JES
Journal of Engineering Sciences

Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

SECURE AND EFFICIENT STORAGE OF LIGHTWEIGHT IDENTITY-BASED AUTHENTICATED DATA SHARING PROTOCOL FOR CYBER-PHYSICAL CLOUD ENVIRONMENT

[1]DR. FAHMIDA BEGUM , [2]DR. K. UMA MAHESHWARI
[1,2]Associate Professor
DEPARTMENT OF CSE
Dr.K V SUBBA REDDY INSTITUTE OF TECHNOLOGY, KURNOOL

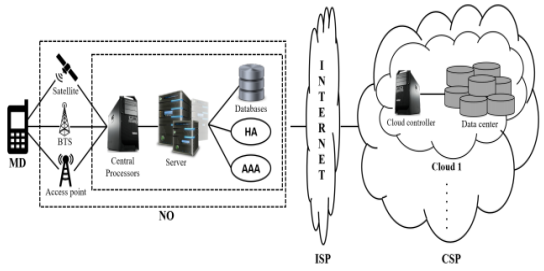
ABSTRACT: Secure and efficient record storage and sharing thru authenticated physical devices continue to be tough to obtain in cyber-physical cloud surroundings, mainly due to the range of methods used to get entry to the offerings and statistics. Thus in this paper, we present a lightweight identification-based authenticated statistics sharing protocol to offer cozy records sharing amongst geographically dispersed bodily devices and customers. The proposed contract is demonstrated to withstand chosen-ciphertext assault (CCA) underneath the hardness assumption of decisional-Strong Diffie-Hellman (SDH) problem. We additionally compare the overall performance of the proposed protocol with existing records sharing protocols in phrases of computational overhead, communique overhead, and reaction time.

Keywords—Cloud computing, Privacy protecting cloud, Identity-based Cryptography, Random oracle model, Data sharing protocol, AVISPA

I. INTRODUCTION

Cloud-assisted cyber-physical Structures (Cloud-CPSs; additionally called cyber-physical cloud structures) have vast applications, ranging from healthcare to intelligent energy grid to smart towns to battlefields to army, and so on [1], [2]. In such systems, purchaser devices (e.G., Android and iOS devices, or aid restricted devices along with sensors) can be used to get right of entry to the applicable offerings (e.g., in the context of a smart energy grid.It can include application utilization records analyzed and saved within the cloud) from/through the darkness. However, purchaser gadgets usually have much less computing skills and as a result, are unlikely to have good enough safety (technical) measures in contrast to the traditional non-public computers (PCs) [3]. One such architecture is illustrated in Figure 1, where the mobile device is used to indicate a patron tool. The cell device connects to the cell community via base stations, including the bottom transceiver station, access factor, or satellite. When a cell user requests for some responsibilities to be processed, facts (e.G., identification and place) is handover to the valuable processors linked to the servers for processing

Based on the house agent (HA) and cellular subscriber records stored inside the relevant databases, mobile network operators can decide whether or not to offer or decline requests to access specific offerings (i.E. Authentication, Authorization, and Accounting – AAA). After the mobile subscriber has been authenticated, the portable consumer's claim (s) could be forwarded to the cloud controllers (CC). The latter processes the requests and affords the applicable services



A modular Layout approach becomes advanced via Demirel et al. [9] to optimize packet forwarding policies and manipulate instructions. More lately, in 2017, Shu et al. [10] proposed a CPS structure designed for complicated industrial packages. The authors also described the solutions for three potential challenges, namely: scheduling of cloud

