ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 9, Issue 6, June 2022

Verification And Key Agreement In View Of Mysterious Character For Shared Cloud

Arulmozhi.G , Bhuvaneshwari.R , FINAL CSE

Mr.K.Karthikeyen(Assistant professor in CSE)

Department of computer science and engineering

Bharathiyar Institute of Engineering For Women

Deviyakurichi-636112

Abstract—One of the most common issues faced by mobile customers is cross-cloud data migration, which is a necessary process when consumers switch their mobile phones to a new provider. However, due to a lack of local storage and compute power, It is frequently very difficult for people to understand the possibilities of smartphones. users should back up all data from the original cloud servers to their personal computers. mobile phones to continue efficient data movement paradigm between cloud providers, as well as mutual authentication and key agreement technique, to address this issue. For P the peer-to-peer cloud, we used cryptographic certificate-free cryptography. The recommended plan aids in the development of mutual trust. different cloud providers and establishes the basis because of its implementation. of data movement from one cloud to another Our scheme's mathematical verification and security accuracy are compared to well-known data migration strategies, demonstrating that ours is superior. In terms of the achieved reduction in both the cost and the time, the suggested plan outperforms previous state-of-the-art schemes. Costs of computation and communication Cloud computing, data transfer, elliptic curve, authentication, and key agreement are all terms that can be found in the index.

I. BEGINNING

With the rapid expansion of the smart phone and mobile terminal sectors, smart phones have become increasingly popular. People find it vital. China had an estimated population of 847 million people. In December 2018, there were 99.1 crores mobile users. % of them use their mobile phones to access the Internet [1]. Due to the computer's limited storage and processing capabilities, Users of cell devices frequently want to save huge data files (video and audio files, as well as streaming media) on their mobile terminals. files) stored on a cloud server This has sped up the study of different viewpoints on the cloud computing paradigm [3]. Manufacturers of smartphones are increasingly introducing and releasing new models. developing their own cloud computing services in order to give services to users, [5] and provide efficient data storage services. People are using hand-held devices like smartphones, tablets, and other such devices in record numbers. It's worth noting that a single person can own and use multiple properties. a number of smart devices Recycling is also very frequent. Given the fact that new technology is being introduced, people use their smart devices rather regularly. Arrivals are marked by more appealing innate characteristics from a wide range of manufacturers When customers want to use a new smart device from a different manufacturer, the data from the prior phone or tablet provider's cloud server should be transferred to the new phone or tablet provider's cloud server. The new smart device provider's cloud server. The Logging onto to the internet is a regular way to implement such transfer. Copy the original data center to the smart device .connect to the new cloud server via terminal devices, and finally transfer the information to the new server As seen in Figure 1 The procedure is inefficient and time-consuming. For this purpose, a more efficient and secure method of data movement from one cloud server to another is required. An optimal data migration model for transferring user data Figure illustrates data exchanged directly between cloud servers. Because models have varied requirements, they cause huge compatibility concerns. Multiple users function is given by

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 9, Issue 6, June 2022

cloud service providers In the process control process, there is both confidence and privacy risks. This ideal data migration model is based on transmission tough to put into practice. In past years, just few researchers that sought to solve data migration problems. For instance, Dana Petcu claimed in 2011 that the largest difficulties in cloud computing is figuring out what to do with all of the data. is cloud interoperability, and has proposed the new model. a method for achieving cloud portability Binz et al. [7] presented a cloud-based computing system. The migration of composites is supported by a motion framework. cloud-based applications or cloud-to-cloud applications Shirazi et al. published a study in 2012. created a system to facilitate data storage portability databases.

