A Review on Various Secure Data Access Schemes and Techniques in Fog Computing For Internet of Things

Bade Ankamma Rao[1], Bondalapati Bhagyasree[2]
Department of MCA
[1] Assistant Professor, St. Mary's Group Of Institutions, Guntur, Andhra Pradesh, India
[2]PG Students, St. Mary's Group Of Institutions, Guntur, Andhra Pradesh, India

Abstract-*Fog computing Provides extending feature for proper Infrastructure, Storage, Computation and services that bring cloud to the edge of network theory, fortunately or unfortunately cloud-Iot Aches from various issues such as network latency, Volume of data uploaded and the data being accessed, privacy and security. There are many schemes and methods that giving the solutions for the research being carried out in iot security, however the practical issues are still exist and in this paper the various schemes such as Distributed computing, Edge computing, homomorphic encryption, fine grained privacy preservation technique, attribute based encryption and other schemes which relates to security are reviewed and check the nature of cloud-iot based encryption schemes, In the meantime the analogy of secure access for proposed schemes such as confidentiality, availability, privacy and Integrity that securely meet the requirements of security in fog and internet of things.Since fog computing originates from and is a non-trivial extension of cloud computing, it inherits many security and privacy challenges of cloud computing, causing the extensive concerns in the research community. To enable authentic and confidential communications among a group of fog nodes, in this paper, we propose an efficient key exchange protocol based on cipher text-policy attribute-based encryption (CP-ABE) to establish secure communications among the participants. To achieve con mentality, authentication, verifiability, and access control, we combine CP-ABE and digital signature techniques. We analyze the efficient of our protocol in terms of security and performance. We also implement our protocol and compare it with the certificate-based scheme to illustrate its feasibility.*

Keywords-Fog computing, security, ciphertext-policy attribute based encryption (CP-ABE), cloud computing, communications security.

I. INTRODUCTION

Cloud has being model for each and every computing paradigm now a days and it provides a elastic nature of computing resource by name of distributed computing and to extend the property of cloud to nature of substance the review has been moved to fog based computing like hosting and working entirely on edge network ends[1,2]. The fogging means in short of edge source and it has distributed computing properties that handles the small processing and the other small resources at the end of the cloud, Fog has the properties of that inherit from the cloud but remember cloud can't just replace the cloud, however it extends the properties of cloud nature[3,4]. An Internet of things has been modeled to solve the real world problems and at the same time it focus on cloud issues related processing structure [5]. Fog has data of analytics and various access points can be connected through the edge placement of the network. The theme of fog in short to reduce the latency and provide security at the edge of the cloud [6,7]. There are techniques that are used and applied in major function of security and privacy. A technique called Homomorphic encryption scheme which has threshold secure combination of variables without revealing of other set of variables [8]. A scheme of methodology called Fine grained privacy preserving query along with location based service ensure the network latency low as per policy[9,10]. Attribute-based Encryption technique are the two main alternatives of ABE schemes to be proposed in variance [11].

There shall be many problems with multi cloud based structure with the IOT devices in order to reduce the cost of constraints and the computation and provides various techniques to address the same of multi tendencies. Secondly internet of things requires a exponential keys to legitimate access for fog, The paper shall address the various challenges for computing IOT. The Chinese remainder theorem calculates the hash of the function and specify the injected data, the light weight preserving scheme typically also plays a vital role in degree of difference attacks. The Internet of things security is susceptible for many active attacks, first is that the most of the time the network is said to be un-attended so the cause will be passive Secondly most of the network issues has been broadcasted and have issues of eaves dropping so the value of the attack will be more and can be actively masquerade the information and identity [19,20].

The main problem is to authenticate and maintain the confidentiality in the neighboring networks. The Main problem with the internet of things is to generate the massive data within the group so it have glitches to which the information has to be passed and RFID cannot help to make the servers to make authentication[19,20]. Attribute-Based Encryption and fog, an innovative creation of mature based encryption technique by assisting impassive nature of Access policy and to make over the control of the decryption possibility and to be a is first Key Policy Attribute-based Encryption scheme and Cipher text Policy.

In two cases, a point of view user has a set of features that assistance with semi use of private key. The character set is used to label a user's Authorizations. In Key Policy-ABE, user's private key is entrenched with an admittance strategy, while cipher text is encoded by a pre-distinct access procedure in Cipher key-ABE existing a enduring self-controllable admission policy so that User would have the crucial switch of the entree to their individual PH[21].

