International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

xx

COPY RIGHT

2024 IJIEMR. Personal use of this material is permitted. Permission from IJIEMR must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. No Reprint should be done to this paper, all copy right is authenticated to Paper Authors

IJIEMR Transactions, online available on 28th May 2024. Link
https://www.ijiemr.org/downloads/Volume-13/ISSUE-5

10.48047/IJIEMR/V13/ISSUE 05/50

TITLE: SCALABLE AND SECURE BIG DATA IOT SYSTEM BASED ON MULTIPLE AUTHENTICATION AND LIGHTWEIGHT CRYPTOGRAPHY

Volume 13, ISSUE 05, Pages: 482-491

Paper Authors **Mrs. B Mahalakshmi, Dhanwada Anisha, Deekonda Aravind, Nakka Shreya, Katikam Umesh Reddy**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

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

Mrs. B Mahalakshmi, Dhanwada Anisha, Deekonda Aravind, Nakka Shreya, Katikam Umesh Reddy

Associate Professor, Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India.
mahal466@gmail.com
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India.
anishadhanwada@gmail.com
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India.
deekondaaravind630@gmail.com
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India.
nakkashreya22@gmail.com
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India.
umeshreddy648@gmail.com

Abstract: There is a developing pattern among associations to utilize distributed computing for Internet of Things (IoT) applications. The tremendous volume of information made by various gadgets can be really put away and overseen by incorporating IoT gadgets with distributed computing innovation. However, these organizations' huge information security represents an issue for the IoT-cloud engineering. We recommend a cloud-empowered Internet of Things (IoT) climate that is upheld by different verification and lightweight cryptographic encryption ways to deal with protect enormous information frameworks to address security concerns. The objective of the recommended cross breed cloud framework is to give incredibly secure information assurance to organizations. Private and public mists are utilized to establish the cross breed cloud climate. We have two classes of IoT gadgets: delicate and non-touchy. Touchy gadgets produce delicate information, similar to clinical records; non-delicate gadgets produce non-touchy information, such information from home devices. An entryway gadget is utilized by IoT gadgets to communicate information to the cloud. Here, delicate information are separated into two segments, with RC6 encryption utilized for one segment and the Feistel encryption calculation for the other. The Advanced Encryption Standard (AES) encryption calculation is utilized to safeguard non-delicate information. To keep up with most extreme security, delicate and nonsensitive information are kept in hidden and public mists, separately. Information clients give their enrolled certifications to the Trusted Authority (TA) during login. To get to the put away information, the TA offers three degrees of validation: read record for first level verification, download document for second level confirmation, and download record from crossover cloud for third level verification. We utilize the NS3 network test system to try the proposed cloud-IoT engineering. We utilized rules like processing time, security strength, encryption time, and decoding time to evaluate the exhibition of the proposed design.

Index Terms: *cloud computing, multiple authentication, lightweight cryptography, RC6, Advanced Encryption Standard, Trusted Authority.*

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

1. INTRODUCTION

IoT and distributed computing have acquired significance pair with the turn of events and far and wide utilization of Internet of Things (IoT) applications, as well as the ascent of remote correspondence and versatile innovation. The Web of Things looks to interface all that with even the most fundamental registering and stockpiling limits. Cloud-coordinated IoT presents huge security difficulties, and client information put away there should be safeguarded safely. In cloud-IoT applications, a lightweight multifaceted got brilliant card-based client validation system is presented. The half and half cloud, IoT gadgets, and clients make up the cloud-coordinated IoT engineering portrayed in Figure 1. Both public and confidential mists are essential for the cross breed cloud. Profoundly delicate information is put away in the confidential cloud, though non-touchy information is kept in the public cloud.

