. The proposed work dynamically creates short-term SLAs offered to cloud subscribers for service delivery while maximizing user satisfaction and fog profit gains. The solution provides a learning mechanism that relies on online and offline simulation results to build guaranteed workflows for new service requests. The configuration parameters of the short-term SLAs are obtained using a modified tabu-based search mechanism that uses previous solutions when selecting new optimal choices. Performance evaluation results demonstrate significant gains in terms of service delivery success rate, service quality, reduced power consumption for fog and cloud data centers, and increased fog profits.

Geeta Sharma and Sheetal Kalra note that with the rapid spread of cloud computing and the ever-increasing big data generated by the Internet of Things (IoT), remote user authentication poses a significant challenge. IoT is a paradigm where every device in the Internet Infrastructure (II) is interconnected into a globally dynamic expanding network. This paper proposes a novel remote user authentication scheme for cloud-IoT applications. The scheme is lightweight, robust against attacks, and has low computational overhead. The proposed scheme satisfies the essential attributes of security. A formal verification performed using the AVISPA tool confirms the security of the proposed scheme.

Panos Papadimitratos and Thiemo Voigt describe that the Constrained Application Protocol (CoAP) has become the de facto web standard for the IoT. Unlike traditional wireless sensor networks, Internet-connected smart thing deployments require security. CoAP mandates the use of the Datagram TLS (DTLS) protocol as the underlying secure communication protocol. In this paper, they implement DTLS-protected secure CoAP for both resource-constrained IoT devices and a cloud backend, and evaluate all three security modes (pre-shared key, raw-public key, and certificate-based) of CoAP in a real cloud-connected IoT setup. They extend SicsthSense—a cloud platform for the IoT—with secure CoAP capabilities and complement a DTLS implementation for resource-constrained IoT devices with raw-public key and certificate-based asymmetric cryptography. To the best of their knowledge, this is the first effort toward providing end-to-end secure communication between resource-constrained smart things and cloud back-ends, supporting all three security modes of CoAP both on the client and server sides. SecureSense—their End-to-End (E2E) secure communication architecture for the IoT—consists of all standard-based protocols, and the implementation of these protocols is open source and BSD-licensed. The SecureSense evaluation benchmarks and open-source, open-license implementation make it possible for future IoT product and service providers to account for security overhead while using all standardized protocols and ensuring interoperability among different vendors. The core contributions of this paper are: (i) a complete implementation for CoAP security modes for E2E IoT security, (ii) IoT security and communication protocols for a cloud platform for the IoT, and (iii) detailed experimental evaluation and benchmarking of E2E security between a network of smart things and a cloud platform.

3.PROBLEM STATEMENT

Existing secure semantic searching schemes typically expand queries based on semantic relationships among words in plaintext. They then perform exact matching using these query words and their semantically related counterparts against specific keywords in outsourced documents. These schemes can be roughly categorized into three types:

Secure semantic searching based on synonyms

Secure semantic searching using mutual information models

Secure semantic searching utilizing concept hierarchies

However, these approaches rely on basic semantic relationships among words. While Word2vec has been introduced to leverage word embeddings' semantic information, its method of directly aggregating word vectors often damages the semantic integrity. We argue that secure semantic searching should fully exploit the rich semantic information among words and achieve optimal matching on ciphertext to enhance search accuracy.

4.METHODOLOGY

In this paper, we propose a secure, verifiable semantic searching scheme that treats the matching between queries and documents as an optimal matching task. I conceptualize document words as “suppliers,” query words as “consumers,” and the semantic information as the “product.” I design the minimum word transportation cost (MWTC) to measure similarity between queries and documents. Using word embeddings to represent words and computing the Euclidean distance as the similarity metric, to formulate word transportation (WT) problems based on these embeddings.

However, directly handling WT problems could expose sensitive information, such as word similarities, to the cloud server. To ensure semantic optimal matching on ciphertext, to introduce a secure transformation that converts WT problems into random linear programming (LP) problems. This allows the cloud to use any existing optimizer to solve the RLP problems and produce encrypted MWTC measurements without revealing sensitive information.

