Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023

SECURED DATA ACCESS WITH CRYPTOGRAPHY FOG COMPUTING

T. RAJKUMARAN, Research Scholar, PG & Research Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam, Tamil Nādu, India
Dr. T. K. SHANMUGAM Research Supervisor, Associate Professor & Head Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam, Tamil Nādu, India

Abstract-
Fog computing is a paradigm that extends cloud computing to the edge of the network. It can provide computation and storage services to end devices in Internet of Things (IoT). Attribute-based cryptography is a well-known technology to guarantee data confidentiality and fine-grained data access control. However, its computation al cost in encryption and decryption phase is linear with the complexity of policy. Fog nodes are implemented near to end-users Internet of Things (IoT) devices, which mitigate the impact of low latency, location awareness, and geographic distribution unsupported features of many IoT applications. Moreover, Fog computing decreases the data off load into the Cloud, which decreases the response time. Despite these benefits, Fog computing faces many challenges in meeting security and privacy requirements.

In this paper, we propose a secure and fine-grained data access control scheme with cipher text update and computation outsourcing in fog computing for IoT. The sensitive data of data owner are first encrypted using attribute-based encryption with multiple policies and then outsourced to cloud storage. Hence, the user whose attributes satisfy the access policy can decrypt the cipher text. Based on the attribute-based signature technique, authorized user whose attributes integrated in the signature satisfy the update policy can renew the cipher text. Specifically, most of the encryption, decryption, and signing computations are outsourced from end devices to fog nodes, and thus, the computations for data owners to encrypt, end users to decrypt, re-encrypt, and sign are irrelevant to the number of attributes in the policies. The security analysis shows that the proposed scheme is secure against known attacks, and the experimental results show that the fog nodes perform most of the computation operations of encryption, decryption, and signing, and hence, the time of encryption for data owner, decryption, re-encryption, and signing for users is small and constant.

Theoretical- Mist computing could be a worldview that amplifies cloud computing to the edge of the arrange. It can give computation and capacity administrations to conclusion gadgets in Internet of Things (IoT). Attribute-based cryptography could be a well-known innovation to ensure information privacy and fine-grained information get to control. Be that as it may, its computational fetched in encryption and decoding stage is direct with the complexity of arrangement. Haze hubs are actualized close to end-users Web of Things (IoT) gadgets, which moderate the affect of moo inactivity, area mindfulness, and geographic dispersion unsupported highlights of numerous IoT applications. Besides, Haze computing diminishes the information offload into the Cloud, which diminishes the reaction time. In spite of these benefits, Mist computing faces numerous challenges in assembly security and security requirements.

In this paper, we propose a secure and fine-grained information get to control plot with cipher content overhaul and computation outsourcing in mist computing for IoT. The sensitive data of information proprietor are to begin with scrambled utilizing attribute-based encryption with numerous approaches and after that outsourced to cloud capacity. Consequently, the client whose traits fulfill the access approach can decode the cipher content. Based on the attribute-based signature strategy, authorized client whose qualities coordinates within the signature fulfill the upgrade approach can recharge the cipher content. Specifically, most of the encryption, unscrambling, and marking computations are outsourced from conclusion gadgets to mist hubs, and in this way, the computations for information proprietors to scramble, conclusion clients to decode, re-encrypt, and sign are

unessential to the number of qualities within the arrangements. The security examination appears that the proposed plot is secure against known assaults, and the exploratory comes about appear that the mist hubs perform most of the computation operations of encryption, decoding, and marking, and thus, the time of encryption for information proprietor, unscrambling, re-encryption, and marking for clients is little and constant.

KEYWORDS:
Web of Things, mist computing, get to control, information security, trait based encryption.

INTRODUCTION

characteristics can be used to sign communications in an ABS system.

Due to the exceptionally tall volume of communication between IoT gadgets and the cloud, centralized computing frameworks are starting to involvement unfortunate transmission delay and disabled usefulness. Mist computing may be a potential innovation that leverages the IoT's area mindfulness, geo dispersion, moo idleness, portability bolster, etc. as well as the cloud computing standards. Scrambling information already some time recently transfer is one conceivable arrangement to such issues. These prerequisites are met by the one-to-many cryptographic method known as attribute-based encryption (ABE). It contains a system that grants get to arrangements and allotted properties between private keys and figure writings to control get to to scrambled material.

