IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 24, 2018, accepted August 10, 2018, date of publication August 14, 2018, date of current version September 7, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2865539

Reputation-Aware Trust and Privacy-Preservation for Mobile Cloud Computing

WAQAS AHMAD[1], (Student Member, IEEE), SHENGLING WANG[1], (Member, IEEE), ATA ULLAH[2,3], (Member, IEEE), SHEHARYAR[1], AND ZAHID MAHMOOD[3]

[1]College of Information Science and Technology, Beijing Normal University, Beijing 100875, China
[2]Department of Computer Science, National University of Modern Languages, Islamabad 44000, Pakistan
[3]School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China

Corresponding author: Shengling Wang (wangshengling@bnu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61772080 and Grant 61472044.

ABSTRACT Mobile Cloud Computing (MCC) is getting growing interest due to its wide applicability in variety of social, industrial, and commercial mobile applications. Mobile and smart devices can share complex computational operations with Cloud Service Providers (CSPs). It also provides storage, access polices enforcement, and security operations. In many cases, CSP requires services from crowd contributors *CC*s for data collection, sharing, and mobile application support. It requires trust management for *CC*s to guard against malicious *CC*s and ensure security and privacy of data. However, end users or data requesters also demand reliable security solutions for sharing their data or accessing data from unknown *CC*s. To ensure strong security, mobile devices are not computationally feasible to perform complex cryptographic operations for desired privacy. To resolve these issues, we propose Reputation-aware Trust and Privacy Preservation scheme for MCC. In first phase, we deal with the trust management by utilizing reputation aware selection of *CC*s and leverage cloud services where CSP maintains trust score for *CC*s and data requesters. In second phase, we manage privacy preservation by using our proposed Anonymous Secure-shell Ciphertext-policy Attribute Based Encryption (AS-CABE). We have also proposed a hybrid policy tree mechanism for dynamic attribute selection used for security solutions and key management. Next, an anonymous secure shell is maintained between the *CC*s and the crowd servers to ensure registration after approval from trusted authority. In the similar vein, we propose outsourced encryption and decryption mechanism for mobiles that further utilize encryption and decryption service providers for complex operations. To the best of our knowledge, we are the first one to deal with the trust issues of data requester and privacy concerns of *CC*s and users both at the same time. After that, we have presented the security analysis to analyze AS-CABE against security attacks. Finally, the results are presented that ensure the supremacy of our proposed scheme as compared to counterparts in terms of reputation score, storage, computation, trust, resilience, encryption, and decryption time.

INDEX TERMS Attribute based encryption (ABE), cloud service provider (CSP), mobile cloud computing (MCC), privacy preservation, trust management.

I. INTRODUCTION

Mobile Cloud Computing (MCC) provides extensive support for processing and storage to resource constrained mobile devices. Mobile with on board sensors can monitor phenomenon. Like body sensors can offload reports to cloud for constant and secure monitoring by doctors at hospitals or anywhere else. It can save preventable loss of precious human lives by taking instant precautionary measures without rushing to hospital. MCC architecture consists of cell phones, internet and cloud which makes it a special case of Cloud Computing. It has enhanced the capabilities of mobile devices to perform complex operations [1]. Though utilization of outsources is a solution to some problems but it creates other issues too. Privacy of sensitive information is one of the most important concern of today's world. Trust on the correctness of reported data to mobile devices is doubtful, as third party vendors who provide services at cloud cannot be fully trusted. In the architecture of MCC, work is done in such fashion that data is stored and processing takes place on external sources rather than on the mobile devices. Architecture of MCC in presented in Figure 1 [2].

Trust and privacy are compulsory for desirable properties in ensuring secure data exchange over cloud. Cryptographic operations are mandatory to secure data in transit and to