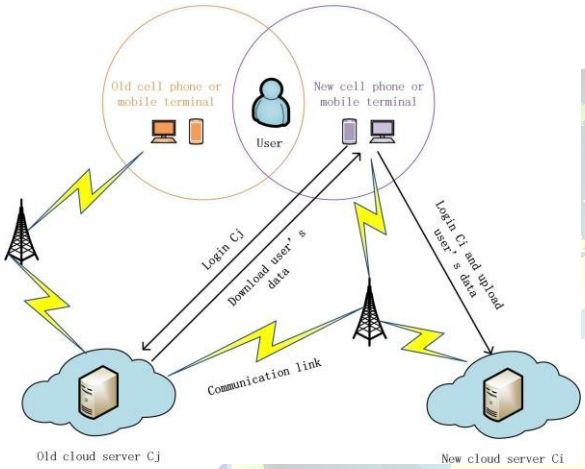


Fig. 1. Original data migration model

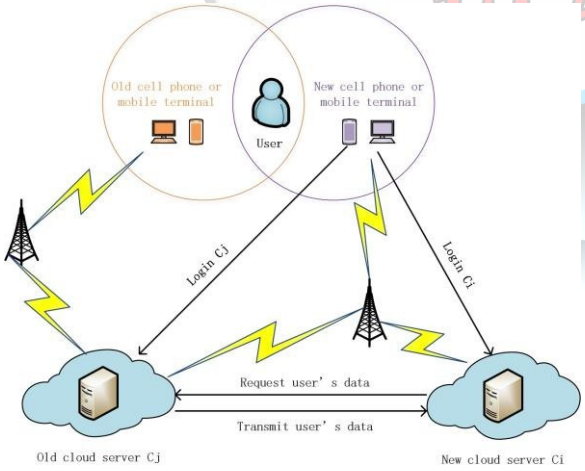


Fig. 2. Ideal data migration model

What Motivates Us

For starters, we learned that studying data migration across cloud platforms had a lot of practical implications. There are several unmet data transformation vulnerabilities between the clouds. challenges that could arise the Efforts that have already been made in the domain of cloud data Migration has clear drawbacks that limit its effectiveness. To put it in another way, further research into the context of cloud data is needed. Migration is a necessary and urgent necessity, particularly in the United States. That to allow faster and easier the data movement between cloud **services** After users switch cellphones, the servers are updated. Second, in the In practice, multi-cloud trustworthiness is difficult to establish. Especially in situations containing sensitive data, this has been accomplished. More security constraints are associated with transfers. As an example of obtaining mutual authentication and the constructing a communication transferring data safe and secure while avoiding potential cyber-attacks There are certain issues to consider. Authentication and key agreement mechanisms can be used to solve these issues in this case. Under light of this, this study provides a different solution. Using anonymous data as a basis for authentication and key agreement. identification for peer-to-peer cloud, with the goal of making it simple and accessible. data transfer between the many clouds in a secure manner

Our Contributions (B)

This is the first authentication and key agreement technique for peer cloud servers that we are aware of. The following are some of papers with most significant contributions.

• A peer-to-peer cloud authentication and key management system is proposed. agreement (PCAKA) mechanism based on the anonymous identity to address the issue of cloud server trust. The encryption is based on the elliptic curve certificate-free cryptography. Our system can create secure session keys between two parties. Session security must be ensured by cloud service providers.

• Our approach is unique in that it does away with the necessity for a trusted authority (TA) and simplifies operations while retaining security. Cloud hosting, under this design, allow data owners who require it to access their data. As a reliable third party, data migration services are available. so that they can trust each other and check each other keys between cloud service providers to ensure session security Our system is unique in that it does away with the necessity for a trusted authority (TA) and streamlines operations while retaining security. The cloud hosting in our scheme allow data owners in need of data migration services to operate as trusted third authorities, allowing them to authenticate each other and establish

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 9, Issue 6, June 2022

trustworthy session keys once each of the participating users has individually performed some calculation. To secure the privacy of service providers and users, our approach employs site obscurity. It is worth noting that both cloud servers participating in the migration process use anonymous identities for mutual authentication and key agreement. This technique is not only protects the privacy of one's identity, but it also protects privacy of others. of the cloud service providers, but this also makes it almost impossible for such service providers to obtain superfluous information, such as the user's IP address Old and new mobile phones belong to Similarly, the users As a result, our process remains consistent. by not disclosing personal information about customers' privacy choice We use our approach to track down malicious cloud servers as it enables us to identify and trace them. If the cloud service providers show up, it'll be a good sign. Any mistakes or illegal actions made during the service procedure Based here on an anonymized profile, users can trace back to the real identity of the related data center. The Structure of the Rest of the Paper We introduce the few pieces related to the data migration and key exchange in Section II. Section III discusses our strategy's key prerequisites as well as their system model. Then we go over the specifics of our PCAKA scheme that we've proposed. Sections V and VI of the fourth section show how to encrypt data. Validate the proposed security level and ensure that it is correct. As an example, strategy This paper comes to a close with Section VII. We begin by sketching out our long-term research goals.