sources, virtualized resource management techniques, and life cycle management

II. RELATED WORK

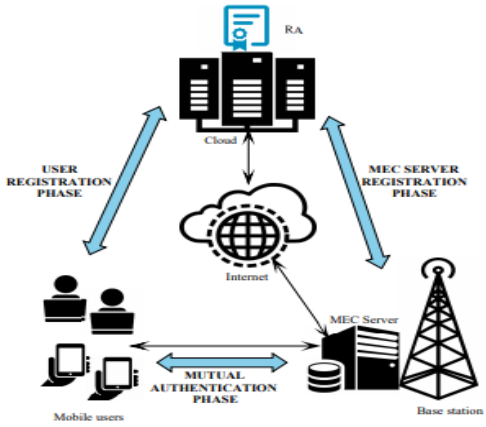
In this paper, out of the blue, we Signify and contend with the difficulty of success but relaxed positioned catchphrase appearance over scrambled cloud statistics. Placed are seeking unusual improve framework comfort through restoring the coordinating information in a posted request with appreciate to specific importance criteria (e.g., watchword recurrence).In this manner, making one step nearer towards down to earth arrangement of protection safeguarding statistics facilitating administrations in Cloud Computing. Supports green ranked keyword search for attaining dominant usage of remotely saved encrypted statistics in Cloud Computing [1].

In a ciphertext-coverage attribute-based encryption (CP-ABE) framework, decoding keys are characterized over characteristics shared by using numerous clients. Given an unscrambling key, it could no longer be continuously conceivable to observe the crucial first proprietor as a decoding gain might be managed through various clients. This difficulty extremely constrains the uses of CP-ABE. A few traceable CP-ABE (T-CP-ABE) frameworks were proposed to address this problem. But the articulacy of methods in those frameworks is restrained wherein only, and entryway with trump card is as of now strengthened [2].

Attribute-Based Encryption (ABE) with re-appropriated unscrambling no longer empowers pleasant-grained sharing of scrambled facts, but moreover beats the talent disadvantage (in the wording of ciphertext length and unscrambling price) of the standard ABE plans. In precise, an ABE plot with redistributed decoding permits an outsider (e.G., a cloud server) to trade an ABE ciphertext into a (quick) El Gamal-type ciphertext utilizing an open exchange key given by way of a client with the purpose that the final can be decoded considerably higher correctly than the previous by means of the purchaser. In any case, a deficiency of the primary redistributed ABE conspire is that the accuracy of the cloud server's exchange can't be checked with the aid of the customer [3].

To date, the development of electronic man or woman statistics ends in a pattern that facts proprietors need to remotely redistribute their information to mists for the pleasure inside the remarkable recuperation also, capacity advantage without stressing the weight of neighbourhood data administration and maintenance. Nonetheless, cozy provide and pursuit for the re-appropriated facts is an excellent sized assignment, which may additionally efficiently purpose the spillage of sensitive man or woman statistics. Useful records sharing and searching for with security is of simple importance [7]. This paper proposes a toolkit for green and privateness-retaining outsourced calculation below a couple of encrypted keys, which we seek advice from as EPOM. Using EPOM, a big scale of customers can securely outsource their information to a cloud server for storage. Moreover, encrypted statistics belonging to a couple of customers may be processed without compromising on the safety of the character consumer "s (authentic) facts and the very last computed outcomes. To lessen the associated key control price and personal key publicity threat in EPOM, we present a Distributed Two-Trapdoor Public-Key Cryptosystem (DT-PKC), the core cryptographic primitive [8].

III. SYSTEM MODEL



A typical MEC Environment includes the subsequent entities, i.E., a trusted Registration Center (RC), cellular users, and MEC servers; as depicted in Fig. 1. Here, the MEC servers are provided with computational and storage functionalities. These servers are geographically dispersed and deployed nearby of the cellular users; frequently at cell base

stations. Their closeness to the users helps lessen the latency and decorate the user revel in substantially. The mobile users can get entry to MEC services thru their motors, smartphones, tablets, etc. On the contrary, the RC is assumed to be a trusted third-celebration that helps initialize the cryptographic parameters and provides a not unusual platform for the registration of the users and MEC servers. The process of registration is critical for the proposed lightweight and privacy-maintaining authentication protocol. In the designed contract, it's far assumed that the customers and MEC servers get registered handiest once at some point of their lifetime. Thus, the RC is deployed on the remote cloud platform and isn't always concerned within the authentication process.