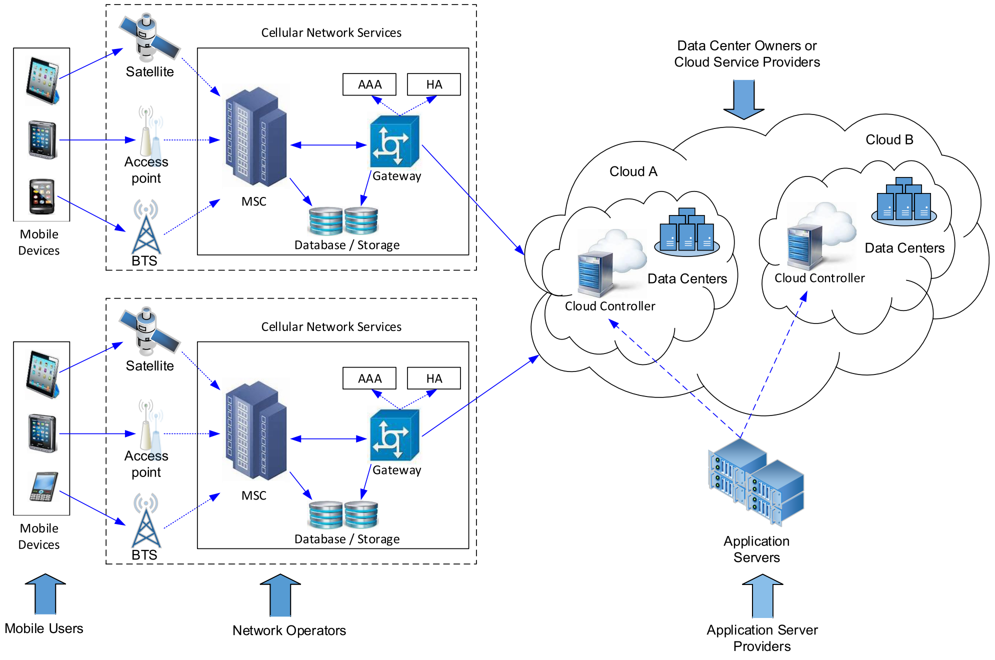


FIGURE 1. General architecture for Mobile Cloud Computing.

avoid misuse of stored data at cloud. Security solutions guard against a number of active and passive attacks including: Man in the middle attack, identity theft attack, ip spoofing and packet sniffing. Proliferation of mobile devices with high precision of sensing capabilities including image, videos, temperature, acceleration, humidity measurements *etc.* are much more capable than ever before. These capabilities bring them to generate sensing data to be processed at cloud in response to fulfill the demand of data requester (*DR*). Query of *DR* in MCC can end up with privacy exposure of different attributes like location, identity, interests and habits. Same is the case with mobile crowd contributors (*CC*), which can be life threating in some cases. Data sanitization is compulsory to prevent privacy disclosure [3]. In sensing domain trust on accuracy, authenticity and consistency of reports is desirable by *DR*s. Moreover non-repudiation, message freshness and integrity protection are necessary measures to ensure secure communication. Data transmission and storage at cloud is in encrypted form to keep it secure even from CSPs. Application servers ensure connectivity and secure retrieval of stored information to/from data centers. Access polices are implied to ensure authorized access.

Schemes for trust and reputation management [4], [5] ensure trustworthiness for Cloud Computing and MCC. Attribute based encryption (ABE) scheme [5] is proposed to give sense of trust and security in MCC. As the mobile devices are resource constraint, services from trusted third party can be utilized to ensure trust and security. Installation and updation of reputation system would require well managed and efficient mechanism at CSPs, which may also require rich storage and computation power. Though CSPs are assumed to have enough storage and computation power but it can be challenging and expensive at large scale. Survey on trust and reputation based approaches has been presented in [6]. Use of complex cryptographic operations could be costly for *CC*s/*DR*s to keep sensitive information private. Framework in [7] is related to our proposed work in a sense as we are considering the sensing domain within MCC.

Reputation aware trust management schemes are also available from microeconomics ranging from simple aggregation of feedbacks to more complex ones based on mathematics and statistical tools. Furthermore these are categorized into centralized and distributed approaches [6]. Maintaining reputation can be a complex task for central authorities, so there is need of an efficient and trustable mechanism at CSP. In our proposed scenario, most of the time *DR* does not upload data for computations, instead put up queries only, for which data may need to be collected from *CC*s. Our work is unique as it includes mobile crowd sensing (MCS) in the perspective of MCC. Trust on sensing reports is so much important that the scheme on the idea of cross validation is proposed in [8]. Limitation of this approach is that it may require extra payments for the process of validations. So these kind of schemes can be costly to be implemented in real world, where feasible budget must be ensured [9]. In this work, we also proposed a reputation based trust in sensing domain with MCC.

