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

Multifactor Authentication and Lightweight Cryptography are used to create a scalable and secure Big Data IoT system

Dr .B Priyanka [1], Dr. Manam Vamsi Krishna [2]
#1 Currently Working as Assistant Professor in CSE dept. Malla Reddy Institute of Technology, Hyderabad..
#2 Currently Working as Assistant Professor in CSE dept. Malla Reddy Institute of Technology, Hyderabad.

ABSTRACT_

Organizations share an evolving hobby in adopting a cloud computing strategy for Internet of Things (IoT) applications. Integrating IoT gadgets and cloud computing science is regarded as an fine method to storing and managing the giant quantity of statistics generated by using a number of devices. However, huge information protection of these companies affords a mission in the IoT–cloud architecture. To overcome safety issues, we advocate a cloud-enabled IoT surroundings supported by means of multifactor authentication and light-weight cryptography encryption schemes to defend massive facts system. The proposed hybrid cloud surroundings is aimed at defending organizations' information in a extraordinarily impenetrable manner. The hybrid cloud surroundings is a aggregate of personal and public cloud. Our IoT gadgets are divided into touchy and nonsensitive devices. Sensitive gadgets generate touchy data, such as healthcare data; whereas nonsensitive units generate nonsensitive data, such as domestic equipment data. IoT gadgets ship their information to the cloud by using a gateway device. Herein, touchy facts are cut up into two parts: one phase of the facts is encrypted the use of RC6, and the different phase is encrypted the usage of the Fiestel encryption scheme. Nonsensitive facts are encrypted the usage of the Advanced Encryption Standard (AES) encryption scheme. Sensitive and nonsensitive information are respectively saved in personal and public cloud to make sure excessive security. The use of multifactor authentication to get entry to the statistics saved in the cloud is additionally proposed. During login, statistics customers ship their registered credentials to the Trusted Authority (TA). The TA gives three stages of authentication to get right of entry to the saved data: first-level authentication - study file, second-level authentication - down load file, and third-degree authentication - down load file from the hybrid cloud. We put into effect the proposed cloud–IoT structure in the NS3 community simulator. We evaluated the overall performance of the proposed structure the usage of metrics such as computational time, protection strength, encryption time, and decryption time.

INDEX TERMS Big Data, Cloud computing, Internet of Things, Multilevel authentication, LightweightCryptography.

1.INTRODUCTION

IoT and cloud computing have become important concepts as a result of the advancement and widespread use of Internet of Things (IoT) applications, as well as the emergence of wireless communication and mobile technologies. The Internet of Things (IoT) aims to provide connectivity for anything with minimal storage and computing capabilities [1] [2]. Security is a major concern in cloud-integrated IoT, and user data stored in the cloud must be secure [3]. In cloud–IoT applications, a lightweight multifactor secured smart card-based user authentication is introduced [4]. Figure 1 depicts the cloud-integrated IoT architecture, which includes the hybrid cloud, IoT devices, and users. The hybrid cloud is made up of both public and private clouds. The public cloud is used for non-sensitive data storage, whereas the private cloud is used for highly sensitive data storage.

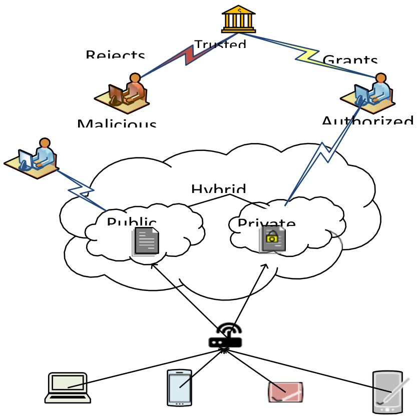


Figure 1:Architecture For Cloud–Iot Environment.