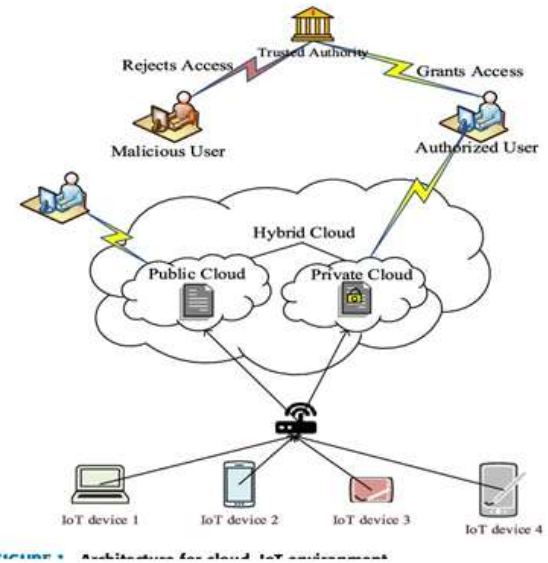

Fig 1 Architecture of cloud integrated IoT

To resolve the issues of ensuring information respectability, mystery, and client validation in enormous scope IoT settings, plan and foster a versatile and secure large information Internet of things (IoT) framework that incorporates lightweight cryptography and multifaceted verification. Eventually, the framework ought to give a hearty and versatile answer for the up and coming age of IoT biological systems by dealing with the rising volume of information created by IoT gadgets productively and ensuring solid safety efforts through the incorporation of multifaceted verification and lightweight cryptographic strategies. The medical care, shrewd city, modern robotization, and individual gadget areas are only a couple of the ventures where the Internet of Things (IoT) is proceeding to develop. Huge volumes of information are delivered because of this increment, and they should be effectively and safely assembled, moved, and dissected. IoT networks are open and dispersed by plan, which makes them powerless against various security gambles with like information breaks, unlawful access, and cyberattacks. The risks related with IoT gadgets are exacerbated by their requirements, specifically their low handling power and short battery duration, which make it challenging to apply customary, complex cryptographic arrangements.

2. LITERATURE SURVEY

Late years have seen significant improvements in various fields, including correspondence conventions, modern informatics, and medical care, because of the union of Cloud and Internet of Things (IoT) innovation. The motivation behind this writing survey is to look at the latest discoveries around here of review, underscoring the significant developments and examples tracked down in the picked works.

A straightforward client verification framework planned explicitly for Cloud-IoT-based medical care administrations was advanced by Sharma and Kalra [1]. The arrangement offers powerful client confirmation methods to address the security issues present in such frameworks.

A beneficial and energy-effective helpful mist answer for Web of Things administrations was presented by Al Ridhawi et al. [2]. This approach shows mist figuring's true capacity for functional purposes by using it to further develop the energy proficiency and execution of IoT organizations.

Psannis, Kim, and Gupta chatted on the best way to safely coordinate distributed computing and IoT [3]. The meaning of safety in empowering smooth joining between these two advances is underlined by their work, which lays the foundation for reliable and solid Web of Things applications.

Sharma and Kalra recommended a lightweight multifaceted secure brilliant card-based distant client validation technique for Cloud-IoT applications [4], expanding on their previous work. By utilizing multifaceted validation techniques, this procedure further develops security and ensures safe admittance to Cloud-IoT administrations.

SecureSense, a start to finish secure correspondence design for the Internet of Things associated with the cloud, was presented by Raza et al. [5]. Their engineering tends to significant security issues in IoT arrangements by focusing on ensuring the privacy, trustworthiness, and genuineness of information moved between IoT gadgets and Cloud servers.

In IoT union Cloud conditions, Jin, Park, and Mun recommended an idea for a protected correspondence convention using RLWE-based homomorphic encryption [6]. Their innovation safeguards delicate information from control and undesirable access by utilizing state of the art cryptographic calculations to protect correspondence diverts in Internet of Things organizations.

For hugely incorporated IoT applications, Chen introduced an IoT-based joint effort based RBAC with a trust assessment calculation model [7]. This design empowers powerful organization of access consents and assets in huge scope IoT conditions by working with job based admittance control and trust assessment methodology.

In a distributed computing setting, Zhou et al. exhibited a lightweight IoT-based validation instrument [8]. To safeguard client information trustworthiness and privacy, their arrangement centers around offering successful and secure confirmation instruments for Internet of Things gadgets getting to cloud administrations.

To sum up, the picked writing stresses the consistent undertakings to handle the security, proficiency, and reconciliation deterrents in Cloud-IoT settings. The previously mentioned works work with the headway of creative arrangements and structures, thus opening entryways for the joining of Cloud-IoT advancements across different applications and areas.

3. METHODOLOGY

i) Proposed Work:

The objective of the review's staggered validation methodology is to further develop security in a coordinated Internet of Things and cloud climate.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

To fortify IoT framework security, it fosters a cross breed cloud design that joins private and public mists. In light of the information they give, gadgets are isolated into touchy and nonsensitive classifications. For added security, touchy information from delicate gadgets is encoded utilizing the Feistel and RC6 encryption plans prior to being put away in a confidential cloud through a passage gadget. Utilizing a practically identical door gadget, nonsensitive information from different gadgets is encoded with the AES strategy and saved in a public cloud. To safeguard information saved in the cloud, a layered validation system with a trusted authority (TA) is laid out. Three phases of confirmation are associated with this methodology, by which the TA contrasts enlisted information and client certifications (secret key, ID, and biometrics). After an effective validation process, clients can peruse and download documents from the cloud, however unapproved endeavors are denied, safeguarding the security and trustworthiness of the information. Nonetheless, in light of the fact that TA coordinates with outsiders, there could be an expansion in cloud administration expenses.