To counter the potential dishonesty of cloud servers, which might return incorrect or forged results, I leverage the duality theorem of linear programming (LP). To derive a set of necessary and sufficient conditions that the intermediate data from the matching process must satisfy. This enables us to verify the cloud’s solution to the RLP problems and ensure the correctness of the search results.

Our contributions are summarized as follows:

It treats the matching between queries and documents as an optimal matching task and develop a secure, verifiable semantic searching scheme based on the fundamental theorems of linear programming (LP), enabling semantic optimal matching on ciphertext.

For secure semantic optimal matching on ciphertext, It formulate the word transportation (WT) problem and introduce a secure transformation to convert WT problems into random linear programming (LP) problems. This transformation ensures that encrypted minimum word transportation costs serve as the

To support verifiable searching, we explore the duality theorem of LP. We propose using the intermediate data from the matching process as proof to verify the correctness of the search results, ensuring the reliability of the cloud server's solutionssimilarity measurements between queries and documents.

5.SYSTEM ARCHITECTURE

The proposed cloud-enabled IoT architecture comprises IoT devices (categorized into sensitive devices (S1, S2, ... Sn) and non-sensitive devices (NS1, NS2, ... NSn)), a hybrid cloud (private and public cloud), a Trusted Authority (TA), users, and a gateway, as illustrated in Figure 2. To protect cloud-stored data from unauthorized access, to implement multifactor authentication for users. Additionally, data from IoT devices are encrypted using RC6 and Feistel encryption schemes to ensure security.

Sensitive data from sensitive IoT devices are encrypted using RC6 and Feistel encryption before being stored in the private cloud. This ensures high security for highly sensitive data and prevents forging. Non-sensitive data from non-sensitive IoT devices are encrypted using the AES algorithm and stored in the public cloud, as this data is less sensitive.

The gateway device routes sensitive and non-sensitive data to the private and public clouds, respectively. To maintain high security for stored information, we enforce user authentication to access stored files. The TA manages user authentication through registered credentials, including user ID, password, and biometric data (e.g., fingerprint or retina scans).

The authentication process comprises three levels:

First Level: The TA verifies the username and password to grant read access to files in the public cloud.

Second Level: For downloading files from the public cloud, the user is authenticated using biometrics, such as fingerprint or retina scans.

Third Level: For accessing files in the private cloud, the TA verifies the user ID, password, and biometrics to provide read and download access.

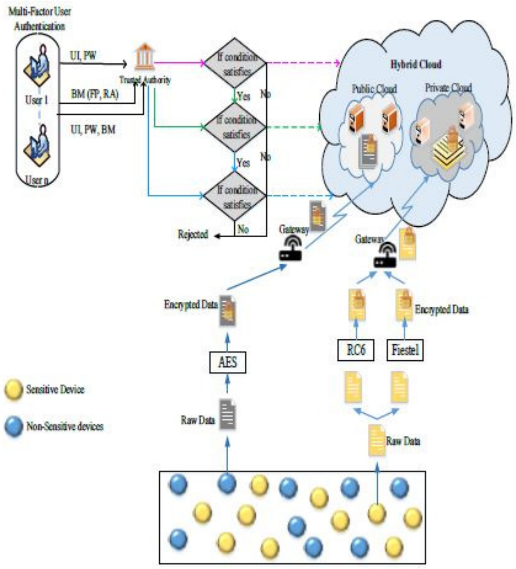


Figure.2: System Architecture

Figure 2 illustrates the proposed architecture, which includes four key entities: the hybrid cloud, IoT devices, the gateway, and the TA.

6. IMPLEMENTATION

MODULE DESCRIPTIONS:

1.IoT Device User: In this module, the IoT Device user is required to register with their personal details to gain access to the system. After successful registration, they can log in and utilize the features available to them. These features include viewing patient reports, adding new patient reports, uploading patient reports, and viewing permissions associated with patient reports.

