SCALABLE AND SECURE BIG DATA IOT SYSTEM BASED ON MULTIFACTOR AUTHENTICATION AND LIGHTWEIGHT CRYPTOGRAPHY

[1]E. Raviteja, [2]Mr K.Srdhar Reddy
[1]Mtech, Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur, Karimnagar, Telangana, INDIA, H.NO: 20S41D5807, ravitejavikky@gmail.com
[2]Professor, Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur, Karimnagar, Telangana, INDIA, sridhark529reddy@gmail.com

ABSTRACT: Organizations share an evolving interest in adopting a cloud computing approach for Internet of Things (IoT) applications. Integrating IoT devices and cloud computing technology is considered as an effective approach to storing and managing the enormous amount of data generated by various devices. However, big data security of these organizations presents a challenge in the IoT–cloud architecture. To overcome security issues, we propose a cloud-enabled IoT environment supported by multifactor authentication and lightweight cryptography encryption schemes to protect big data system. The proposed hybrid cloud environment is aimed at protecting organizations' data in a highly secure manner. The hybrid cloud environment is a combination of private and public cloud. Our IoT devices are divided into sensitive and nonsensitive devices. Sensitive devices generate sensitive data, such as healthcare data; whereas nonsensitive devices generate nonsensitive data, such as home appliance data. IoT devices send their data to the cloud via a gateway device. Herein, sensitive data are split into two parts: one part of the data is encrypted using RC6, and the other part is encrypted using the Fiestel encryption scheme. Nonsensitive data are encrypted using the Advanced Encryption Standard (AES) encryption scheme. Sensitive and nonsensitive 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 cloud–IoT architecture in the NS3 network simulator. We evaluated the performance of the proposed architecture using metrics such as computational time, security strength, encryption time, and decryption time.

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

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 aim 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.

ISSN: 0972-2750
Vol-12 Issue-11 No.01: 2022

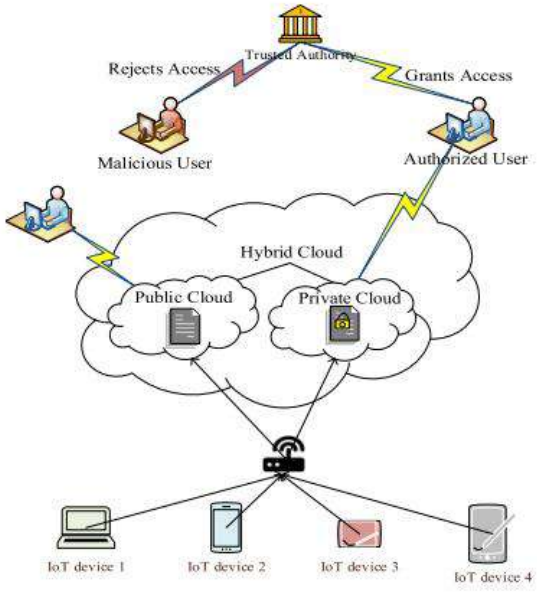

Fig.1: Example figure

The hybrid cloud includes public andprivate cloud. The public cloud is used to store nonsensitive 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 trust-based 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].

2. LITERATURE REVIEW

A Lightweight User Authentication Scheme for Cloud-IoT Based Healthcare Services:

With the ongoing revolution of cloud computing and Internet of Things, remote patient monitoring has become feasible. These networking paradigms are widely used to provide healthcare services and real-time patient monitoring. The sensors that are either wearable or embedded within the body of a patient transmit patient's data to the remote medical centers. The medical professional can access patient's data stored in the cloud anywhere

across the globe. As the sensitive data of the patient are 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 AVISPA tool confirms the security of the proposed scheme.

A profitable and energy-efficient cooperative fog solution for IoT services:
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, we 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 datacenters, and increased fog profits.

Secure Integration of IoT and Cloud Computing:
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, we 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 datacenters, and increased fog profits.

A Lightweight Multi-Factor Secure Smart Card Based Remote User Authentication Scheme for Cloud-IoT Applications:
With the rapid spread of cloud computing and ever increasing big data generated by Internet of Things (IoT), remote user authentication poses the biggest challenge. Internet of Things is a paradigm where every device in the Internet Infrastructure (II) is interconnected into a global dynamic expanding network. This paper proposes a novel remote user authentication scheme for cloud-IoT applications. The scheme is lightweight and robust to attacks and also has low computational overhead. The proposed scheme satisfies the desired essential attributes of security. A formal verification performed using AVISPA tool confirms the security of the proposed scheme

SecureSense: End-to-End Secure Communication Architecture for the Cloud-Connected Internet of Things:
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 we 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. We extend SicsthSense– a cloud platform for the IoT– with secure CoAP capabilities, and compliment a DTLS implementation for resource-constrained IoT devices with raw-public key and certificate-based asymmetric cryptography. To the best of our knowledge, this is the first effort toward providing end-to-end secure communication between resource-constrained smart things and cloud back-ends which supports all three security modes of CoAP both on the client side and the server side. SecureSense– our End-to-End (E2E) secure communication architecture for the IoT– consists of all standard-based protocols, and implementation of these protocols are open source and BSD-licensed. The SecureSense evaluation benchmarks and open source and open license implementation make it possible for future IoT product and service providers to account for security overhead while using all standardized protocols and while 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. METHODOLOGY

Most of the existing secure semantic searching schemes consider the semantic relationship among words to perform query expansion on the plaintext, 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.