The end-to-end tightly closed verbal exchange structure is proposed for a cloud-connected IoT environment. Herein, a confined utility protocol is proposed for a tightly closed conversation between IoT and the cloud [5]. A homomorphic encryption device primarily based on the ring gaining knowledge of with error algorithm is used for cloud person authentication [6]. Role-based get right of entry to manage (RBAC) with the have confidence comparison (TE) algorithm is used to supply get admission to manipulate to IoT resources. RBAC entails three TE algorithms, namely, neighborhood have faith comparison algorithm, digital have faith contrast algorithm, and cooperative have faith comparison algorithm [7]. A light-weight IoT-based cryptography authentication scheme is delivered to furnish safety in a cloud–IoT environment. A proposed light-weight authentication scheme adopts a one-way hash feature and one of a kind OR operation [8]. An superior light-weight authentication scheme primarily based on formal and rigorous casual protection evaluation is proposed for a cloud-assisted IoT environment. Formal safety evaluation is carried out via a random oracle mannequin [9]. A trust-based IoT cloud surroundings is delivered to supply a impenetrable storage in a cloud environment. The previous records of every IoT system is accumulated the use of a centralized IoT have confidence protocol regarded for safety evaluation [10]. A invulnerable and compliant non-stop evaluation framework (SCCAF) is proposed to guard person facts in a cloud-assisted IoT environment. The SCCAF offers pointers for cloud customers in evaluating the safety and compliance stages of cloud carrier vendors [11]. Lightweight context-aware IoT offerings are furnished to the user. Moreover, the enacted light-weight context-aware provider makes use of a filter to ahead the most relevant records to customers on the foundation of their context [12]. The fuzzy analytical hierarchical technique (FAHP) algorithm is proposed to consider the influential elements in IoT. The FAHP offers a nice evaluation of tangible factors, namely, security, value, and connectivity [13]. A light-weight bootstrapping mechanism is used for invulnerable IoT services. The Ephemeral Diffie–Hellman Over COSE protocol is used to standardize key agreements in IoT gadgets [14].

2.LITEARATURE SURVEY

2.1) DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party

AUTHORS: Ali, M., Malik, S. and Khan, S.,

Off-site information storage is an utility of cloud that relieves the clients from focusing on records storage system. However, outsourcing records to a third-party administrative manipulate entails serious safety concerns. Data leakage may additionally appear due to assaults by means of different customers and machines in the cloud. Wholesale of statistics through cloud carrier issuer is but any other trouble that is confronted in the cloud environment. Consequently, high-level of protection measures is required. In this paper, we advocate Data Security for Cloud Environment with Semi-Trusted Third Party (DaSCE), a records safety machine that presents (a) key administration (b) get entry to control, and (c) file certain deletion. The DaSCE makes use of Shamir's (k, n) threshold scheme to manipulate the keys, the place okay out of n shares are required to generate the key. We use a couple of key managers, every web hosting one share of key. Multiple key managers keep away from single factor of failure for the cryptographic keys. We (a) put into effect a working prototype of DaSCE and consider its overall performance based totally on the time fed on in the course of more than a few operations, (b) formally mannequin and analyze the working of DaSCE the usage of High Level Petri nets (HLPN), and (c) affirm the working of DaSCE the usage of Satisfiability Modulo Theories Library (SMT-Lib) and Z3 solver. The outcomes disclose that DaSCE can be successfully used for safety of outsourced statistics with the aid of using key management, get right of entry to control, and file certain deletion.

2.2) Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption

AUTHORS: Jung, T., Li, X. Y., Wan, Z. and Wan, M

Cloud computing is a innovative computing paradigm which allows flexible, on-demand and affordable utilization of computing resources, however the records is outsourced to some cloud servers, and a variety of privateness issues emerge from it. Various schemes based totally on the Attribute-Based Encryption have been proposed to tightly closed the cloud storage. However, most work focuses on the facts contents privateness and the get admission to control, whilst much less interest is paid to the privilege manage and the identification privacy. In this paper, we current a semi-anonymous privilege manipulate scheme AnonyControl to tackle no longer solely the information privateness however additionally the consumer identification privateness in current get entry to manipulate schemes. AnonyControl decentralizes the central authority to restriction the identification leakage and as a result achieves semi-anonymity. Besides, it additionally generalizes the file get admission to manage to the privilege control, via which privileges of all operations on the cloud records can be managed in a fine-grained manner. Subsequently, we current the AnonyControlF which wholly prevents the identification leakage and obtain the full anonymity. Our safety evaluation indicates that each AnonyControl and AnonyControl-F are impervious underneath the DBDH assumption, and our overall performance comparison well-knownshows the feasibility of our schemes.

2.3) Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services

AUTHORS: Liu, J. K., Au, M. H., Huang, X., Lu, R., and Li, J

In this paper, we introduce a new fine-grained two-factor authentication (2FA) get entry to manipulate device for web-based cloud computing services. Specifically, in our proposed 2FA get right of entry to manipulate system, an attribute-based get admission to manage mechanism is applied with the necessity of each a person secret key and a light-weight safety device. As a consumer can't get right of entry to the gadget if they do no longer maintain both, the mechanism can beautify the safety of the system, specially in these situations the place many customers share the identical laptop for web-based cloud services. In addition, attribute-based manipulate in the gadget additionally permits the cloud server to preclude the get admission to to these customers with the equal set of attributes whilst maintaining person privacy, i.e., the cloud server solely is aware of that the consumer fulfills the required predicate, however has no thought on the specific identification of the user. Finally, we additionally elevate out a simulation to display the practicability of our proposed 2FA system.