The get to arrangement for the information is characterized utilizing Figure content Upgrade and Computation Outsourcing over a run of qualities that the client must have in arrange to translate the figure content. Information privacy and granular get to control may be guaranteed in this way.

The client who upgrades the figure text must thus be able to demonstrate to the cloud benefit supplier (CSP) that he may be a true blue client, as typically the vital component of secure figure content upgrading. The customary strategy involves marking the upgraded information, which requires that CSP at the same time keep up a open key list of genuine clients to affirm the users' personalities. The key list would require a parcel more work to preserve on the off chance that there were a part more clients, and CSP may learn the characters of clients in this strategy, which compromises client protection. An inventive cryptographic strategy called attribute-based signature (ABS) can help CSP in deciding whether the client is genuine. A claim arrangement and the user's characteristics can be utilized to sign communications in an ABS system.

2.PRINCIPLES OF CRYPTOGRAPHY

Clients would have genuine stresses around information security when putting away delicate information on cloud servers through haze hubs since, like cloud servers, they are not totally trusted .Since the organize engineering and framework models are distinctive, a modern get to control technique counting the cloud, mist, and clients ought to be taken into thought. In this conspire, mist hubs ought to help clients, coming about in diminished computational complexity and more noteworthy adaptability for users.

In arrange to execute adaptable, versatile, and fine-grained get to control frameworks, ABE may be a practical cryptographic strategy. Sahai and Waters were the ones who at first proposed the thought of ABE as a new approach to fluffy identity-based encryption. There are two sorts of ABE: CP-ABE and key-policy ABE (KP-ABE). made a secure information transmission convention between wearable sensors and information shoppers. A CP-ABE method against key-delegation abuse in haze computing was presented by Jiang et al. Yeh et al. recommended a fine-grained cloud-based get to administration design for wellbeing data for convenient IoT devices.

The primary objective of display frameworks is to spread computations of the CP-ABE encryption and decoding stage in arrange for compelled IoT gadgets to outsource the lion's share of

the resource-intensive errands to arrange hubs. For restorative WSNs, Lounis et al. created a cloud-based design where sensor hubs designate encryption chores to a solid portal, which hence scrambles information utilizing CP-ABE some time recently sending it to the cloud. In any case, it is inconceivable to effectively outsource computers since, in this way, information encryption is managed by a completely legitimate firm.

These strategies, be that as it may, can as it were empower either outsourced encryption or decoding. The difficult computation of encryption and decoding is outsourced to mist hubs in Zhang et al.'s proposed get to control procedure for mist computing, so the calculations for information proprietors to scramble and users to decode are disconnected to the sum of characteristics in get to policy.

To execute figure content overhaul administrations in haze communication, the CSP must be able to confirm the user's verification some time recently tolerating the modern figure content. Mysterious client confirmaction is given utilizing the rising signature method known as ABS. In this approach, information is confirmed by the cloud earlier to sparing without information of the client displayed an expressive ABS framework for the Web of Things that takes utilize of an quality tree to guarantee that as it were a client who complies with the get to approach criteria and has the essential qualities may support the message. In any case, a expansive sum of preparing time and cash are required for the signature stage of the current ABS strategies, and this taken a toll rises directly with the size of the predicate formula.

3. CRYPTOGRAPHY AND PRELIMINARIES

Let G0 and GT be two multiplicative bunches of prime arrange p. A bilinear outline could be a work $e : G0 \times G0 \rightarrow GT$ with the taking after properties:

1) Computability. There's an effective calculation to compute $e(g, h) \in GT$, for any $g, h \in G0$
2) Bilinearity. For all $g, h \in G0$ and $a, b \in Zp$, we have $e(g^a , h^b) = e(g, h)^{ab}$.
3) Non-degeneracy. In the event that g could be a generator of G0, at that point e(g, g) is additionally a generator of GT .

3.1 Get to Tree

Let T stand for a tree, which speaks to an get to approach coherently. With the assistance of its descendant and a edge esteem, each non-leaf hub x speaks to a edge entryway. Let numx stand for a hub x's number of children and kx for its edge esteem. We have ky=1 for each leaf hub y. Let parent(z) stand in for the parent hub of the hub z within the tree, and let at try stand for an property related to leaf hub y within the tree. Within the tree, each child hub of the hub x is named from 1 to numx, and index(x) gives the name that compares to the hub x. This get to tree's hubs are given these list values in arrange to be uniquely recognized by a particular key in an subjective manner

3.2 Ciphertext-policy Encryption Based on Attributes

A CP-ABE system for get to approach T comprises of the taking after four algorithms.