One of the problem in designing a good reputation management schemes is that decision on recruitment of *CC*s is non-revertible as in an online sensing scenario. Moreover observations need to be maintained at the same time to take well educated decisions. An exemplary scenario of Indian

Ocean tsunami is presented in [1], where sensing is exploited with the blend of MCC. In our application scenario, *CC*s can also perform sensing tasks with a compulsion that once a *CC* is rejected, cannot be recruited again for that particular task. So selection of *CC*s is tricky as instant action is required. To get good quality of tasks, reputation is likely to maintain which may require large storage at CSP. *CC*s are considered to be rational so they expect good incentives for sensing services but right now it is not the concern of this paper. Another issue is that selection based on reputation may require traversing of records. In this process, privacy of sensitive information is the concern of both end mobile devices. By the end users we mean, anyone who is making contribution and the other who is getting the services. As the end devices are assumed to be the mobile devices with known resource constraints so cannot uphold required actions for privacy. On the other hand if *DR*'s trust lacked, then he may not get services from that particular CSP. So it is in the benefit of CSP to maintain good check and balance to maintain trust. Without an efficient reputation aware recruitment, probability of false reporting is likely. *CC* would also be reluctant to participate in data collection process due to risk of privacy leakage.

To deal with this situation, we have divided our proposed Reputation-aware Trust and Privacy Preservation (*RTPP*) scheme into two parts: part one deals with lack of trust and the second part with privacy preservation of mobile devices in MCC. *RTPP* is proposed for sensing domain in MCC by effectively utilizing crowdsourcing and outsourcing. As strict reputation aware selection and updation system is maintained for *CC*, proposed approach is expected to ensure trust of *DR*s in part one. To establish the level of confidence of *DR* on *CC*'s sensing reports, we have adopted and enhanced ''Beta Reputation'' system from [10] to be implemented at CSP. Storage overhead of CSP is reduced by the concept of ageing factor, where passage of time affects in the reduction of effective history of *CC*s. Selection of *CC*s is dependent on the weight factor, where lower values ultimately can result in de-registration. It can also reduce time complexity of history traversal. We have presented a scheme that can deal with the issues of *CC* and *DR*, where *CC*s can enjoy privacy and *DR*s are ensured for authenticity of information. It is done by keeping an eye on limited resources of mobile devices.

Privacy is maintained in second part by offering Anonymous Secure-shell Ciphertext-policy based Attribute Based Encryption (AS-CABE) scheme. *DR*s are ensured for authenticity of information by considering limited resources of mobile devices. *AS*s are installed near the end devices to provide anonymous communication. Anonymous secure shell is established between end mobile devices and *AS*s. To the best of our knowledge, we are first to integrate reputation aware trusted sensing with privacy preservation in MCC. Proposed system is validated using a testbed with web services at Amazon cloud and a mobile application for android phones. Results have proven that our proposed approach can provide trusted reporting. Lack of resources at mobile devices is dealt by outsourcing the complex computational and storage tasks to CSPs (Encryption/Decryption Service Providers and Cloud Storage Center). AS-CABE kept only critical part of computations at mobile devices, so it is computationally less complex. *AS*s can also play role for non-repudiation, which is a situation that may occur when *CC* at first accepts published tasks and later on refuse to perform.

Contributions in this work are summarized as:

1) Trust of *DR*s on *CC*s is ensured by implying reputation system at CSP. This reputation system in maintained to make well-aware recruitment of *CC*s in future for quality reporting.
2) To provide privacy in MCC, we proposed to use CP-ABE based complex scheme, which can be a big obstacle for mobile devices with limited resources. To handle this, we proposed to use services from outside entities. Installment of *AS*s would also shift some of the workload of enforcing access policies from end devices. Non-critical part of computations would be shifted to CSPs and critical but minimal calculations are kept at end nodes. Outsourced services can be verified by double hash functions.

Rest of the paper is organized as follows. Section 2 presents preliminaries used in this work. Section 3 discusses related work on reputation aware trust and the privacy preservation based schemes in the perspective of MCC. In Section 4, we have presented system model. In section 5, working of Reputation aware Trust and Privacy Preservation (*RTPP*) scheme is presented. The proposed construction and its security analysis are explored in Section 6. We discussed the results and analysis of the proposed approach in Section 7. Conclusion and Future work are presented in Section 8.