Proposed Method

In Proposed system, we introduced Relaxed and green file storage and sharing cloud surroundings the use of cell cloud. Mutual authentication could be essential among target tool because the person and to the cloud server as mutual authentication makes the server to believe the cloud storage where a person can store the facts and from server ceases, the server will verify the person credential to provide any service to that precise user.

Mutual authentication may be carried out with the aid of the use of the Diffie Hellman algorithm. DF set of rules will provide the standard key to sever and to the user based on their parameter. Vital Generation Centre might be the total relied on authority to generate the keys to the user as key are making at KGC the overload can't be there in the cell. When a user wants to add any record into cell cloud, then the person will generate the parameter for that unique record and offer the consumer attribute and request to KGC to create a key-based totally on that parameter. From that key person will encrypt the document and saved in the cellular cloud.

Cloud consists of the encrypted information at the side of the parameter associated with that file. If any person requests to the cloud server with some characteristic, based on the attribute cloud will redirect all the related data to the user. Which will decrypt the reporting person want the key for that report for that consumer request to KGC with the document characteristic.

IV. IMPLEMENTATION

Attribute-Based Encryption:

The main goal of the ABE is Amplify the safety in a higher manner and manage the accessibility of the information amongst humans the usage of it. ABE is an efficient set of rules which makes use of a public key, and with the collection of attributes values, it does its encryption and decryption manner effectively. It takes the consumer facts and the attribute set into essential attention to do the vital thing technology to use while decrypting the effects. Collusion resistance is the decisive element of the safety inside the system of Encryption in attributes primarily based Encryption. The keys reflect a real get right of entry to shape. The decryption is completed if and simplest if the keys are glad. The problem with the attribute-based Encryption is that it's the person. Who does Encryption does not realize all the set of attributes to nullify, and there may be danger of ending up with significant characteristics. When storage is a problem, the lack of records can be less. There isn't any want of server that mediates the report as an alternative the access guidelines should be widely known, and that is sufficient for the complete protection. The drawbacks of characteristic based Encryption totally can be its inefficiency and the coordination of the keys and the fundamental escrow problem.

Ciphertext Attribute-Based Encryption:

CP-ABE was introduced Sahai, and it is the next version of attribute-based Encryption. CP-ABE works at the scheme that the cipher textual content pertains to the two most important elements like the access policy. Which might be given to set of attributes and next is that it has to comprise a non-public key which is likewise associated with that set of characteristics. The decryption method occurs most effective if the ciphertext suits the policy this is connected with the collection of attributes. If this in shape, then a user can decrypt the cipher textual content. It works on one-many encryption techniques

and provides relaxed and flexible surroundings to the cloud authentication.

It works inside the contrary way of Key-Policy characteristic primarily based Encryption. The one extra feature of CPABE is that after the records are encrypted through pleasurable the guidelines, the non-public keys can be shared many of the customers. So, the Encryption can be finished without considering guidelines, but the decryption is achieved most effective if the instructions match.

Identity-Based Encryption

: It is one of the prominent methods Of cryptography. It works on public keys and contains a unique identity for the identity. The individual identification may be considered as an essential thing. ID-based Encryption was delivered in1984 by way of Adi Shamir. The central authority generated the keys for all the consumers. Usually, the name of the game keys and the distinct identification are made in the manner as an example sign-in quantity or the cope with. The server who has all get entry to to the ones parameters of the gadget can encrypt the facts the use of those parameters. Later the centralized one sends the vital thing to the purchaser. Identity-Based Encryption has the rights to generating public keys, and the non-public keys are made from the main authority. This can also cause critical escrow trouble. The IBE machine can also lessen the infrastructure of the general public key generation.