ii) System Architecture:

All inside the field of computer programming, engineering configuration alludes to the central structure of a framework, which incorporates its constituent parts as well as the connections among them and the general climate. Moreover, this plan incorporates directing thoughts that directed its development and advancement after some time. Execution, security, practicality, and versatility are only a couple of the quality highlights of the framework that are enormously influenced by how well the engineering is planned. Specialists might augment these characteristics via cautiously planning the design, ensuring the framework fulfills its practical requirements and is strong and adaptable enough to conform to changes in its working climate. Thus, engineering configuration is critical in deciding the general execution and sturdiness of programming frameworks.

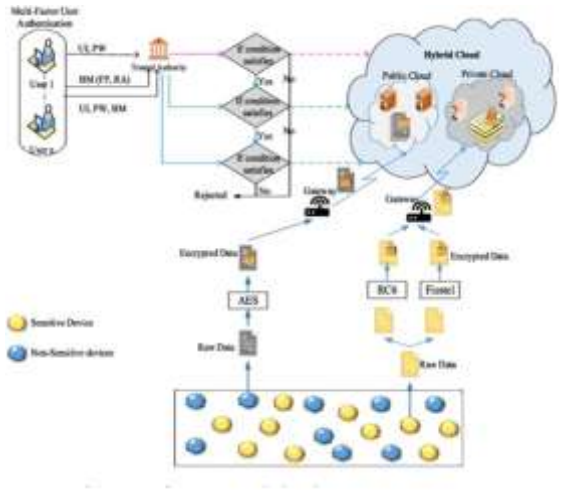

Fig 2 Proposed Architecture

iii) Modules:

To implement this project we used the following modules. They are:

- IOT DEVICE USER
- USER
- TRUSTED AUTHORITY
- HYBRID CLOUD

IoT Device User:

Prior to having the option to get to the IoT Gadget module, clients should enroll with their data. Guaranteeing client validation and approval through enlistment helps framework security. Subsequent to enrolling, clients can get to various highlights by signing in:

View patient reports:

The framework permits clients to recover and look at patient reports that are put away there. Medical care suppliers or other approved staff can undoubtedly survey patient data because of this instrument.

Upload patient reports: New quiet reports can be added to the framework by approved clients. The continuous support and refreshing of patient records is made conceivable by this usefulness.

Patient reports from outside sources, like clinical gadgets or symptomatic gear, can be transferred by clients. The framework's capacity to coordinate information from many sources is worked with by this component.

View patient report permissions: Clients can handle the privileges related with patient reports, which incorporates the capacity to see and alter individual reports. This element ensures both administrative consistence and information security.

Taking everything into account, the IoT Gadget module offers urgent elements for effectively dealing with clinical information and safely putting away tolerant reports.

User:

To get to the stage, clients need to enroll with their subtleties in the IoT Gadget framework's Client module. Signing in requires enrollment to guarantee right client validation and approval. Subsequent to enlisting, clients can get to framework includes and oversee patient reports in various ways, including:

inspect patient reports: The framework permits clients to recover and analyze patient reports that are put away there. At the point when essential, this component permits approved people or medical care specialists to survey patient data.

View patient reports: Utilizing different boundaries, such the patient's name, ID, or ailment, clients can look into individual patient reports. Compelling patient information recovery is made simpler by this element.

Clients can demand the Master Session Key (MSK), which is essential for safe correspondence and information trade inside the framework.

Download patient report: The framework permits approved clients to download patient reports for disconnected review or extra investigation. At the point when required, this capability makes patient information effectively open.

MSK response: The framework makes and sends the Master Session Key (MSK) to the client in light of a solicitation for it, opening up secure channels of correspondence.

Request Content Key: The Substance Key, which is required inside the framework to encode and disentangle delicate information, is accessible for clients to ask for.

Response Content Key: to safeguard the security and classification of the client's information, the framework gives the expected encryption key in light of the solicitation for the Substance Key.

In synopsis, the Client module gives a broad scope of highlights for dealing with patient reports and accessing fundamental framework keys,

consequently smoothing out medical care information organization and empowering safe correspondence all through the IoT Gadget stage.