One of the real world applications that motivates our prob-lem formulation is smart grids. A smart grid system is an electrical grid that intelligently controls, measures, and balances energy. It can automatically change to a differ-ent energy resource depending on the availability and the energy demand, which can help consumers optimize their consumption and lower the cost of the bill. A smart grid sys-tem consists of suppliers, cloud, and grid sensors or devices as shown in Fig. 1. Each smart grid gathers data and sends it back to the cloud via fog to analyze the behaviors of the consumers and the suppliers. Then, the smart grid acts based on the results of the analysis of the collected data. At this point, it is clear that the smart grid system requires real-time process-ing and distributed control. Fog computing can provide an interplay between real-time and batch analytics, but it also introduces new security challenges. In particular, attackers can easily launch many attacks when data is transmitted via a wireless channel and expose the users' information. Specically, the transmitted data between fog nodes and the cloud for processing purposes allow the adversary to launch more sophisticated attacks. Additionally, existing protocols suffer from several drawbacks as mentioned in Section VI-C. Thereby, we need an efcient protocol to establish secure communications between fog nodes and the cloud.

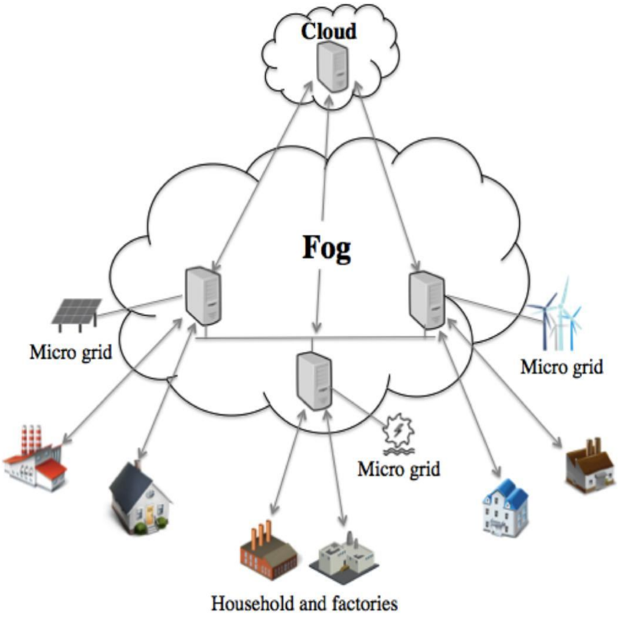


FIGURE 1. An example smart grid based on fog computing.

II. LITERATURE REVIEW

A very large methods have been projected by scholars and researchers in security and confidentiality procedures of fog in Internet of things. In this View, a short analysis of some significant assistance can be done to the existing work can be obtained.

Author name: Hu,et al.[12] :Method Used by the author and brief description:Face Identification and resolution in fog iot framework firstly suffers from the various security and privacy concerns. In order to set a overcome we use session key agreement, Integrity and data encryption schemes are proposed for the scheme of face Identification and resolution.

Author name: Jiang,et al.[13] :Method Used by the author and brief description:Key delegation scheme provides the uniqueness by generating the new set of the private keys for the original subset of attributes

Author name: Huang,et al. [14] :Method Used by the author and brief description:Fine grained Access control of which the data attributes satisfy the particular policy only can decrypt the original set of attributes the Iot device plays the major role in creating new access policy, with the cloud server the attributes satisfy the access policy only can be decrypt the information and stored in the cloud basis. The sensitive information is uploaded will not leak any sensitive information.

Author name: Alrawais,et al.[15]Method Used by the author and brief description:Here the digital signature is verified with the hash of the algorithm and establish a secure network over the fog – cloud over the Internet of things and above to that CP_ABE methods give the accuracy of authentication, confidentiality and access control.

Author name: Huang,et al.[16]Method Used by the author and brief description:Cipher Update along with computation in cloud-fog for IOT was proposed, In this sensitive data is encrypted with the multiple policies and stored in cloud, hence the rule that satisfies only can decrypt.