1) Setup(1^κ): The setup calculation takes as input the security parameter κ and yields a open key PK and a ace mystery key MK.
2) KeyGen(PK, MK, S): The key era calculation takes as input the open key PK, the ace mystery key MK, a set S of traits, and yields a mystery key SK.
3) Enc(PK, M, T): The encryption calculation takes as input the open key PK, a message M and an get to arrangement T , and yields a ciphertext CT.
4) Dec(PK, SK, CT): The decoding calculation takes as input the open key PK, a mystery key SK, a ciphertext CT with an get to approach T . In the event that $S \in T$, it outputs the message M.

3.3 Signature Based on Attributes

The ABS conspire comprises of four calculations as follows:

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023

1) Setup(1κ): The system setup is the calculation run by the quality specialist for which the input is the security parameter κ and the yields are open key PK and ace mystery key MK.
2) KeyGen(PK, MK, S): The key generation is the calculation run by the trait specialist on inputs open key PK, master secret key MK and a set of qualities S to create the mystery key SK for the underwriter.
3) Sign(PK, M, T , SK): The marking is the calculation run by a endorser on inputs PK, a message M, a claim arrangement T and mystery key SK to produce a signature ST for the message.

3.4 Validate (PK, M, T , ST):

The confirming is the calculation run by a verifier on inputs PK, a message M, a claim arrangement T and a signature ST. The yield is genuine on the off chance that ST may be a substantial signature by a underwriter whose traits fulfilling T.

4. SYSTEM MODEL AND SECURITY MODEL

The framework show of our proposed conspire comprises of property specialist, CSP, mist hubs, information proprietors and users.

4.1 Property authority

The property specialist could be a completely trusted party which is in charge of creating framework parameters as well as mystery key for each client.

4.2 Csp

The CSP may be a semi-trusted party which gives high-capacity and online information capacity benefit. It is additionally capable for confirming the signature some time recently tolerating the overhauled cipher text.