II. PRELIMINARIES

In this section, we have presented some of the important preliminaries which are useful for better understanding of this research work. This section explores the overview of bilinear maps and its applicability in the finite composite order groups, where we have also explored the matrix multiplication scenario to explore the expressions for bilinear maps. If V, W, X are vectors then a function $B : V * W \rightarrow X$ is represented as a bilinear map. The matrix multiplication can be considered as a bilinear map represented with a function $M_1(v, w) * M_2(w, x) \rightarrow M_3(v, x)$. A matrix M can be represented as $(v, w) \mapsto v'Mw$, then the associates of the matrix rises to following expressions as illustrated in Table 1. It utilizes the concept of algebraic dual space where each vector has a dual space containing the co-vector like row and column vectors in matrix multiplication. The product matrix M_3 can be expressed as $M_{3_{ij}} = M_{1_{i_1}} M_{2_{1_j}} + \ldots + M_{1_{iW}} M_{2_{W_j}} = \sum_{p=1}^{W} M_{1_{ip}} M_{2_{p_j}}$, where $M_{1_{i_1}}$ represents the column 1^s i^{th} row of matrix M_1 and $M_{2_{1_j}}$ represents the row 1 in j^{th} column of matrix M_2.

We have explored the set of finite composite order groups like G_v and G_w that utilize bilinear map $B : G_v \times G_v \rightarrow G_w$ or $B : {G_v}^2 \rightarrow G_w$ [11].

TABLE 1. Matrix associates using algebraic dual space.

$V \times V \xrightarrow{M} \mathbb{R}$ $(v,w) \mapsto v^{'}Mw$ $M_{ij} = M(b_i, b_j)$ $M \in V^* \otimes V^*$ $M = M_{st}\beta^s \otimes \beta^t$	$V \times V^* \xrightarrow{M} \mathbb{R}$ $(v,f) \mapsto v^{'}Mf^{'}$ $M_i{}^j = M(b_i, \beta^j)$ $M \in V^* \otimes V$ $M = M_s{}^t\beta^s \otimes b_t$ $M_s{}^t = M_{su}g^{ut}$ MG^{-1}
$V^* \times V \xrightarrow{M} \mathbb{R}$ $(f,w) \mapsto fMw$ $M^i{}_j = M(\beta^i, b^j)$ $M \in V \otimes V^*$ $M = M^s{}_t b_s \otimes \beta^t$ $M^s{}_t = g^{su}M_{ut}$ $G^{-1}M$	$V^* \times V^* \xrightarrow{M} \mathbb{R}$ $(f,g) \mapsto fMg^{'}$ $M^{ij} = M(\beta^i, \beta^j)$ $M \in V \otimes V$ $M = M^{st}b_s \otimes b_t$ $M^{st} = g^{su}M_{uv}g^{vt}$ $G^{-1}MG^{-1}$

Following properties are explored for bilinear maps and finite composite order groups:

1) *Bilinear*: By considering all $m, n \in G_v$ and $a, b \in Z_p$, $B(m^a, n^b) = B(m, n)^{ab}$, where Z_p represents a group of large prime numbers with an order p.
2) *Non-degeneracy*: There exist $m, n \in G_v$, where $B(m, n) \neq 1$.
3) *Computable*: The operations in groups G_V and G_W and map B are computable in polynomial interval of time.

III. RELATED WORK

We have explored approaches from literature regarding reputation aware trust management along with privacy preservation in MCC. Zhu *et al.* [7] presented the integration of Wireless Sensor Networks (WSN) with MCC . We focused on the sensing domain with the perspective of MCC, where CSP by itself may need to get services from outsources like *CC*s. To be more particular, we considered *CC*s as the owners of resource constrained (battery, limited bandwidth and computation power) mobile devices. When services from outsources are bought, naturally trust must lack especially when CSPs by themselves get services from other CSPs or from *CC*s as in our case. Typically trust on sensing reports may also lack due to heterogeneous sensing devices, personal experiences. On the other hand, we cannot avoid the intentional malicious behavior. To attain trust, we suggest to use reputation aware recruitment of *CC*s.

The proposed implementation is in MCC, entities are: CSPs, *DO/CC* (Data Owner/Crowd Contributor) and *DR*. In case of *DO*, who is assumed to have stored data at cloud, authorised access should be granted to *DR* by CSP. *CC* is a crowd contributor for data collection process conducted by the CSP to respond the request of *DR*. Due to resource constraints *DR* may request some computations to be done at CSP or to store data at data center.