III. RELATED WORK

The main purpose of this paper is to propose an encrypted key exchange protocol based on CP-ABE to resist several sophisticated attacks in the fog computing network. Hence, in this section, we summarize the most closer works along two lines:

ABE: Several existing researches [7] [11] utilize ABEas a part of their proposed solution to achieve different security objectives. Li et al. [12] proposed a patient-centric framework for data sharing access control to personal health record stored in cloud servers. They used the ABE techniques to achieve a high degree of the user's privacy and a fine-grained data access control for personal health records. Another effort in [13] com-bined KP-ABE with other techniques to simultaneously achieve data confidentiality and scalable data access control in the cloud server. Recently, Hur [14] proposed a novel CP-ABE scheme for data-sharing to enforce an efficient data access control based on the data sharing characteristics.

Fog Computing: The fog computing platform providesa highly scalable solution for IoT devices and applications. Many works discussed the role of fog comput-ing in IoT environment. Alrawaiset al. discussed the security and privacy challenges of fog computing in IoT environments. Fundamentally, they described how to use fog computing to enhance the security and privacy issues in IoT environments. Additionally, Hong et al. [16] ana-lyzed the programming model for large scale and latency sensitive IoT applications utilizing the fog computing platform. They studied the model with a camera network and connected vehicle applications and showed the efficient role of fog computing in IoT. Another work [17] evaluated the suitability of fog computing in the context of IoT environments. The authors developed a mathematical model to evaluate the applicability of fog com-puting and compared it with the traditional cloud com-puting in terms of latency, cost, and power consumption. Their results depicted the efficiency, provisioned QoS, and eco-friendliness of fog computing in IoT technology compared to cloud computing. Recent works have demonstrated the role of fog computing on more specific IoT applications. Al Faruque and Vatanparvar [18] proposed a Software Defined Network (SDN) based on vehicle ad hoc networking supported by fog computing. The proposed architecture solves many issues in vehicle ad hoc networks by increasing the connec-tivity between vehicles, vehicle-to-infrastructure, and vehicle-to-base-station while integrating fog computing to reduce latency and provide resource utility. The work in [19] introduced the fog platform as a novel solu-tion for energy management. They illustrated the energy management as a service over fog computing on two dif-ferent domains of home energy management and micro grid-level energy management. Their results showed that fog computing can improve efficiency, flexibility, inter-operability, and connectivity, and can minimize the cost and time of energy management services. Another effort in [20] focused on health care applications, specifically a pervasive health monitoring application, which requires low latency and low network overhead. The authors employed fog computing to monitor falls or strokes by analyzing the data throughout the network and provide real-time detection. Their experiments showed that the proposed system achieves a low miss rate and low false positive rate.

IV. NETWORK MODEL AND PRELIMINARIES

NETWORK MODEL

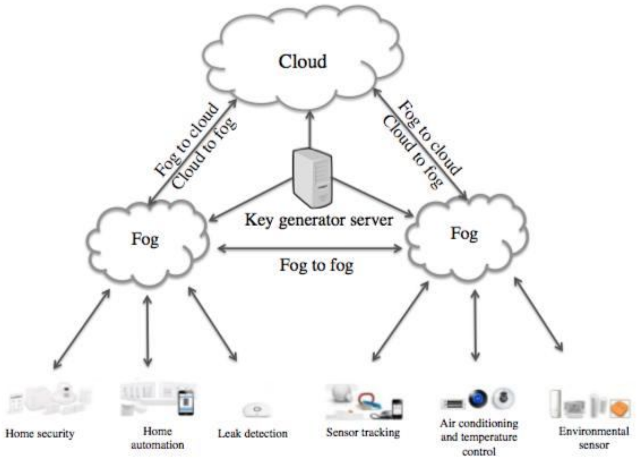


FIGURE 2. Our proposed protocol.

A representative network architecture for fog and cloud com-puting is illustrated in Fig. 2. This network architecture is composed of the following entities: a cloud, a key genera-tor server, fog nodes, and IoT devices. The key generator server is used to generate and distribute the keys among the involved entities. The cloud defines the access structure A and performs the encryption to get ciphertext. We assume that the access structure A is given to all fog nodes. The fog node carries a set of attributes that is defined by an access structure an associated with the cipher text. In particular, we assume that each fog node is associated with S attributes that can be viewed as a meaningful string of arbitrary length. For example, each fog node can have the following set fogiD fmodel_number;manufactured_company;locationg;: : fogn D flocation; model_numberg. Thus, fogi can exe-cute the protocol to establish secure communications with other fog nodes and the cloud, if only its attributes set Sisatisfies A. Thereby, a party of fog nodes whose attributes satisfy the access structure A can compute the shared key.