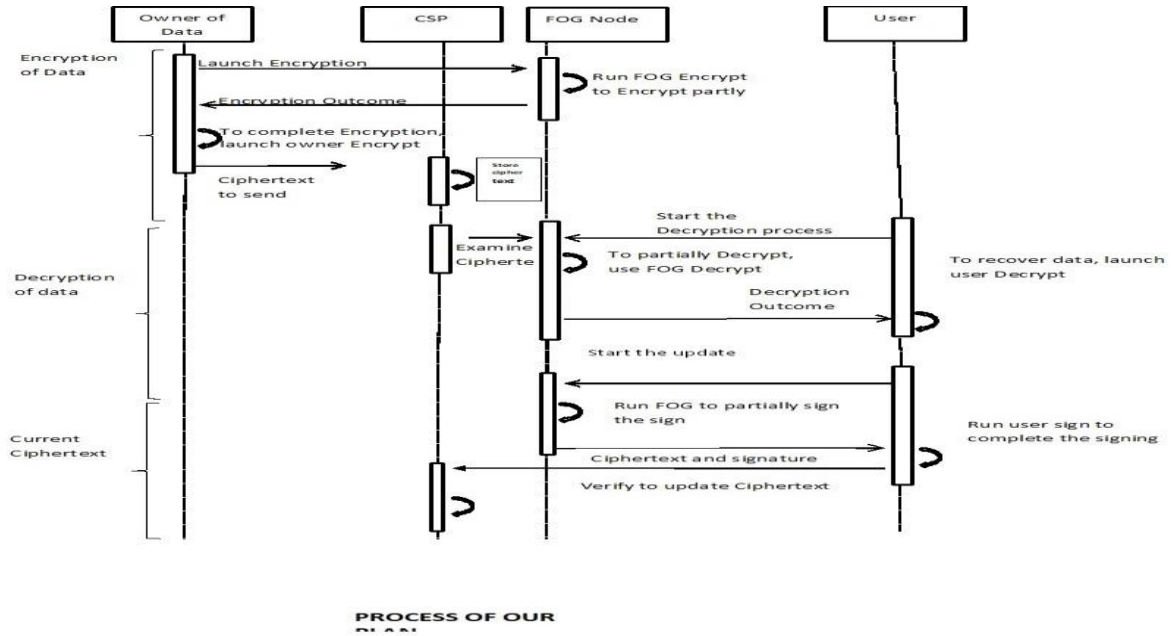
4.3Fog node

The mist hubs, which are introduced at the organize edge and give a run of services, are too semi-trusted parties. They are capable for making a parcel of the figure content, uploading the complete figure content to the CSP, and helping clients in decoding the figure content after it has been downloaded from the CSP. Moreover, they offer assistance conclusion clients sign the ask for a figure content update.

The work stream of our plot is appeared in Fig. 2. At the initialization stage, property specialist employments the Setup calculation to create frameworks parameter. By the KeyGen calculation, quality specialist produces mystery keys for information proprietors and clients. In arrange to attain tall encryption proficiency, the information proprietor to begin with scrambles the collected information with a irregular DK by applying symmetric encryption calculation and characterizes an get to arrangement and an upgrade approach, the mist hub employments the Haze. Scramble calculation to mostly scramble the data with the get to approach, and after that information proprietor employments the Proprietor. Scramble calculation to wrap up the encryption with both the get to arrangement and upgrade approach and stores it to the CSP. When accessing the information, the mist hub to begin with employments the Fog.

The client can at that point utilize the Client. interpret calculation to recover the information after utilizing the TDecrypt strategy to mostly interpret the figure content. The client scrambles the adjusted information utilizing the methods from the encryption step after making changes to the information. The fractional signature provided by the haze hub, which performs the Haze Sign calculation, is utilized by the client to construct the signature some time recently performing the ultimate modification. The modified figure content is at that point acknowledged by the CSP in case the signature is substantial after being confirmed by the Confirm calculation. Eventually, other clients get the upgraded information with the unscrambling calculations. Hence, the clients with IoT gadgets can get to and overhaul private information in haze computing efficiently.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023



PROCESS OF OUR

4.5 Security Model

In our conspire, we accept that cloud servers and mist hubs are genuine but inquisitive, which suggests they execute the tasks and may collude to induce the unauthorized information. Specifically, the security show covers the taking after aspects.

1) Information privacy. The unauthorized clients which are not the expecting receivers defined by information proprietor ought to be anticipated from getting to the information.

2) Fine-grained access control. The information proprietor can custom expressive and adaptable approaches so that the information as it were can be gotten to and overhauled by the clients whose traits fulfill these arrangements.

3) Verification. In case clients seem not fulfill the overhaul approach in cipher writings, it ought to too be prevented from overhauling the cipher writings.

4) Collaboration resistance. Two or more clients cannot combine their mystery and outsourcing keys and get get to to the information they cannot access individually.

5. DATA ENCRYPTION AND DECRYPTION ALGORITHMS

Since the larger part of IoT gadgets are resource-constrained, making decreased computational complexity could be a crucial need for mist computing. To begin with, we offer an viable figure content upgrading method based on CP-ABE and ABS as well as fine-grained information get to control. The figure content can be unscrambled by approved clients whose traits satisfy the get to approach, and the figure content can be reestablished in the event that the overhaul arrangement is fulfilled. The lion's share of the encryption, unscrambling, and signature calculations from conclusion IoT gadgets are outsourced to mist hubs employing a secure outsourcing structure that we offer as our second offering. The development data is recorded below.

5.1 System Setup

The quality specialist runs Setup calculation to choose a bilinear outline e : G0 × G0 → GT , where G0 and GT are two multiplicative bunches with prime arrange p, and g is the generator of G0. At that point the trait specialist arbitrarily chooses h ∈ G0 and α, β ∈ Zp, chooses cryptographic hash capacities H1 : {0, 1} ∗ → Z ∗ p , H2 : {0, 1}∗ → G0, at last yields a framework open key PK = (g, h, g α , g β , h β , e(g, g) αβ) and a ace mystery key MK = (α, β).