COMPARISION OF CHARACTERISTICS OF ALGORITHM

TABLE.1

Characteristics	*ABE*	*IBE*	*CPABE*
Platform	Cloud computing	Cloud computing	Cloud computing
Time of execution	54	28	9.89
Type of security	Less	moderate	more
Capacity of data encryption	256	256	3196
Authentication type	Less compared to CP-ABE	Better than ABE	More efficient
Memory usage	more	more	less

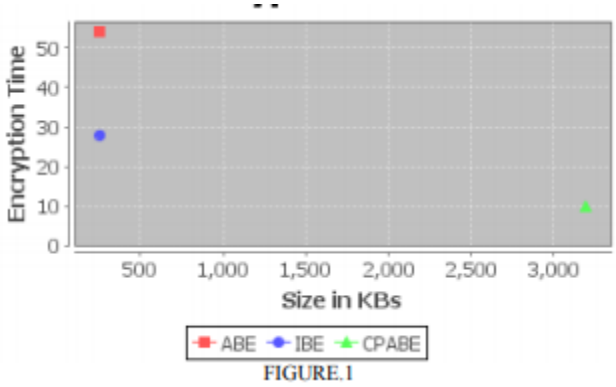


FIGURE.1

V. CONCLUSION

In this paper, a new identity-based Authenticated facts sharing (IBADS) protocol is designed for cyber-physical cloud systems primarily based on bilinear pairing. In the IBADS, there are two levels. First, new facts proprietor needs to register. Second, the facts proprietor sends an encrypted message to the untrusted cloud controller the usage of a few purchaser devices. We then have proven the safety and correctness of the protocol, in addition to evaluating its overall performance

In destiny studies, we intend to enforce a prototype of the proposed contract so that we will compare its practicability in an actual-world setting.

REFERENCES

[1] Nurul Hidayah Ab Rahman, William Bradley Glisson, Yanjiang Yang, and Kim-Kwang Raymond Choo. Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Computing, 3(1):50–59, 2016.

[2] Quang Do, Ben Martini, and Kim-Kwang Raymond Choo. Cyberphysical systems information gathering: A smart home case study. Computer Networks, 138:1–12, 2018.

[3] Hoang T Dinh, Chonho Lee, Dusit Niyato, and Ping Wang. A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing, 13(18):1587–1611, 2013.

[4] Qiang Liu, Jiafu Wan, and Keliang Zhou. Cloud manufacturing service system for the industrial-cluster-oriented application. 15(3):373–380, 2014.

[5] Daqing Zhang, Jiafu Wan, Qiang Liu, Xin Guan, and Xuedong Liang. A taxonomy of agent technologies for ubiquitous computing environments. KSII Transactions on Internet and Information Systems (TIIS), 6(2):547– 565, 2012.

[6] Jiafu Wan, Hehua Yan, Di Li, Keliang Zhou, and Lu Zeng. Cyberphysical systems for optimal energy management scheme of an autonomous electric vehicle. The Computer Journal, 56(8):947–956, 2013.

[7] Ragunathan Rajkumar. A cyber-physical future. Proceedings of the IEEE, 100(Special Centennial Issue):1309–1312, 2012.

[8] Akshay Rajhans, Ajinkya Bhave, Ivan Ruchkin, Bruce H Krogh, David Garlan, Andre Platzer, and Bradley Schmerl. Supporting heterogeneity in 'cyber-physical systems architectures. IEEE Transactions on Automatic Control, 59(12):3178–3193, 2014.

[9] Burak Demirel, Zhenhua Zou, Pablo Soldati, and Mikael Johansson. The modular design of jointly optimal controllers and forwarding policies for wireless control. IEEE Transactions on Automatic Control, 59(12):3252– 3265, 2014.

[10] Zhaogang Shu, Jiafu Wan, Daqing Zhang, and Di Li. Cloud-integrated cyber-physical systems for complex industrial applications. Mobile Networks and Applications, 21(5):865–878, 2016.