V. SECURITY GOALS

Our main security goals are to establish secure communications in the fog computing network. Thus, the system should achieve the following security objectives:

Confidentiality: Sensitive data should be only disclosed to legitimate entities. In our system, we utilize CP-ABE to ensure Confidentiality of the transmitted data.

Authentication: The system should prevent an active adversary who does not have the privilege to change or learn information of the transmitted data. Thus, a proper security mechanism should be adopted to ensure the authenticity of the data.

Access Control: To reduce the risk of data exposure by an active adversary, a fine-grained access control should be enforced. The primary goal of our scheme design is to exchange the shared key securely; however, our scheme can be utilized to grant different access rights for each fog node in the same group.

Verifiability: From the entity's signature, the fog node can be convinced that the message is generated by the same entity.

VI. PROPOSED MODEL

In order to achieve the security requirements of the commu-nications between fog nodes and the cloud, we propose an encrypted key exchange protocol based on CP-ABE [1], [22]. More specifically, we design a protocol such that each fog node is associated with a set of attributes, and assign each ciphertext with an expressive access structure that is defined over these attributes. This feature enforces the decryption procedure based on the fog node's attributes. Each cipher text carries an access structure such that the fog can decrypt the cipher text and obtain the shared key only if it possasses the specified attributes in the access structure. In this section, we propose our protocol based on the combination of CP-ABE and digital signature techniques. First, we define the access structure of our protocol. Then, we detail our protocol algorithms.

In our protocol, we utilize an access tree proposed by [1] as an access structure A, which is shown in Fig. 3. Let T be a tree representing an access structure, where each non-leaf node is a threshold gate, and each leaf node describes an attribute. Assume that numx is the number of children of node x, and kxis the threshold value, then 06kx6numx. Each interiornode x is associated with two parameters kx and numx . The threshold value kx outputs 1 if it is an OR gate, and outputs numxif it is an AND gate. For each leaf node x, we definethe threshold value to be kx D 1. To facilitate the access tree structure description, the following functions are defined: parent(x) is the parent of the node x in the tree,att(x) is theattribute of the leaf node x, and index(x) is the function that returns a uniquely assigned number that is associated with node x.

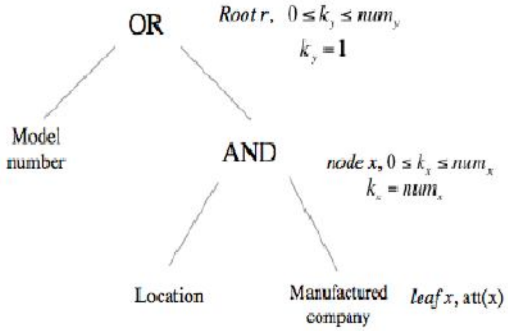
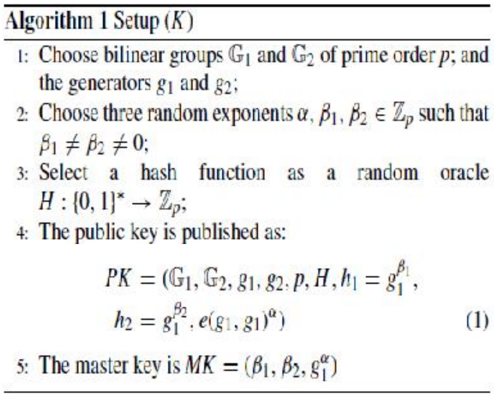


Fig: Access structure

To satisfy the access tree, let T be a tree with a root node R, and let Tx be a subtree rooted at node x. If a set of the attributes satisfiesTx , then Tx ( ) D 1. We compute Tx( ) D 1 recursively as follows:

If x is a non-leaf node, we evaluate Tx â€™( ) based on the children of x; if and only if at least kx of the children return 1, Tx ( ) D 1. If x is a leaf node, then Tx( ) D 1 if and only if att(x) 2 .