5.2 Key Generation

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023

The quality specialist runs KeyGen algorithm to choose a random γ ∈ Zp, which could be a interesting mystery relegated to each client. At that point the quality specialist chooses a arbitrary ε ∈ Zp, and arbitrary rj for each trait j ∈ S, where S is the property set of client, and yields the mystery key and outsourcing key. SK = (D = g (α γ)β) SK0 = (D1 = g γ h ε , D2 = g ε , {D˜ j = g γβH1(j) rj , D˜0 j = g rj }j∈S) (1) The outsourcing key SK0 = (D1, D2,{D˜ j, D˜0 j}j∈S) of client is sent to the haze hubs, and the client as it were stores SK.

5.3 Data Encryption

Before submitting information to the CSP, the information proprietor to begin with chooses a arbitrary DK Zp and employments the symmetric encryption method C = SEDK (M) to scramble the information M with the chosen DK. After that, the information proprietor makes an overhaul approach Tu and an get to approach Ta, and transmits Ta to mist hubs. To carry out the outsourced encryption, the mist hubs utilize the Mist Scramble calculation. The haze hubs select a polynomial px for each hub x within the access policy tree Ta. The determination of the px is done top-down, beginning with the root hub R. Set the degree dx of the polynomial px for each hub x within the tree to be one less than the edge esteem kx of that hub, that's , dx = kx 1.

5.4 Data Decoding

If properties of the client fulfill the get to approach Ta, he can decode CT successfully by running the taking after decoding calculation and get the symmetric key DK. Haze hubs run Fog.Decrypt calculation to get cipher content from the CSP. The mist hubs to begin with run DecryptNode calculation which could be a recursive calculation. The calculation takes a cipher content CT, SK0 , and a hub x from the get to tree Ta as input.

$$\text{DecryptNode}(CT, SK0, x) = e(\tilde{D} z, \tilde{C} x)$$

$$e(\tilde{D}0\, z, \tilde{C}0\, x)$$

$$= e(g\, \gamma\beta H1(z)\, rz, g\, px(0),)$$

$$e(g\, rz, H1(attrx)\, px(0))$$

$$= e(g, g)\, \gamma\beta px(0)$$

5.5 Ciphertext Overhaul

The client at that point adjusts the decoded information as expressed within the information encryption stage, re-encrypts the overhauled information, and signs the figure content upgrade ask with his characteristics. The figure content may as it were be revived by CSP in case the user characteristics in the signature meet the update approach Tu. The client updates the policy with the ask U and sends it to the mist hubs. The outsourced marking is carried out by the haze hubs utilizing the fog.sign strategy. The mist hubs select a polynomial qx for each hub x within the overhaul arrangement tree Tu.

Beginning from the root hub R, the qx is chosen in a top-down way. For each hub x within the tree, set the degree d x of the polynomial qx to be one less than the threshold value k x of that hub, that is d x = k x − 1. Beginning with the root hub R, the calculation chooses a irregular r ∈ Zp and sets qR(0) = r. At that point, it chooses d R other focuses of the polynomial qR haphazardly to characterize it totally. For any other hub x, it sets qx (0) = qparent(x)(index(x)) and chooses d x other focuses arbitrarily to completely define qx . Let Z be the set of leaf hubs in Tu, the haze hubs yield a worldwide key GK.

6. SECURITY EXAMINATION ANALYSIS

If there exists a probabilistic polynomial time (PPT) foe can win our plot with non-negligible advantage, at that point there's a PPT calculation that can recognize a decisional bilinear Diffie-

Hellman (DBDH) tuple from a arbitrary tuple, as sealed. Consequently, our plot is secure to the DBDH suspicion. We analyze the security properties of our plot as follows.

6.1 Confidentiality of Data

The mystery of the information may be guaranteed against clients who do not have a set of qualities that satisfy the get to approach once the information is at first scrambled utilizing the get to arrangement and upgrade arrangement. Indeed whereas the mist hub conducts encryption calculations for the client, it is still incapable to get to the information without the mystery key amid the encryption stage. Since the set of traits cannot satisfy the access approach within the figure content amid the decoding stage, the cloud servers or haze hubs are incapable to recoup the esteem A = e(g, g) t to advance get the required esteem DK since they are ignorant of the D of the client. In this way, as it were clients who have fitting characteristics and follow to the get to rules are able to decode the figure text.