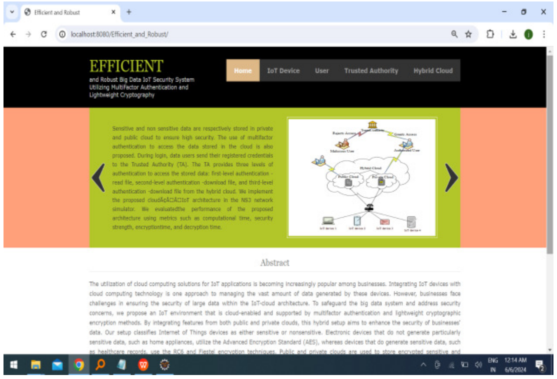
2.User: Similar to the IoT Device user, the user must also register with their personal details to access the system. Post-registration, users can log in and perform various tasks such as viewing patient reports, searching for specific patient reports, requesting the Master Security Key (MSK), downloading patient reports, receiving responses related to MSK requests, requesting content keys, and receiving responses for content key requests.

3.Trusted Authority: This module is designed for the Trusted Authority, who has the ability to oversee several critical functions. The Trusted Authority can view patient reports, monitor MSK requests, and track content key requests, ensuring the security and integrity of the system.

4.Hybrid Cloud: The Hybrid Cloud module is managed by the cloud administrator who has comprehensive oversight of the system. The administrator can view all users and IoT Device users, authorize users for application access, view all patient reports, monitor all transactions, manage security key requests and responses, and review time delay results. This module ensures that the cloud environment is secure and efficiently managed.

7.RESULTS

Home Page

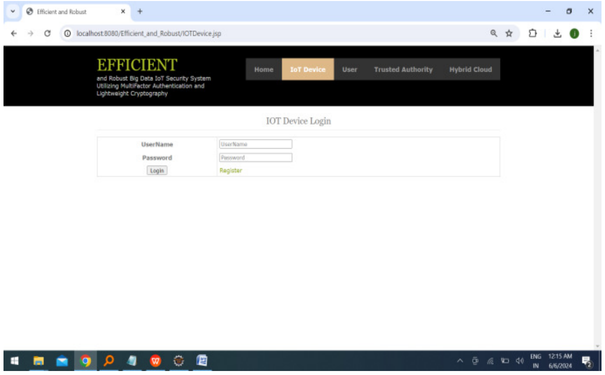


Sensitive and non sensitive data are respectively stored in private and public cloud to ensure high security. The use of multifactor authentication to access the data stored in the cloud is also proposed. During login, data users send their registered credentials to the Trusted Authority (TA). The TA provides three levels of authentication to access the stored data: first-level authentication - read file, second-level authentication -download file, and third-level authentication -download file from the hybrid cloud. We implement the proposed cloudÃ¢Â□Â□IoT architecture in the NS3 network simulator. We evaluatedthe performance of the proposed architecture using metrics such as computational time, security strength, encryptiontime, and decryption time.

Abstract

The utilization of cloud computing solutions for IoT applications is becoming increasingly popular among businesses. Integrating IoT devices with cloud computing technology is one approach to managing the vast amount of data generated by these devices. However, businesses face challenges in ensuring the security of large data within the IoT-cloud architecture. To safeguard the big data system and address security concerns, we propose an IoT environment that is cloud-enabled and supported by multifactor authentication and lightweight cryptographic encryption methods. By integrating features from both public and private clouds, this hybrid setup aims to enhance the security of businesses' data. Our setup classifies Internet of Things devices as either sensitive or nonsensitive. Electronic devices that do not generate particularly sensitive data, such as home appliances, utilize the Advanced Encryption Standard (AES), whereas devices that do generate sensitive data, such as healthcare records, use the RC6 and Fiestel encryption techniques. Public and private clouds are used to store encrypted sensitive and