WORK IN CONNECTION WITH THE SECOND

A few approaches [9] through [13] have used techniques to facilitate the sharing of data in the cloud. Liang and Cao [9], for example, proposed the property-based proxy. a re-encryption mechanism that allows users to gain authorization. When it comes to access control, Lian and Au [10] disagree. It was pointed out that this system lacks adaptive security. as well as the CCA security features. Sun et al. [12] proposed the new concept. PBR is a proxy broadcast repeat encryption system that has been proven to work. In a CCA (selective decryption attack), its security The decision n-BDHE assumption generates a random oracle model. Ge and Liu [13] suggested a removable The agency in this circumferential scheme will use the re-encryption key to modify a collection of the representatives that the principal has defined. They also mentioned that the broadcast agent re-encryption is identity-based (RIB-BPRE). As a result, schemes do not make use of cloud computing. Cloud service services are inconvenienced. Liu et al. [14] suggested a method for securely transferring data across several owners. strategy for their cloud-based dynamic groupings. On the basis of the group Any solution that includes signatures and variable broadcast encrypting is appropriate. Users of the cloud can share their data with others anonymously. Yuan et al. [15] proposed a system to validate the quality of cloud user data. It depends on the updating of the polynomial authentication tag and their agent tag. technology that allows for multi-user modification in order to combat Other capabilities involve collusive attack. [16] Ali et al. based broadcast agent encryption (RIBBPRE) security paradigm to overcome the problem. The main revocation issue Se Da SC is a secure data sharing cloud approach that encrypts information using a single encryption key. Data confidentiality and integrity, forward and backward access control, data exchange, and other services are all provided by this scheme. Li et al. [17] offered a fresh way of looking at things. a data-sharing mechanism based on attributes to help mobile users. Cloud computing has a finite amount of resources. Authentication and key agreement is a technique that allows you to authenticate and agree on a set of keys. Both participants must calculate the session key in secret on a public computer. channel, which has been extensively investigated [18][31]. As early as possible, Maurer [18] argued in 1993 with simply a change in the use of received signals aids in the achievement of full cryptographic security. no matter how powerful the enemy's computer is. However, they have not taken into account the benefits of authorized communicants. notwithstanding, suffices for establishing absolute cryptographic security notwithstanding. The adversary's computer power [19] Lu and Lin proposed a medical key negotiation scheme is based on the symptoms of the patient. matching He et al. [32] pointed out, however, that Lu's No identification, tracking, or resistance is provided by the scheme. As well as the cross-domain A handshake mechanism that can be used in a medical mobile social network as well as an Android app for experimentation. Liu and Ma [20] later discovered that He et cetera. did not work. fend off a repeat attack. and Lo [21] suggested a distributed mobile cloud computing service authentication technique with a variety of features, including user anonymity. Irshad and Sher [23] improved [the 21] technique to make a it more suited. for use in a variety of wireless mobile access scenarios. Networks, on the other hand, were mentioned by Jia and He [33]. The system proposed by et al. is vulnerable to impersonation and man-in-the-middle attacks. In addition, Irshad et al.'s Perfect forward privacy isn't supported by the scheme. Love and adoration Abbas [24] presented a strategy for fog verification. In the context of user anonymity, users and fog servers interact. The Mahmood et al. [26] presented an anonymous key negotiation. A Smart Meter can connect to providers surreptitiously using this protocol for power systems. However, Wang and Wu [31] pointed out that Amor et voila. susceptible to thIt is vulnerable to verifier attacks. Attacks such as man-in-the-middle and impersonation are common

[III. PRELIMINARY CONFERENCE]

Elliptic Curve (A)

An elliptic curve E(F p) is supported by a finite field FP, where p is positive integer. is a significant prime number. Y FP is defined as:

x = 2 3 + x+ output and equals 4 are constants.27 + 2

2 + 6 = 0. After modifying We refer to the point of infinity as O. I. and all other points as P. The multiplicative cycle group Meghan exists in the E (FP) form.

B. Difficulty Issue

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 9, Issue 6, June 2022

Any probabilistic linear time adversary has yet to solve the following complexity problem: We'll make use of them. Later on in the process of management and access control The problem of the Elliptic Curve Computable Discrete Logarithm (ECCDL) is as follows: Allow GQ to speak for itself. P is the GQ generator. The most important thing is to figure out Z.∗ q which is not well-known and to Ensure that the criterion P is met. After each of the people interested has individually computed anything, the session keys are created.