6.2 Fine-Grained Get to Control

The adaptability of Fine-grained get to control empowers for the detail of unmistakable get to benefits for distinctive clients. We utilize CP-ABE to escort the symmetric encryption key in arrange to force this frame of get to confinement. The information proprietor may execute an expressive and adaptable get to arrangement, scramble the symmetric key that's utilized to encrypt the data, and after that outsource the figure content to cloud servers amid the encryption stage of our approach. In particular, the get to approach of scrambled information set up within the get to tree permits modern operations such as AND and OR gates, which can speak to any required property set.

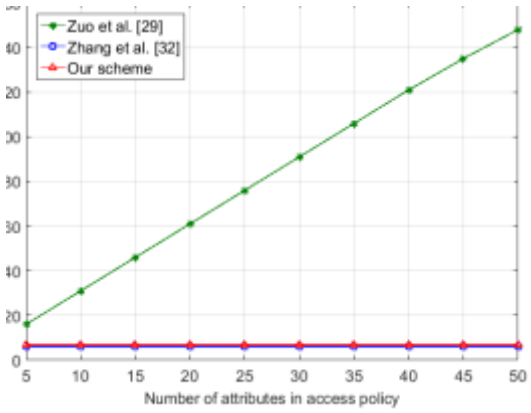
6.3 Authentication

Our plot abuses ABS to attain cipher content upgrade with authentication, indeed foe may attempt to forge a signature with the overhaul arrangement that his traits don't fulfill. Let F be an enemy who makes at most qH1, qH2, qO, qK and qS inquiries to arbitrary prophets H1, H2, outsourcing key era prophet, mystery keys era prophet and marking prophet separately, and produces a effective imitation against our conspire with a non-negligible likelihood ρ.

7.PERFORMANCE ANALYSIS

7.1 Efficiency in Performance

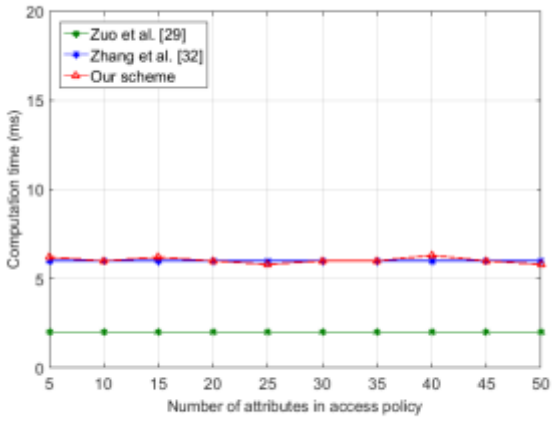
Here we analyze the execution proficiency of our conspire with the a few IoT-based and fog-based information sharing plans based on ABS or ABE, in terms of computational complexity on client when performing encryption, unscrambling and marking. The comparison result is appeared in Table 1. Let TP be the computational taken a toll of a single blending, T0 be the computational fetched of an type operation in G0,TEbe the time for an example operation in GT , NC be the number of traits in a cipher content. We overlook the basic duplication, hash, symmetric encryption and unscrambling operations



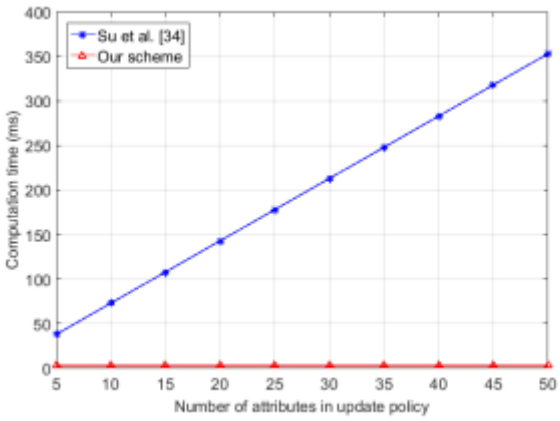
7.2 Investigative Analysis

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023

We conduct recreation tests on a tablet as mist hub and an android phone as IoT gadget. The tablet is with Intel CPU at 2.53 GHz, 4 GB memory and Ubuntu 16.04. The android phone is Samsung G9600V with a quad center processor, 2 GB memory, and Android 6.0.1. The test code employments the pairing-based cryptography library to recreate the plans. We utilize a pairing-friendly type-A 160-bit elliptic bend gather based on the super particular bend y 2 = x 3 x over a 512-bit limited field. The Progressed Encryption Standard (AES) is chosen as the symmetric key encryption scheme.