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) as the 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. For 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.

ISSN: 0972-2750
Vol-12 Issue-11 No.01: 2022

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.

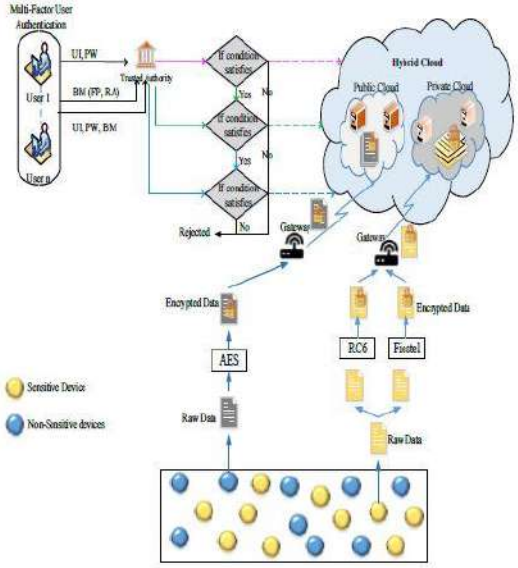

Fig.2: System architecture

The proposed cloud-enabled IoT architecture comprises IoT devices (sensitive devices (S1, S2, . . . Sn) and nonsensitive devices (NS1,NS2,, . . .NSn)), cloud (private and public cloud), TA, users, and gateway (Figure 2). To protect cloud-stored data from unauthorized users, we provide multifactor authentication to users. Furthermore, we protect data from IoT devices by encrypting the data using RC6 and Fiestel encryption schemes. Sensitive data from sensitive IoT devices are encrypted using RC6 and Fiestel encryption. The encrypted data are stored in a private cloud. We store highly sensitive data in a private cloud to provide high security to stored data. Sensitive data are also encrypted using the two aforementioned schemes to avoid forging. Nonsensitive data from nonsensitive IoT devices are encrypted using the AES algorithm because they contain nonsensitive information

FIGURE 2. Architecture for proposed cloud–IoT environment. that is stored in a public cloud. Sensitive and nonsensitive data are respectively stored in private cloud and public cloud via a gateway device. To provide high security to the stored information, we implement user authentication to access stored files. The TA performs user authentication through registered credentials, such as user ID, password, and biometrics (e.g., fingerprint or retina). The TA provides three levels of authentication when a user reads or downloads a file from the private and public cloud. In the first level of authentication, the TA verifies the username and password to provide read access to the files in the public cloud. The second level of authentication is performed when the user wants to download a file from the public cloud. The user is authenticated via biometrics, such as fingerprint or retina. Lastly, the third level of authentication is performed. The TA receives the user ID, password, and biometrics from the user and then provides them with access to read and download files in the private cloud. Figure 2 shows the proposed architecture for the cloud–IoT environment. The proposed architecture comprises four entities, namely, hybrid cloud, IoT devices, gateway, and TA.

4. IMPLEMENTATION

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.

MODULES:

1. **IOT DEVICE USER**
2. **USER**
3. **TRUSTED AUTHORITY**
4. **HYBRID CLOUD**

ISSN: 0972-2750
Vol-12 Issue-11 No.01: 2022

MODULES DESCRIPTION:

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.

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,
- Request Content Key,
- Response Content Ket,

3. Trusted Authority:

In This Module

- View Patient Reports,
- View MSK Request,
- View Content Key Request

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.

5. EXPERIMENTAL RESULTS

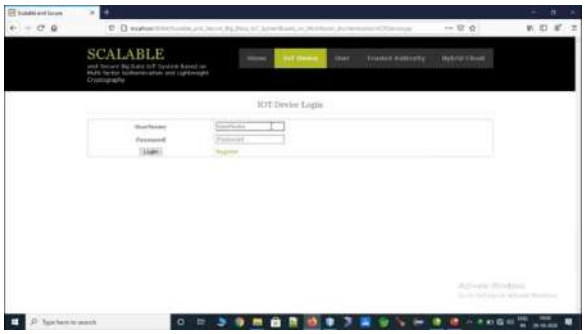

Fig.3: IOT device login

ISSN: 0972-2750
Vol-12 Issue-11 No.01: 2022

Fig.4: Upload patient report

Fig.5: TA login

Fig.6: View content

Fig.7: Download file

ISSN: 0972-2750
Vol-12 Issue-11 No.01: 2022

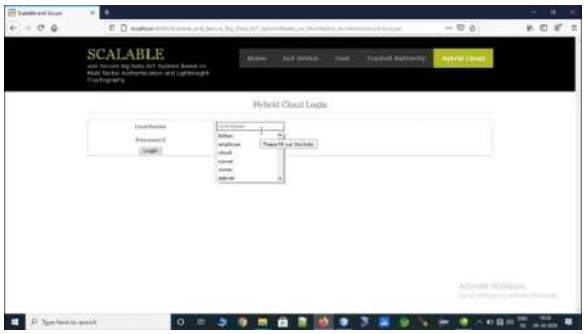

Fig.8: Hybrid cloud login

Fig.9: Master secrete key request

Fig.10: view time delay

6. 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 nonsensitive 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, nonsensitive 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 the proposed 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

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.