• To preserve the privacy of consumers, you utilize network anonymity. Providers and users of services. It's worth noting that both of their cloud servers that will be used in the migration For mutual cryptographic verification, organizations use anonymous personalities. [6] discussed because of various appealing focal points, agreeable correspondences have been broadly viewed as one of the promising systems to enhance throughput and scope execution in remote interchanges. The System's Representation Due to the uniqueness of our concept, we substitute a trusted authority (TA) for the typical trusted authority (TA). the users, in order to generate system parameters and partial results. distribution of keys Our approach includes three entities, including a smartphone user U and two cloud servers Ci, C j, as shown in Fig. 3.

• U: The consumer of either a cell phone who makes system parameters public. This sends out partial private keys to both the cloud and the user servers.

• Cloud or Ci

The cloud server for requesting data. This website's server verifies the user's identity and performs reciprocal check With the help of C j, I was able to verify my identity and negotiate a key.

• C j or Cloud j: The online cloud which also holds their source data. This website's server verifies the user's identity and performs reciprocal checks Using Ci for authentication and key negotiation Users should register and connect to both the cloud server Ci (the new provider) and the cloud server C j (the original mobile device) while changing their mobile devices in our model. telephone service provider). The two cloud servers are now in a peer-to-peer relationship. scenario. The user shares a portion of the private key with both parties over a secure link to the cloud servers Then there were Ci and C j. Ci sends a request message, and they exchange information. to C j to start the mutual authentication and key exchange process.

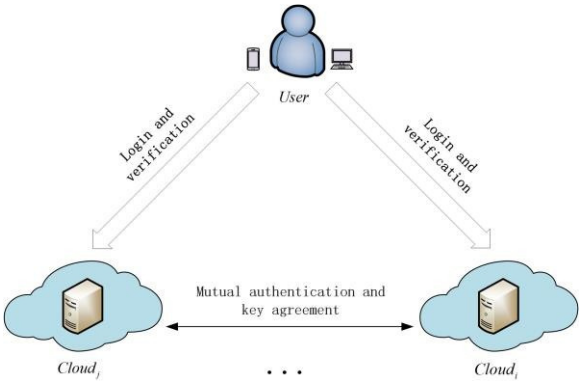


FIGURE 3: SYSTEM MODEL IV. THE PACKAGE PROPOSED SCHEME

This section goes over the specifics of our proposed strategy. There are three phases to the proposed PCAKA project. The PCAKA scheme employs the symbols listed below.

• IIDA Intelligent Design) Ci's real name is ci

• C j 's identity (I D j) the page Ci's alter ego

• C j 's pseudonym is paid.

FIGURE 3: THE PCAKA PROPOSED SCHEME FOR SYSTEM MODEL IV

The specifics of our recommended plan are discussed in this section. The intended PCAKA project is divided into three parts. The symbols used in the PCAKA scheme are mentioned below.

• I D I (Intelligent Design) (Intelligent Design)

Ci is Ci's true name.

• C j s real name (I D j)

Ci's doppelganger

• PIDJ is C j' s pseudonym.

Phase B: Log in

The user logs in and assigns a key to the cloud server at this point. This process is carried out by the user and the cloud server as indicated in Figures 4 and 5.

Ci Participate in Phase

1) User U accesses the Ci cloud server. computes Xi =xiP, and saves (xi,yYi as its private key if all else fails. Finally, Ci makes Ri and the public key public (Si, Xi).