3.PROPOSED SYSTEM

Our proposed work improves security by utilising multifactor authentication and cryptography encryption schemes. As shown in Figure 2, user requests are classified into three types: downloading, reading, and both. If the request is only for reading content from the cloud, the user is granted access via the password and user Id. If the user requests to download content from the cloud, he will be

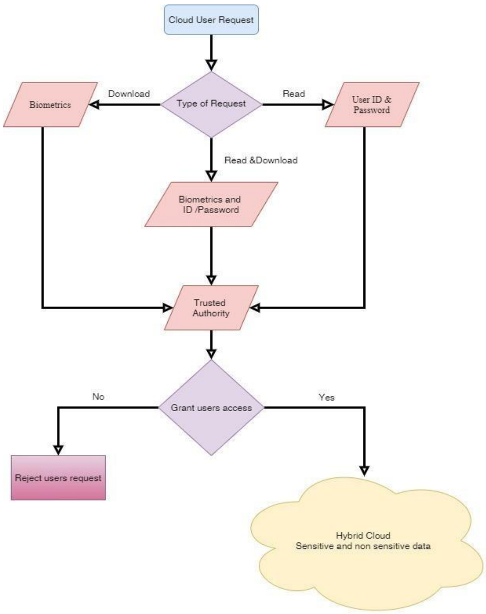


FIGURE 2 Procedure of Multifactor Authentication and Lightweight Cryptography method

asked for his biometrics; if the user's request is for both cases (reading and downloading content), the password and user name will be used in addition to the biometrics. In all cases where the request is successful, the trusted authority grants the user permission to get entry to the hybrid cloud otherwise, his request is rejected The proposed cloud-enabled IoT structure consists of IoT gadgets (sensitive gadgets ($S1$, $S2$, … Sn) and nonsensitive units ($NS1$, $NS2$,, … NSn)), cloud (private and public cloud), TA, users, and gateway (Figure 3). To guard cloud- saved statistics from unauthorized users, we grant multifactor authentication to users. Furthermore, we shield information from IoT units through encrypting the statistics the use of RC6 and Fiestel encryption schemes. Sensitive facts from touchy IoT units are encrypted the use of RC6 and Fiestel encryption. The encrypted records are saved in a non-public cloud. We keep noticeably touchy information in a personal cloud to grant excessive safety to saved data. Sensitive statistics are additionally encrypted the usage of the two aforementioned schemes to keep away from forging. Nonsensitive records from nonsensitive IoT gadgets are encrypted the use of the AES algorithm due to the fact they include nonsensitive data that is saved in a public cloud. Sensitive and nonsensitive statistics are respectively saved in personal cloud and public cloud through a gateway device. To grant excessive safety to the saved information, we put into effect consumer authentication to get right of entry to saved files. The TA performs consumer authentication via registered credentials, such as person ID, password, and biometrics (e.g., fingerprint or retina). The TA offers three degrees of authentication when a consumer reads or downloads a file from the non-public and public cloud. In the first degree of authentication, the TA verifies the username and password to grant study get entry to to the archives in the public cloud. The 2d degree of authentication is carried out when the consumer wishes to down load a file from the public cloud. The consumer is authenticated with the aid of biometrics, such as fingerprint or retina. Lastly, the 1/3 stage of authentication is performed. The TA receives the person ID, password, and biometrics from the person and then offers them with get right of entry to to study and down load documents in the personal cloud. Figure three indicates the proposed structure for the cloud–IoT environment. The proposed structure includes 4 entities, namely, hybrid cloud, IoT devices, gateway, and TA.

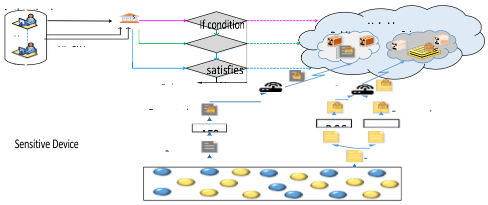
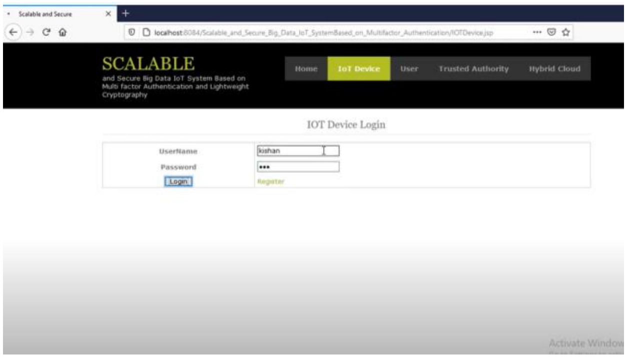


Figure 3:Architecture For Proposed Cloud–IOT Environment.