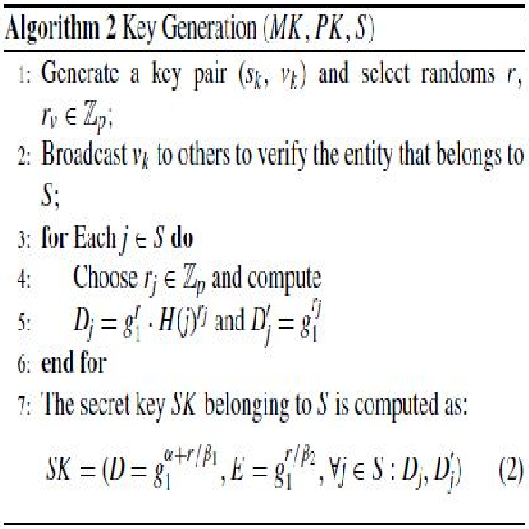
At the beginning of our protocol, each fog node is asso-ciated with an access structure A. The protocol can be exe-cuted with the following algorithms: Setup, Key Generation, Encryption, and Decryption. A private key is issued for each fog node based on the corresponding attribute set S. Then, the cloud runs the encryption algorithm that outputs an encrypted symmetric key. The cloud broadcasts the encrypted key to a group of fog nodes. Upon receiving the encrypted key, each fog node runs the decryption algorithm using its private key to extract the symmetric key. Our protocol consists of four algorithms that are detailed as follows:



```
Algorithm 1 Setup ($K$)
Choose bilinear groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order $p$; and the generators $g_1$ and $g_2$;
Choose three random exponents $\alpha, \beta_1, \beta_2 \in \mathbb{Z}_p$ such that $\beta_1 \neq \beta_2 \neq 0$;
Select a hash function as a random oracle $H : \{0, 1\}^* \to \mathbb{Z}_p$;
The public key is published as:
    $PK = (\mathbb{G}_1, \mathbb{G}_2, g_1, g_2, p, H, h_1 = g_1^{\beta_1}, h_2 = g_1^{\beta_2}, e(g_1, g_1)^{\alpha})$   (1)
The master key is $MK = (\beta_1, \beta_2, g_1^{\alpha})$
```

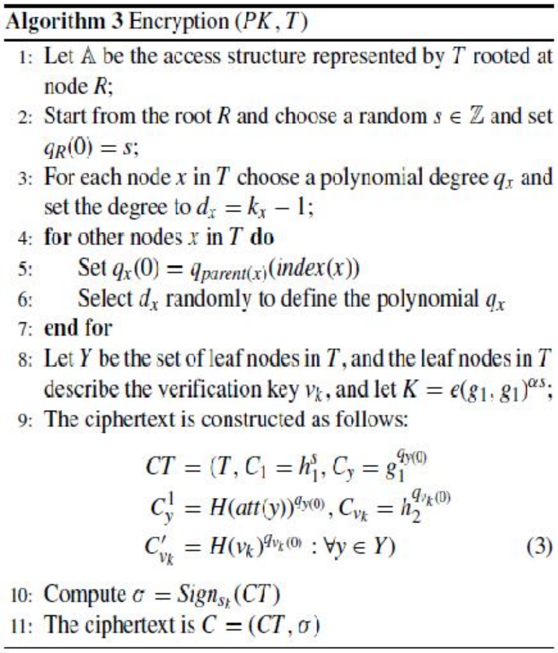
Algorithm 1 describes the system setup and is executed bythe key generator server. It takes the security parameter K as an input, publishes the public parameters PK to all involved entities, and holds the master key MK .

Algorithm 2 is also performed by the key generator serverto generate the secret key SK that belongs to an entity spec-ied by its set of attributes S. It takes the public parameters PK , the master key MK , and the set of attributes S to generatethe secret key SK for the entity possessing S.



```
Algorithm 2 Key Generation ($MK, PK, S$)
Generate a key pair ($s_k$, $v_k$) and select randoms $r$, $r_v \in \mathbb{Z}_p$;
Broadcast $v_k$ to others to verify the entity that belongs to $S$;
for Each $j \in S$ do
    Choose $r_j \in \mathbb{Z}_p$ and compute
    $D_j = g_1^r \cdot H(j)^{r_j}$ and $D'_j = g_1^{r_j}$
end for
The secret key $SK$ belonging to $S$ is computed as:
    $SK = (D = g_1^{\alpha + r/\beta_1}, E = g_1^{r/\beta_2}, \forall j \in S : D_j, D'_j)$   (2)
```

Algorithm 3 provides the details of the encrypted sharedkey K . It is executed by the cloud that takes as inputs the public parameters PK and the access tree structure T . It outputs the ciphertext C that contains the symmetric key.