Cj Participate in the Phase

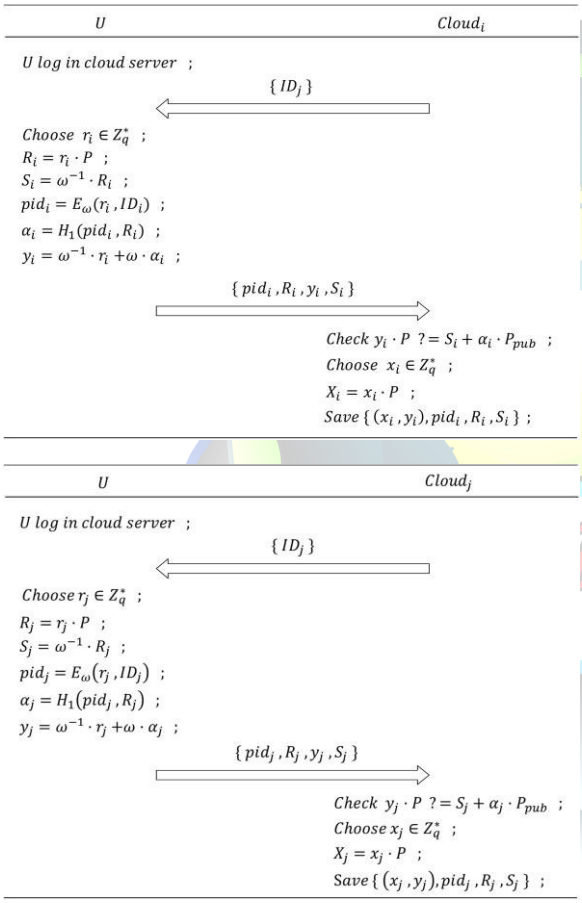
1) log in to the cloud server C j as user U.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 9, Issue 6, June 2022

2) C j uses the encrypted channel to convey its identify ID j to U.

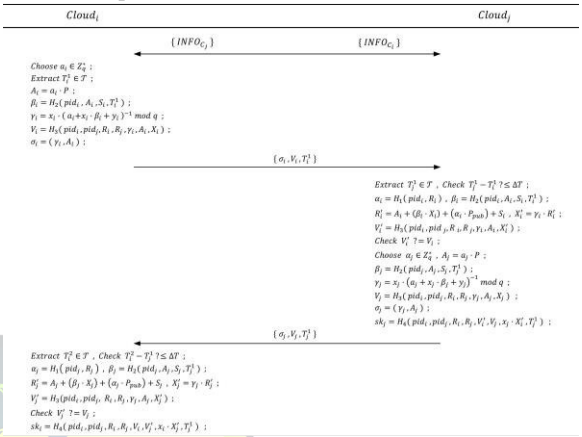
3) U selects an element r j Z q at random and saves it secretly. U creates C j's pseudo identity pi dj = E by computing R j = r j P ,S j = 1Rj and R j = r j P, S j = 1Rj (r j, ID j). Then U computes j = H1(pi d j, R j),y j = 1rj + j as j = H1(pi d j, R j). Finally, U uses a secure channel to communicate pi d j ,R j, y j, S j to C j. [8] discussed that Helpful correspondence is developing as a standout amongst the most encouraging procedures in remote systems by reason of giving spatial differing qualities pick up. The transfer hub (RN) assumes a key part in agreeable correspondences, and RN choice may generously influence the execution pick up in a system with helpful media get to control (MAC),



A phase of the C. Cloud Handshake

Proof. Assume that adversary A can fabricate a lawful login or the related response information with a non-negligible probability. Now we'll show how challenger C can solve the ECCDH problem with a non-negligible probability. nm. C chooses the request cloud CI at random and then considers the responder cloud CJ as the challenge cloud, both of which have IDI and IDJ as their identities. C generates four integers at random at the start of the P and sends Pub, H1, H2, H3,H and 4 to A as arguments. The following is how challenger C interacts with adversary A:

• H k MK k): When A runs the query with message me, C checks if the tuple is in the list L H k (MK ,nk).