Trusted Authority:

The Trust Supervisor goes about as an outsider evaluator in the Confided in Power module, regulating the keys and access honors that end clients and information proprietors have inside the framework. This position is fundamental for keeping up with secure access control and holding unlawful clients back from getting to cloud information. The accompanying moves can be initiated subsequent to signing into the Trust Director account:

View Patient Reports: The Trust Director can get to patient reports that are kept on record in the framework. Oversight and checking of patient information access and utilization are made conceivable by this ability.

View MSK Request: Request made by clients for the Expert Meeting Key (MSK) are apparent to the Trust Director. Guaranteeing secure correspondence channels are laid out when vital is worked with by checking MSK demands.

View Content Key Request: The Trust Director might see what demands clients make for Content Keys. Delicate information inside the framework should be encoded and unscrambled utilizing content keys. By watching out for these solicitations, proper information security conventions are maintained.

Taking everything into account, the situation's information security and access freedoms the executives are incredibly helped by the Confided in Power module. The abilities of the Trust Supervisor add to the general respectability and security of the framework by offering oversight and command over significant region of its activity.

Hybrid Cloud:

Clients can see any remaining clients and IoT Gadget clients in the framework inside the Mixture Cloud Module. To guarantee secure access control, approval is fundamental before clients can sign in to the program. The accompanying highlights are remembered for this module:

View All Patient Reports: All quiet reports that are kept on document in the framework are available to clients. Approved laborers can audit patient data completely on account of this capacity.

View All Transactions: This module gives clients admittance to the framework exchanges that have been all made. This covers all correspondences between clients, information moves, and different activities recorded by the framework.

View Security Key Request: The framework permits clients to see security key demands that have been made. To ensure information security and honesty, demands for Master Session Keys (MSK) or Content Keys are remembered for this.

View Security Key Response: The solutions to security key solicitations are accessible for clients to view, and they contain the encryption keys expected for safe information trade and framework correspondence.

View Time Delay Results: The module gives clients admittance to data about fundamental time delays. Execution markers, dormancy issues, or

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

some other postponements debilitating framework usefulness might fall under this classification.

In light of everything, the Cross breed Cloud Module gives a broad scope of elements for controlling client access, watching out for framework activities, and ensuring information security in the half and half cloud setting. This module makes it more straightforward to oversee and administer framework assets and activities by giving perceivability into significant region of the framework's activity.

4. EXPERIMENTAL RESULTS

Fig 3 IoT Device Login

Fig 4 Upload Patient Report

Fig 5 Patient Report Details

Fig 6 Upload File

Fig 7 Trusted Authority Login

Fig 8 User Interface of TA

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Fig 9 TA Home

Fig 10 MSK and CK Keys Generated

Fig 11 Provide Permission

Fig 12 User Login

Fig 13 Search Patient Result

Fig 14 Search Result Dropdown List

Fig 15 Downloaded File Successfully

5. CONCLUSION

Since they have such countless significant purposes in organizations, the confidential area, homes machines, and so on, cloud-coordinated IoT applications have acquired prevalence among specialists as of late. This article proposes using lightweight cryptographic methods and multifaceted validation to establish a protected cloud-IoT climate. IoT gadgets are partitioned into

delicate and nonsensitive gadgets utilizing the recommended way. We recommend utilizing a half breed cloud, which consolidates private and public mists. The RC6 and Feistel encryption calculations are utilized to part delicate gadget information into two separate encoded records. Through a passage gadget, this information are kept in a hidden cloud for greatest security. Then again, non-delicate gadget information is saved in a public cloud through an entryway gadget and scrambled utilizing AES. The TA offers multifaceted confirmation. By entering their qualifications, which incorporate their client ID, secret key, and biometrics (like their unique mark and retina), the client goes through three phases of validation in this technique. We use standards, for example, handling time, security strength, encryption time, and unscrambling time to evaluate the viability of the proposed approach. We exhibit that the deep strategy beats FCS, CPABE, and MCP-ABE in light of the near information. We need to recommend shared confirmation in the future between IoT gadgets and entryway gadgets. Besides, we want to recommend identifying DDoS assaults on cloud servers.

6. FUTURE SCOPE

Blockchain reconciliation, quantum-safe encryption, improved multifaceted validation, bound together security conventions, further developed edge figuring, lightweight cryptography, computer based intelligence mix, and administrative advancements are basic to the improvement of versatile and safe Enormous Information IoT frameworks later on. With the quantity of associated gadgets expanding at an outstanding rate, these progressions try to guarantee the possibility and adequacy of IoT advancements by resolving significant issues like security, versatility, and compelling information the board.

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.