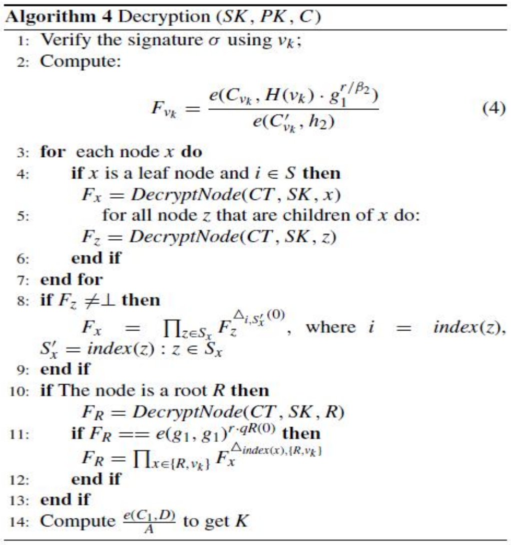


```
Algorithm 3 Encryption ($PK, T$)
Let $\mathbb{A}$ be the access structure represented by $T$ rooted at node $R$;
Start from the root $R$ and choose a random $s \in \mathbb{Z}$ and set $q_R(0) = s$;
For each node $x$ in $T$ choose a polynomial degree $q_x$ and set the degree to $d_x = k_x - 1$;
for other nodes $x$ in $T$ do
    Set $q_x(0) = q_{parent(x)}(index(x))$
    Select $d_x$ randomly to define the polynomial $q_x$
end for
Let $Y$ be the set of leaf nodes in $T$, and the leaf nodes in $T$ describe the verification key $v_k$, and let $K = e(g_1, g_1)^{\alpha s}$;
The ciphertext is constructed as follows:
    $CT = (T, C_1 = h_1^s, C_y = g_1^{q_{y(0)}}$
    $C_y^1 = H(att(y))^{q_{y(0)}}, C_{v_k} = h_2^{q_{v_k}(0)}$
    $C'_{v_k} = H(v_k)^{q_{v_k}(0)} : \forall y \in Y)$   (3)
Compute $\sigma = Sign_{s_k}(CT)$
The ciphertext is $C = (CT, \sigma)$
```

Algorithm 4 describes the decryption procedure to obtain a shared symmetric key. This algorithm is executed by each fog node, which takes as inputs the public parameters PK , the secret key SK , and the ciphertext C. Then, it outputs either the symmetric key K or ?. Note, the Lagrange's coefcient 4i;S for i 2 Zp and a set of elements in Zp is de nedas 4i;S D Q xi jj . Note that Algorithm 4 employs arecursive function DecryptNode(), which was detailed in [1].

VII. ANALYSIS OF THE PROPOSED PROTOCOL

In this section, we rst show the feasibility and correctness of our protocol. Then we analyze the security properties of the proposed protocol by examining how it can resist several major attacks.



```
Algorithm 4 Decryption ($SK, PK, C$)
Verify the signature $\sigma$ using $v_k$;
Compute:
    $F_{v_k} = \frac{e(C_{v_k}, H(v_k) \cdot g_1^{r/\beta_2})}{e(C'_{v_k}, h_2)}$   (4)
for each node $x$ do
    if $x$ is a leaf node and $i \in S$ then
        $F_x = DecryptNode(CT, SK, x)$
            for all node $z$ that are children of $x$ do:
        $F_z = DecryptNode(CT, SK, z)$
    end if
end for
if $F_z \neq \perp$ then
        $F_x = \prod_{z \in S_x} F_z^{\triangle_{i, S'_x}(0)}$, where $i = index(z)$,
    $S'_x = index(z) : z \in S_x$
end if
if The node is a root $R$ then
        $F_R = DecryptNode(CT, SK, R)$
    if $F_R == e(g_1, g_1)^{r \cdot qR(0)}$ then
        $F_R = \prod_{x \in \{R, v_k\}} F_x^{\triangle_{index(x), \{R, v_k\}}}$
    end if
end if
Compute $\frac{e(C_1, D)}{A}$ to get $K$
```