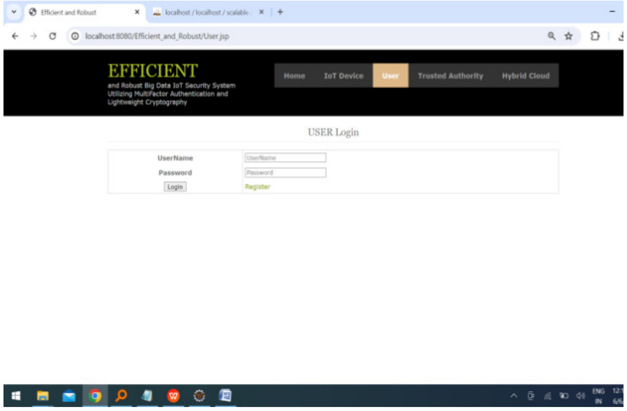
IOT Device Login Page



IOT Device Login

UserName	UserName
Password	Password

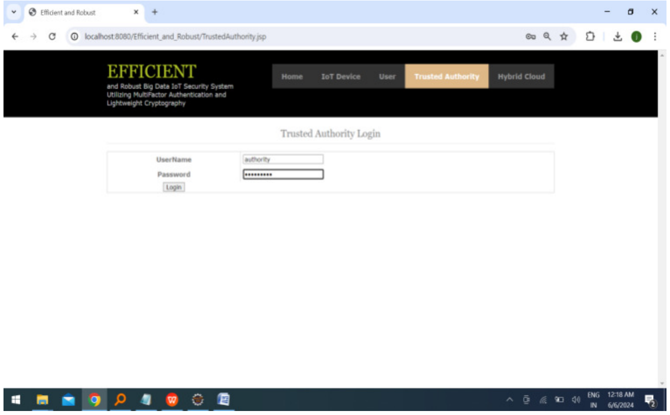
User Login Page


Efficient and Robust
localhost / localhost / scalable
localhost:8080/Efficient_and_Robust/User.jsp
EFFICIENT
and Robust Big Data IoT Security System
Utilizing MultiFactor Authentication and
Lightweight Cryptography
Home
IoT Device
User
Trusted Authority
Hybrid Cloud
Login
Register
ENG
IN

USER Login

UserName	UserName
Password	Password

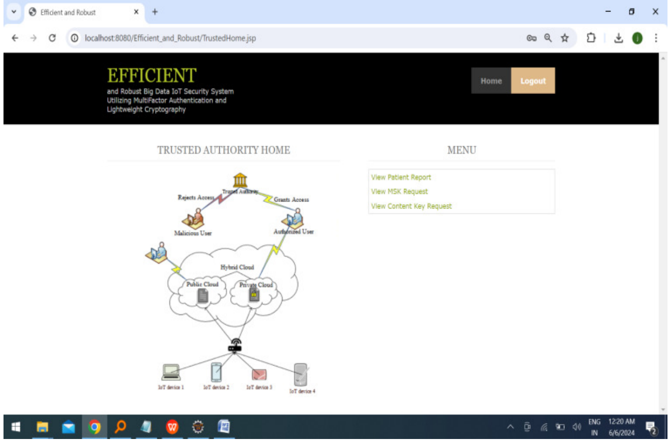
Trusted Authority Login Page


Efficient and Robust
localhost:8080/Efficient_and_Robust/TrustedAuthority.jsp
EFFICIENT
and Robust Big Data IoT Security System
Utilizing MultiFactor Authentication and
Lightweight Cryptography
Home
IoT Device
User
Trusted Authority
Hybrid Cloud
Login
ENG
IN
12:18 AM
6/6/2024