. If it exists, C returns nk to A; Otherwise, C randomly produces a number nk ∈ Z ∗ q, and insert the tuple (mk, into Lk , where k = 1, 2, 3, 4. Finally, C gives nk to A as the return value. • SymEnc MKk, kk, ck): Upon receiving the symmetric encryption query on message MKk and key kk, C checks if the list Lse has the tuple MK k,). If it exists, C returns CK to A; Otherwise, C randomly produces a string CK∈ ZCK q, (m k, n into to L where k = 1, 2, 3, 4. Finally, C gives n k to A as the return value. • Extract Sec(ID k): Upon receiving the extract query with cloud identity ID k, C checks if the list L 1 cloud has the tuple (ID k, x k, X k). If it exists, C returns xk to A; Otherwise, C randomly selects a number x k ∈ Z ∗ , computers X k= x k P. Finally, C stores the new tuple in L 1 cloud and returns it to A. • Extract P are (ID k): Upon receiving the extract query with cloud identity IDk, C checks if the list L 2 cloud has the tuple (ID k, Rk, yk)YKIf it exists, C returns yk to A; Otherwise, C executes as follows: - If IDk = ID , C selects random numbers I , pidI ∈ Z ∗ q And then, C inserts the tuple (rII ⊥, pidI) into the list Lse. C computes RI = rIP and sets yI =⊥. Finally, C stores (pi d I , I αI) an (and I , pride, RI , ⊥) into LH1 and L 2 cloud respectively. - If IDk = IDJ , C selects random numbers RJ , pidJ ∈ Z ∗ q. Now, C inserts the tuple (rJ ⊥ , pidJ) into the list L se. C computes RJ = rJP and sets yI you. Finally, C stores (piDJRJ , αJ) and (IDJ , pidJ , RJ , ⊥) into LH1 and L 2 cloud respectively herewise, C selects random numbers rk, pidkpink ∗ q . Now, C inserts the tuple (rk, ⊥, pidk) into the list Lse. C selects a random number αk ∈ Z ∗ q , comutes Rk = rkP − αkPpub and sets yk = rkαk. Finally, C stores (pidkpinkinkk) and (IDk, pidk, Rk, yk) into LH1 and L 2 cloud respectively. • Send(Πk Λ , m): When receiving the query of message m, C responds as follows: - If m = (σi , i): he query is message m, which is from Ci to Cj . ∗ If Ci = CI , C terminates the session. ∗ If Ci 6= CI , C= CJ , C terminates session. ∗ If Ci 6= CI , Cj 6= CJ , C per coperates to the protocol's specification. - If m = (σj , Vj): The query is message m, which is from Cj to Ci . ∗ If C = CJ , C terminates the session ∗ If Cj 6= CJ , Ci = CJ , C terminates the session. ∗ If Cj 6= CJ , Ci 6= C , according to

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 9, Issue 6, June 2022

the protocol's specification. • Reveal(Πk Λ): When receiving the query, C checks if Πk Λ = ΠK CI or Πk Λ = ΠK CJ . If yes, C aborts the session. Otherwise, C gives the session key of Πk Λ to A as the return value. • Corrupt(IDk): When receiving the query, C looks up the tuple (IDk, xk, Xk) and (IDk, pink, pinky) from the list L 1 cloud and L 2 cloud respectively. At last, C returns (xk, Xk, Rk, yYK to A. Now, A outputs a legal login message σi or respond message σ j of its correspondent. If (Ci , Cj) 6= (CI , CJ), C terminates the game. Otherwise, C randomly selects a tuple (∗, pidi pidj , Ri , R , γi , X0 i , ∗) or (∗, pdi , pidj , Ri , Rj , γj , A , X0 j , ∗) form the list LH3 . Ten C outputs X 0 i or X 0 j as the solution of ECCDH problem. If C can solve the ECCDH problem with the probability 0 , the system to satisfy the following events.

• E1: C does not terminate any Extract Sec query.

• E2: C does not terminate while responding to Send query.

• E3: C outputs a legitimate login message or its responder's message.