VIII. THE CORRECTNESS OF THE PROPOSED PROTOCOL

In this subsection, we illustrate that our protocol is correct and feasible. The fog node must rst verify the signature on C using vk to correctly decrypt the ciphertext. The veri cation is processed as follow:

$$\begin{aligned} F_{v_k} &= \frac{e(C_{v_k}, H(v_k) \cdot g_1^{r/\beta_2})}{e(C'_{v_k}, h_2)} \\ &= \frac{e(C_{v_k}, g_1^{r/\beta_2}) \cdot e(C_{v_k}, H(v_k))}{e(C'_{v_k}, h_2)} \\ &= \frac{e(h_2^{q_{vk}(0)}, g_1^{r/\beta_2}) \cdot e(e(h_2^{q_{vk}(0)}, H(v_k))}{e(H(v_k)^{q_{vk}(0)}, h_2)} \\ &= e(g_1^{\beta_2 \cdot q_{vk}(0)}, g_1^{r/\beta_2}) \\ &= e(g_1, g_1)^{r q_{vk}(0)} \qquad (5) \end{aligned}$$

Then, a recursive function DecryptNode(CT ; SK ; R) D e(g1; g1)r qR(0) D e(g1; g1)rs is executed on the root R of the subtree T . Let A D e(g1; g1)rs, the decryption procedure to obtain the symmetric key is calculated as follow:

$$\begin{aligned} K' &= \frac{e(C_1, D)}{A} = \frac{e(h_1^s, g_1^{\alpha + r/\beta_1})}{e(g_1, g_1)^{rs}} \\ &= \frac{e(g_1, g_1)^{s(\alpha+r)}}{e(g_1, g_1)^{rs}} \\ &= e(g_1, g_1)^{\alpha s} = K \qquad (6) \end{aligned}$$

SECURITY ANALYSIS

In this subsection, we analyze the security strength of our pro-posed protocol from the aspects of collusion attack resistance, message authentication, and unforgeability.

1) COLLUSION ATTACK RESISTANCE

In the proposed scheme, we employ CP-ABE to guarantee the security of the shared key (session key). CP-ABE provides an access structure for each encrypted data, and requires only a subset of the attributes for decryption. Since the secret key involves a unique random number for each attribute in the access policy, CP-ABE can defend against collusion attacks. Thus illegal users can not obtain the exchanged shared key via collusion activities.

2) MESSAGE AUTHENTICATION

Assume that the cloud wants to send the symmetric keyto the fog nodes, which has the common attributes, the cloud encrypts K with Algorithm 3, then it broadcasts the encrypted message. When the fog nodes obtain theencrypted message, they need their private keys SK D (D D g1 Cr= 1 ; E D gr1= 2 ; 8j 2 S V Dj; D0j), which are computed byAlgorithm 2. Meanwhile, the fog nodes obtain the cloud's veri cation key vk . Then, the fog nodes verify the signa-ture via Algorithm 4. If passed, the fog nodes decrypt the encrypted message to obtain the symmetric key K ; otherwise, it is discarded.

3) UNFORGEABILITY

An adversary who wants to create a valid signature of a legal user must possess the user's private key. However, an adver-sary cannot infer the private key SK . On the other hand, it is impossible for the adversary to create a new, valid ciphertext and signature from another user's ciphertext and signature. If the adversary modies the ciphertext of the shared key, the receiver can verify that the ciphertext is illegal using Algorithm 4. If the adversary colludes with other users to forge the ciphertext and signature, it cannot succeed because CP-ABE can defend collusion attacks. Thus we claim that our proposed scheme is unforgeable under chosen message attacks.

IX. CONCLUSION

In this paper, we style Associate in Nursing encrypted key exchange protocol to ascertain secure communications among a bunch of fog nodes and the cloud. In our protocol, we utilize the digital signature and CP-ABE ways to attain the first security goals: confidentiality, authentication, verifiability, and access management. we analyze the protection of our protocol and show its correctness and practicability. we have a tendency to conjointly offer an implementation of our theme. we more compare the projected theme with the certificate-based theme and illustrate its potency. In our future analysis, we will specialize in the subsequent directions. First, we will style a secure protocol with less computation overhead to create it appropriate for IoT communications. Second, we are going to style an economical access structure for fog computing and IoT devices.