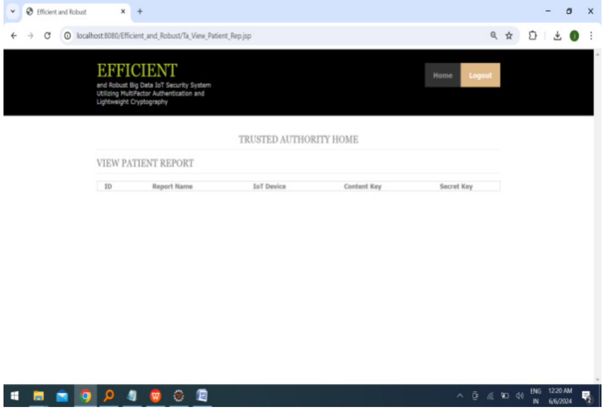
Trusted Authority Login

UserName	authority
Password	•••••••••

Trusted Authority Login Page



View Patient Report

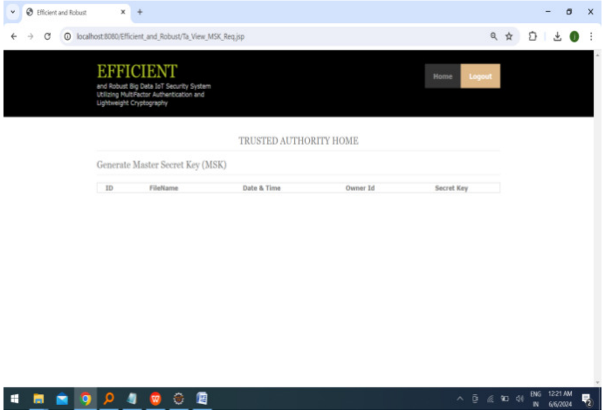

Efficient and Robust
localhost:8080/Efficient_and_Robust/Ta_View_Patient_Rep.jsp
EFFICIENT
and Robust Big Data IoT Security System
Utilizing MultiFactor Authentication and
Lightweight Cryptography
Home
Logout
ENG
IN
12:20 AM
6/6/2024

TRUSTED AUTHORITY HOME

VIEW PATIENT REPORT

ID	Report Name	IoT Device	Content Key	Secret Key

Master Key Request page



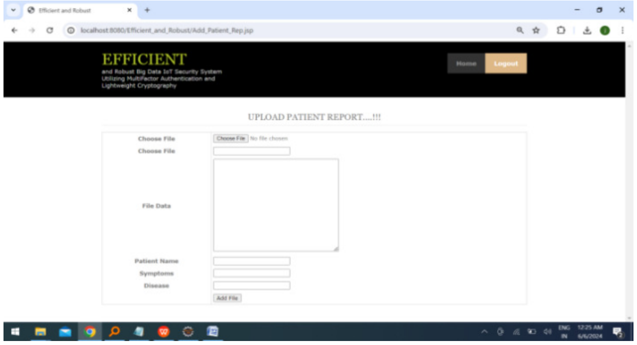
EFFICIENT
and Robust Big Data IoT Security System
Utilizing MultiFactor Authentication and
Lightweight Cryptography

TRUSTED AUTHORITY HOME

Generate Master Secret Key (MSK)

ID	FileName	Date & Time	Owner Id	Secret Key

Upload Patient Report page

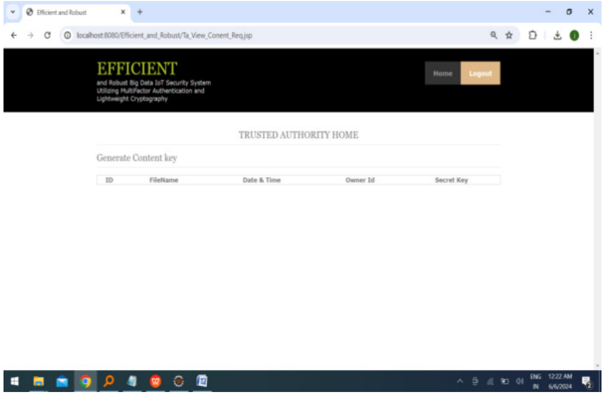


EFFICIENT
and Robust Big Data IoT Security System
Utilizing MultiFactor Authentication and
Lightweight Cryptography

UPLOAD PATIENT REPORT....!!!

Choose File: No file chosen
Choose File
File Data
Patient Name
Symptoms
Disease

Content Key Request page



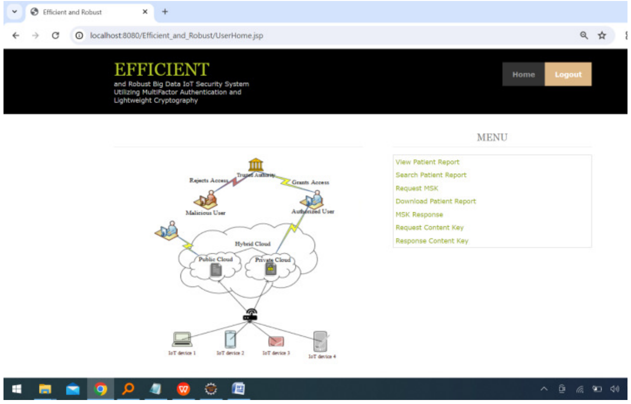
EFFICIENT
and Robust Big Data IoT Security System
Utilizing MultiFactor Authentication and
Lightweight Cryptography

TRUSTED AUTHORITY HOME

Generate Content key

ID	FileName	Date & Time	Owner Id	Secret Key

User Home Page



EFFICIENT
and Robust Big Data IoT Security System
Utilizing MultiFactor Authentication and
Lightweight Cryptography

8. CONCLUSION

Academic interest in cloud-integrated IoT applications has surged in recent years due to the technology's critical usage across various domains, including enterprises, the commercial sector, and household appliances. This work proposes a secure cloud-IoT ecosystem built with lightweight cryptographic algorithms and multifactor authentication.