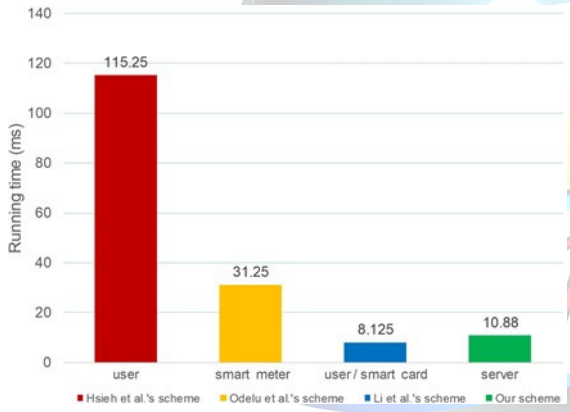
• E4: response Cj) = (ΠK CI , ΠK CJ). • E5: C selects a right tuple from the list LH3 . Letthesend , denotes of Extract Sec queries, Send queries, Hash queries and instance Πk Ci (or Πk Cj). n denotes the number of, cloud service providers registered by users in the system. Then we obtain: P r[E1] ≥ (1 − 2 q + 1) qes P r[E2|E1] ≥ (1 − 2 send + 1) send P r[E3|E1 A E2] ≥ P r[E4|E1 A E2 A E3] ≥ 1 mi[E5|E1 A E2 A E3 A E4] ≥ 2 qH3 Therefore, the probability 0 that C can solve the ECCDH problem is calculated as below. 0 = P r[E1 A E2 A E3] A E4 A E5] = P r[E1] · [P r[E2|E1] · P r[E3|E1 A E2]· P r[E4|E1 A E2 A E3] · P r[E5|E1 A E2 A E3 A E4] ≥ 2 · (1 − 2 qes+1) qes · (1 − 2 qsend+1) qsend n · qins · qH3 (1) This is the opposite of the difficulty of send ECCDH problem. Thus we obtain the conclusion that any PPT adversary C can not fake a legal login information or the corresponding response information with a non-negligible probability. Theorem 1. When the ECCDH problem is hard, the proposed PCAKA protocol P is MA-secure. ng to lemma 1, we know that there no polynomial adversary can fake a legal login information a corresponding response information that on while the ECCDH problem is hard. Hence, we to confirm that the PCAKA protocol is MAsecure. Theorem 2. The proposed PCAKA protocol P is AKA-secure if the underlying ECCDH problem is hard. Proof. We assume that a PPT adversary A can correctly guess b with a non-negligible probability during the T est query. A challenger C solves the ECCDH problem with a non-negligible probability as follows. Let ESK represents the event that A acquire the right session key about Ci and Cj . We can et P r[ESK] ≥ 2 , due to the probability that A guesses a right b is at least 1 2 . Let ET esti and ET estj represent the event that A usthe T est query to Ci and Cj and obtains their session key, respectively. If A can forge a legal login message, then A can break the Ci − to − Cj authentication. This event is denoted by Ei→j . Thus, we obtain the below. P r[ESK] = P r[ESK A ET esti] + P r[ESK A ET estj] = P r[ESK A ET esti] + P r[ESK A ET estj A Ei→j] + P r[ESK A ET estj A ¬Ei→j] ≤ P r[ESK A ET esti] + P r[Ei→j] + P r[ESK A ET estj A ¬Ei→j] (2) That is to say, P r[ESK A ET esti] + P r[ESK A ET estj A ¬Ei→j] ≥ 2 − P r[Ei→j] (3) Because ET estj A¬Ei→j and ET esti are equivalent, we get P r[ESK A ET esti] ≥ 4 − P r[Ei→j] 2 (4) Thus, the probability that A breaking the authenticated key agreement is P r[ski = H4(∗, ∗, ∗, ∗,(xi · xj) · P, ∗)|xi, xj ∈ Z ∗ q] ≥ 4 − P r[Ei→j] 2 (5) According to the above, we know that P r[Ei→j] is negligible and is non-negligible. Thus, 4 − P r[Ei→j] 2 is non-negligible. Namely, the adversary A can solve the ECCDH problem. This conclusion contradicts with of the ECCDH problem. Thus, we conclude that PCAKA protocol is AKAsecure on the premise that ECCDH problem is hard. C. Security Analysis In this section, we analyze the security characteristics of the PCAKA scheme under the above "Security Model". Mutual Authentication. According to lemma 1, no polynomial probability time adversary A can fake a legal login or response information. [2] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). Thus thesession key ski = H4(pidi , pidj , Ri , Rj , xi ·X 0 j , T1 j) iscalculated. In the same way, Cj figure out skj = H4(pidi , pidj , Ri , Rj , xXj· X 0 i , T1 j).Xj according to section 4,however,Xi = X 0 i (Xj = X 0 j), xi · X 0 j = xi · xj · P = xj · X 0 i . WeXjan obtain ski = skj . Thus, the proposed PCAKA scheme supports session key negotiation. Identity Anonymity. The two parties participating in the cloud handshakes and interactions with anonymous identities pidi = Eω(ri , IDi) apickidj = Eω(rj , IDj) in the PCAKA protocol. For them, anonymity protects the privacy of their identities when interacting with data on public channels. The adversary A can not extract the IDi(IDj) from the pidi(pidj). Thus, the proposed PCAKA protocol supports cloud anonymity. Identity Traceability. Cloudi (or Cloudj) uses an anonymous identity pidi (or pidj) to send error messages or illegal information tothe , user U can use ω to extract the real identity IDi(or IDj). Therefore, the PCAKA scheme supports identity tracking. Perfect Forward Secrecy. Suppose the adversary A can access the current private keys (xi , yi) and (xj , yj) of the cloud servers, respectively. However, the random numbers xi and xj are generated by Ci and Cj , respectively, and are updated with the process of building the session key each time. In addition, in order to obtain the previous xi and xj , A needs to them from the previous Xi and Xj , so that Xi = xi · P, Xj = Xj · P. That means A needs to be dealt with the ECCDL problem. Therefore, the PCAKA scheme provides perfect forward secrecy. Replay attack. Timestamps (T 1 i , T1 j , T2 i) are used in the authentication process of the PACAKA protocol.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 9, Issue 6, June 2022