4.RESULTS AND DISCUSSION



Scalable and Secure

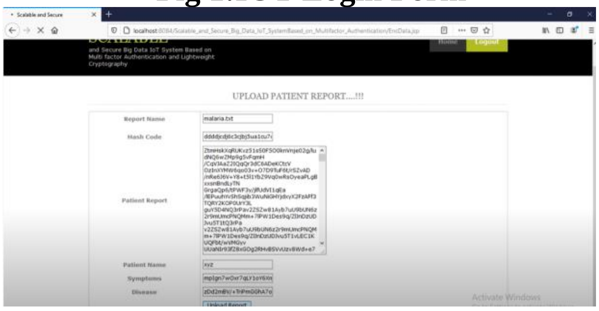
localhost:8084/Scalable_and_Secure_Big_Data_IoT_SystemBased_on_Multifactor_Authentication/IOTDevice.jsp

SCALABLE
and Secure Big Data IoT System Based on Multi factor Authentication and Lightweight Cryptography

IOT Device Login

UserName: kishan
Password: •••
Login
Register

Fig 1:IOT Login Form



Scalable and Secure

localhost:8084/Scalable_and_Secure_Big_Data_IoT_SystemBased_on_Multifactor_Authentication/EncData.jsp

and Secure Big Data IoT System Based on Multi factor Authentication and Lightweight Cryptography

UPLOAD PATIENT REPORT....!!!

Report Name: malaria.txt
Hash Code: ddddjcdj6c3cjbj5ua1cu7
Patient Report:
ZbeHskXqRUKvz51s50F5O0kmVnje02g/tu
dNQ6wZMp9g5vFgmH
/CqV1AaZ20QqQr3dC6ADeKCtcV
Oz1nXYMW6qo03v+O7D9TuF6UrSZvAD
/nRe6J6V+Y8+t5l1Yb29Vq0wRsOyeaPLgB
xxsnBndLyTN
GrgaQp6/tPWF3v/jRUdVl1qEa
/EPuuhmVShSqjib3WuNiGHYjdxyX2FzAFf3
TQRY2KOP0UrY3L
guY5D4NQ3rPav2ZSZw81Ayb7uU9bUN6z
2r9mUmcPNQMm+7lPW1Des9q/ZIlnDzUD
Jvu5T1tQ3rPa
v2ZSZw81Ayb7uU9bUN6z2r9mUmcPNQM
m+7lPW1Des9q/ZIlnDzUDJvu5T1vLEC1K
UQFbt/wVMGyv
UUaNIr93fZ8xGOg2RHvBSVvUzvBWd+e7
Patient Name: xyz
Symptoms: mplgn7wOxr7qLY1oY6Xt
Disease: zDd2mBV/+TnPmG0hA7o
Upload Report

Fig 2:Encrypted data

5.CONCLUSION

In latest years, cloud-integrated IoT purposes have emerge as famous amongst researchers due to their quintessential functions in organizations, non-public sectors, home appliances, etc. This work proposes a tightly closed cloud–IoT surroundings the usage of multifactor authentication and light-weight cryptography schemes. The proposed approach splits IoT units into touchy and nonsensitive devices. We recommend the use of a hybrid cloud that incorporates public cloud and personal cloud. Sensitive system records are divided into two and encrypted the use of the RC6 and Fiestel encryption algorithms. These statistics are saved in a personal cloud to grant excessive protection by a gateway device. By contrast, nonsensitive system statistics are encrypted the use of AES and saved in a public cloud through a gateway device. Multifactor authentication is supplied through the TA. In this process, the person undergoes three tiers of authentication by means of offering their credentials, such as consumer ID, password, and biometrics (e.g., retina and fingerprint). We consider the overall performance of the proposed technique the use of metrics that consist of computational time, safety strength, encryption time, and decryption time. From the evaluation results, we show that the proposed approach performs higher than FCS, CP-ABE, and MCP-ABE.

FUTURE SCOPE

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 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: 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.

Author's Profile:

Dr B.Priyanka

Completed here B. Tech. In Computer Science Engineering (2014) Completed M.Tech. in Computer Science Engineering (2016)
Received her PhD degree in computer science and engineering department from Sri Satya Sai University Technology & Medical Sciences in September 2021.
Research interest: Big data, Machine learning, Data mining Working As Assistant Professor in Mallareddy Institute of Technology

Dr. MANAM VAMSI KRISHNA.

Received his PhD degree in computer science and engineering department from Sri Satya Sai University Technology & Medical Sciences in July 2021. Currently Working as Assistant Professor in CSE dept. Malla Reddy Institute of Technology, Hyderabad. His Research interests in cryptography & Network security, Cyber Security, computer networks, Data mining.