IRE 4. Comparison of computational overhead for decryption.



The time complexity on clients of cipher content overhaul which basically alludes to marking calculations in both our plot and Su et al. [34] is given in Fig.5. Concerning on the neighborhood computation performed by the endorser, our plot accomplishes much about steady execution compared with the direct expanding productivity of the plot of Su et al. [34] by outsourcing numerous computations to mist hubs. This advantage permits our conspire to be connected for the resource-constrained IoT gadgets to total the marking task.

8.CONCLUSION

In this paper, we propose a secure information get to control plot in mist computing for IoT based on CP-ABE and ABS. The delicate information of clients are to begin with scrambled with both get to approach and overhaul approach, and after that outsourced to cloud servers through mist hubs. Hence, the clients whose properties fulfill the get to arrangement can unscramble the cipher content. In arrange to address the issue of information adjustment, the CSP will check the signature, to guarantee that as it were the clients whose traits fulfill the overhaul approach can reestablish the cipher content. Subsequently, our conspire accomplishes both fine-grained information get to control and secure

cipher content overhaul. By doling out the lion's share of the errands to haze hubs, our approach too offers an outsourced encryption, decoding, and signature development. The comes about of the nitty gritty execution think about and testing appear that our strategy can handle a developing number of characteristics, making it suitable for resource-constrained IoT gadgets in mist computing.

REFERENCES

[1] Q. Huang, Z. Ma, Y. Yang, J. Fu, and X. Niu, ‘‘EABDS: attribute-based secure data sharing with efficient revocation in cloud computing,’’ Chin. J. Electron., vol. 24, no. 4, pp. 862–868, 2015.
[2] Q. Huang, L. Wang, and Y. Yang, ‘‘DECENT: Secure and fine-grained data access control with policy updating for constrained IoT devices,’’ in World Wide Web. May 2017. [Online]. Available: https://doi.org/ 10.1007/s11280-017-0462-0
[3] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext-policy attribute-based encryption,’’ in Proc. IEEE Symp. Secur. Privacy, Berkeley, CA, USA, Mays 2007, pp. 321–334.
[4] S. Ruj, A. Nayak, and I. Stojmenovic, ‘‘Distributed fine-grained access control in wireless sensor networks,’’ in Proc. IEEE Int. Parallel Distrib. Process. Symp., Anchorage, AK, USA, May 2011, pp. 352–362.
[5] S. Hohenberger and B. Waters, ‘‘Online/offline attribute-based encryption,’’ in Proc. 17th Int. Conf. Pract. Theory Public-Key Cryptogr., Buenos Aires, Argentina, 2014, pp. 293–310.
[6] N. Oualha and K. T. Nguyen, ‘‘Lightweight attribute-based encryption for the Internet of Things,’’ in Proc. 25th Int. Conf. Comput. Common. Netw., Waikoloa, HI, USA, Aug. 2016, pp. 1–6.
[7] L. Yang, A. Humayed, and F. Li, ‘‘A multi-cloud based privacy-preserving data publishing scheme for the Internet of Things,’’ in Proc. 32nd Annu. Comput. Secur. Appl. Conf., Los Angeles, CA, USA, 2016, pp. 30–39.
[8] H. K. Maji, M. Prabhakaran, and M. Rosulek, ‘‘Attribute-based signatures,’’ in Proc. 11th Cryptographers’ Track at RSA Conf., Topics Cryptol., San Francisco, CA, USA, 2011, pp. 376–392.
[9] F. Zhao, T. Nishide, and K. Sakurai, ‘‘Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems,’’ in Proc. Inf. Secur. Pract. Exper.-7th Int. Conf., Guangzhou, China, 2011, pp. 83–97.
[10] G. Fortino, A. Rovella, W. Russo, and C. Savaglio, ‘‘On the classification of cyberphysical smart objects in the Internet of Things,’’ in Proc. Int. Workshop Netw. Cooperating Objects Smart Cities, Berlin, Germany, 2014, pp. 3–9.
[11] B. Lynn. The Pairing-Based Cryptography Library, accessed on 2013. [Online]. Available: http://crypto.stanford.edu/pbc/