Our method classifies Internet of Things (IoT) devices into two categories: highly sensitive and lowly sensitive. It employs a hybrid cloud architecture that combines public and private clouds. Sensitive data from IoT devices are separated and encrypted using the Feistel and RC6 algorithms, then stored in a private cloud via a gateway device for enhanced security. In contrast, non-sensitive data are encrypted using a gateway device and stored in a public cloud.

Multifactor authentication, managed by the Trusted Authority (TA), further enhances security by requiring users to undergo three distinct authentication processes. Credentials required for system access include user IDs, passwords, and biometric information (such as fingerprints or retina scans).

It evaluate the proposed method using metrics such as computational time, security level, encryption time, and decryption time. Our solution demonstrates superior performance and security compared to existing approaches like FCS, CP-ABE, and MCP-ABE.

9.FUTURE ENHANCEMENT

In the future, i intend to propose mutual authentication between gateway devices and IoT devices. Additionally, we aim to develop methods for detecting DDoS attacks on cloud servers.

10.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 MultiFactor 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: End-to-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, “Trust-Based IoT Cloud Participatory Sensing of Air Quality,” Wireless Personal Communications, pp. 1–14, 2019.

11.BoddupalliAnvesh Kumar, Dr.V.Bapuji ,”EFFICIENT AND PRIVACY-PRESERVING MULTI-FACTOR DEVICE AUTHENTICATION PROTOCOL FOR IOT” International journal of innovative Research inTechnology . (IJIRT).Volume9,Issue7,ISSN:2349-6002.December 2022,(UGC CARE LIST-1). https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/66109

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.BoddupalliAnvesh Kumar ,Dr.V.Bapuji ,"Secure And Lightweight Authentication Protocols for Devices in Internet of Things",Tuijinjishu/Journal of Propulsion Technology,Vol.44, NO.5,Pages:2419-2427,ISSN: 1001-4055, December 2023.

14. Salvador Pérez, Dan Garcia-Carrillo, Rafael MarínLópez, 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. BoddupalliAnvesh Kumar, Dr.V.Bapuji "Efficient Privacy Preserving Communication Protocol For IoT Applications" ,The Brazilian Journal of Development ISSN 2525-8761, published by Brazilian Journals and Publishing LTDA.(CNP) 32.432.868/0001-57)Vol.No.10,Pages:402-419 January 2024.

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.Sathish Polu and Dr. V. Bapuji. "Analysis of DDOS Attack Detection in Cloud Computing Using Machine Learning Algorithm", Tuijin Jishu/Journal of Propulsion Technology, Vol. 44, No.5, Pages:2410-2418, ISSN:1001-4055, December2023. https://www.propulsiontechjournal.com/index.php/journal/article/view/2978

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.Sathish Polu and Dr. V. Bapuji," "Mitigating Ddos Attacks in Cloud Computing Using Machine Learning Algorithms", The Brazilian Journal of Development ISSN 2525-8761, published by Brazilian Journals and Publishing LTDA. (CNPJ 32.432.868/0001-57) Vol.No.10, Pages:340-354January2024.

20. M. B. Mollah, M. A. K. Azad and A. Vasilakos, "Secure Data Sharing and Searching at the Edge of CloudAssisted 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.

21. 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.

22. 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.

23. 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

24.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.

25. Sathish Polu and Dr. V. Bapuji, "Distributed Denial of Service (DDOS) Attack Detection in Cloud Environments Using Machine Learning Algorithms", International Journal of Innovative Research in Technology, (IJIRT), Volume 9, Issue7, ISSN:2349-6002.December 2022, (UGC CARE LIST – I).

26 .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.