REFERENCES

[1] R. Ostrovsky, A. Sahai, and B. Waters, ``Attribute-based encryption with non-monotonic access structures,'' in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 195 203.

[2] A. Lewko and B. Waters, ``Unbounded HIBE and attribute-based encryp-tion,'' in Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn., 2011,547 567.

[3] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, ``Fully secure functional encryption: Attribute-based encryption and (hierarchi-cal) inner product

encryption,'' in Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn., 2010, pp. 62 91.

[4] T. Okamoto and K. Takashima, ``Fully secure functional encryption with general relations from the decisional linear assumption,'' in Proc. Annu. Cryptol. Conf., 2010, pp. 191 208.

[5] L. Cheung and C. Newport, ``Provably secure ciphertext policy ABE,'' in Proc. 14th ACM Conf. Comput. Commun. Security, 2007, pp. 456 465.

[6] G. Wang, Q. Liu, and J. Wu, ``Hierarchical attribute-based encryption for ne-grained access control in cloud storage services,'' in Proc. 17th ACM Conf. Comput. Commun. Secur., 2010, pp. 735 737.

[7] Z. Wan, J. Liu, and R. H. Deng, ``HASBE: A hierarchical attribute-based solution for exible and scalable access control in cloud computing,'' IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743 754, Apr. 2012.

[8] D. Huang, Z. Zhou, L. Xu, T. Xing, and Y. Zhong, ``Secure data processing framework for mobile cloud computing,'' in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), Apr. 2011, pp. 614 618.J.-M. Do, Y.-J. Song, and N. Park, ``Attribute based proxy re-encryption for data con dentiality in cloud computing environments,'' in Proc. 1st ACIS/JNU Int. Conf. Comput., Netw., Syst. Ind. Eng. (CNSI), 2011,248 251.

[9] L. Xu, X. Wu, and X. Zhang, ``Cl-PRE: A certicateless proxy re-encryption scheme for secure data sharing with public cloud,'' in Proc. 7th ACM Symp. Inf., Comput. Commun. Secur., 2012, pp. 87 88.

[10] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, ``Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,'' IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1,131 143, Jan. 2013.

[11] S. Yu, C. Wang, K. Ren, and W. Lou, ``Achieving secure, scalable, and ne-grained data access control in cloud computing,'' in Proc. IEEE INFOCOM, Mar. 2010, pp. 1 9.

[12] J. Hur, ``Improving security and efciency in attribute-based data sharing,'' IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271 2282, Oct. 2013.

[13] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, ``Fog computing for the Internet of Things: Security and privacy issues,'' IEEE Internet Comput., vol. 21, no. 2, pp. 34 42, Mar. 2017.

[14] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwalder, and B. Koldehofe, ``Mobile fog: A programming model for large-scale applications on the Internet of Things,'' in Proc. 2nd ACM SIGCOMM Workshop Mobile Cloud Comput., 2013, pp. 15 20.

[15] S. Sarkar, S. Chatterjee, and S. Misra, ``Assessment of the suitability of fog computing in the context of Internet of Things,'' IEEE Trans. Cloud Comput., to be published, doi: 10.1109/TCC.2015.2485206.

[16] N. B. Truong, G. M. Lee, and Y. Ghamri-Doudane, ``Software de ned networking-based vehicular Adhoc network with fog computing,'' in Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM), May 2015,1202 1207.

[17] M. Al Faruque and K. Vatanparvar, ``Energy management-as-a-service over fog computing platform,'' IEEE Internet Things J., vol. 3, no. 2,161 169, Apr. 2012.

[18] Y. Cao, S. Chen, P. Hou, and D. Brown, ``Fast: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation,'' in Proc. IEEE Int. Conf. Netw., Archit. Storage (NAS), Aug. 2015, pp. 2 11.

[19] A. Beimel, ``Secure schemes for secret sharing and key distribution,'' Ph.D. dissertation, Faculty Comput. Sci., Tech.-Israel Inst. Technol., Haifa, Israel, 1996.

[20] M. C. Gorantla, C. Boyd, and J. M. G. Nieto, ``Attribute-based authen-ticated key exchange,'' in Proc. Austral. Conf. Inf. Secur. Privacy, 2010, 300 317.