Communications from both the side generate fresh random numbers (ai , aj) and compute Ai = ai · P, Aj

computationally trivial hash operation and modular exponentiation operation when designing operations for the session sponsor. However, in our scheme, although the session sponsor is the cloud server, it used the elliptic curve point multiplication operation with cross computational overheads, so the sponsor's computational overhead is still greater than that ofder side the session , both Hs et al.'s Odelle and Odelu et al.'s scheme used point-to-points and bilinear pairing operations that require an intense computation, so their schemes characterize high computational overheads. In Li et al. scheme, although theircomputationally intensive contains containsnly one bilinear operation and one hash-to-point operation, the responder side still comprises high computational overheads. Our scheme only uses five point multiplication and other low-computational operations, a the lowest characterizesl overhead among the studied four schemes. [4] discussed that the activity related status data will be communicated consistently and shared among drivers through VANETs keeping in mind the end goal to enhance driving security and solace. Along these lines, Vehicular specially appointed systems (VANETs) require safeguarding and secure information correspondences.



CONCLUSION

This paper proposed a novel scheme to transfer user data between different cloud servers based on a key agreement protocol. Through the mathematical analysis and comparative evaluation presented in this paper, the advantages of our schemeare proved from three aspects: security performance, calculation costs, and communication costs. Our proposed scheme can efficiently solve the primary problem of trust during data migration between cloud servers and further can provide anonymity for the identity of cloud servers. On the premise of protecting the privacy of cloud service providers, our proposed scheme indirectly protects the privacy of users. In addition, the identity traceability provided by our proposed scheme alsoenables users to effectively constrain the cloud service providers. In future work, we plan to explore and develop a protocol that allows multiple users to share data across different cloud servers, with the motivation of enhancing the efficiency of data sharing among multiple users.

REFERENCES

[1] C. I. network information center, "The 44thchina statistical report internet development," http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/ 201908/P020190830356787490958.pdf, 2019.

[2] Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)..

[3] J. Cui, H. Zhou, H. Zhong, and Y. Xu, "Akser: attribute- based keyword arch with efficient revocation in cloud computing," Information Sciences, vol. 423, pp. 343–352, 2018.

[4] Christo Ananth, Dr.S. Selvakani, K. Vasumathi, "An Efficient Privacy Preservation in Vehicular Communications Using EC-Based Chameleon Hashing", Journal of Advanced Research in Dynamical and Control Systems, 15-Special Issue, December 2017,pp: 787-792.

[5] J. Cui, H. Zhou, Y. Xu, and H. Zhong, "Ooabks: Online/offline attributebased encryption for keyword search in mobile cloud," Information Sciences, vol. 489, pp. 63–77, 2019.

[6] Christo Ananth, Dr. G. Arul Dalton, Dr.S.Selvakani, "An Efficient Cooperative Media Access Control Based Relay Node Selection In Wireless Networks", International Journal of Pure and Applied Mathematics, Volume 118, No. 5, 2018,(659-668).

[7] T. Binz, F. Leymann, and D. Schumm, "Cmotion: A framework for migration of applications into and between clouds," in 2011 IEEE International inference on Service-Oriented Computing and Applications (SOCA). IEEE, 2011, pp. 1–4.

[8] Christo Ananth, Joy Winston.J., "SPLITTING ALGORITHM BASED RELAY NODE SELEC-TION IN WIRELESS NETWORKS", Revista de la Facultad de Agronomía, Volume 34, No. 1, 2018,(162-169).

[9] X. Liang, Z. Cao, H. Lin, and J. Shao, "AttriAttribute-babasedebbased with delegating capabilities," in Proceedings of the 4th tInternationalposium on Information, Computer, and Communications Security, 2009, pp. 276–286.

[10] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, Y. Yu, and Yang, "A secure and efficient ciphertext-policy attribute-based re-encryption for cloud data sharing," Future Generation Computer Systems, vol. 52, pp. 95–108, 2015.