DR may have various concerns like: secrecy of requested task details, verification of decryption accuracy and integrity of message, matching replies from CSP and truthful reporting in case of *CC*'s participation in data collection process. On the other side *DO/CC* are concerned about privacy when making contribution. In next two sub-sections, we have described trust in participatory sensing and privacy preservation in MCC and tried to relate them with our presented scenario.

A. TRUST IN PARTICIPATORY SENSING

Scheme [12] presented work on trust and reputation management for cloud computing, naturally trust is not of associative neither distributed nor transitive property. In the perspective of resources, reliability can be defined as consistent availability of hardware and software services. Reliability of any resource R = $\{R1, R2, R3 \ldots\}$ presents the number of successfully completed jobs, as given in (1).

$$RE_{R_K} = W_G \times \frac{C_{Kg}}{A_{Kg}} + W_l \times \frac{C_{Kl}}{A_{Kl}} \tag{1}$$

Where C_{Kg} and C_{Kl} are representing the completed jobs, globally and locally by the resource R_k. W_G, W_l are the weightage of global and local task performed by R_k. Where $K = \{1, 2, 3 \ldots m\}$ is the set of jobs and A_{Kg}, A_{Kl} are the total number of those jobs that are accepted by the resource R_k globally and locally. According to [12] important components in building trust for cloud environment are: availability of resource, reliability, integrity, identity, capability and behavior. In our proposed approach, we are concerned about reliability which is the effect of reputation and ultimately leads to trust.

Trust is calculated based on different parameters AV_{Rk}, RE_{RK}, DI_{Rs}, ID_{RK} and CA_{Rk}. Details on some of the equations related to our work are presented here, for further in-depth study we refer to Equation (1) to (5) in [12]. $W_{AV} + W_{RE} + W_{DI} + W_{ID} + W_{CA} = 1$ are the trust values of prior mentioned components. Then trust value of resource R_k will be T_{Rk}.

$$T_{R_K} = W_{AV} \times AV_{R_K} + W_{RE} \times RE_{R_K} + W_{DI} \times DI_{R_K} + W_{ID} \times ID_{R_K} \tag{2}$$

Finally reputation in their proposed model is calculated as: $W1 + W2 + W3 + W4 + W5 = 1$. These are weight factors. N_{Kg} is representing the total tasks assigned to a resource for global period T, g represent globally, A_{Kg} are the accepted tasks by the resource (any device at cloud), C_{Kg} is number of task that have been successfully performed, D_{Kg} represent integrity of provided data, ID_{Rk} is identity, CA_{Rk} is ability of resource of Rk and RE_{Rk} is the reliability of resource R_k in (3).

$$RE_{R_K} = W1\frac{A_{Kg}}{N_{Kg}} + W2 \times \frac{C_{Kg}}{A_{Kg}} + W3 \times \frac{D_{Kg}}{C_{Kg}} + W4 \times ID_{R_K} + W5 \times CA_{R_K} \tag{3}$$

Survey on IoT based trust management schemes is conducted in [13]. Trust composition in terms of quality of service, social trust ands its propagation in terms of distributed and centralized have been discussed. In threat model various attacks are also discussed. Trust is updated in two ways, event and time driven. In event based approaches updation of reputation is performed just after the task completion and in the former one it took place after some specific time interval. Authors also raised some very interesting challenges with respect to trust like: its composition, propagation, updation, aggregation and formation.

False reporting and data generation by the compromised senor nodes in WSN is handled by general reputation concept in [14]. Functional reputation is exploited to detect malicious behavior of compromised nodes. Their proposed methodology can lead to secure data gathering and transmission. Trust based on reputation remained a hot research topic in the paradigms like IoT: [13], WSN [14], cloud computing [12], mobile cloud computing [5] and mobile crowd sensing [15]. In [16] several approaches related to trust evaluation in cloud based services are presented. Hybrid approach based on reputation and compliance is presented to calculate the trust on CSPs [17]. Collective feedback is used to evaluate the trust level. Reputation based trust for cloudlets is discussed in [18]. Taxonomies based on different perspectives for MCC are presented in [1], [19], and [20]. These approaches also considered trust and security issues which are inherited in MCC from cloud computing. A trust management scheme for femtocell in MCC is presented in [21].

Different from the approaches in literature, we considered trust in participatory sensing which is more related to MCS (Mobile Crowdsensing). In contrast to these approaches, we have proposed reputation aware trust from microeconomics to be applied in MCC by doing necessary enhancement. This scheme would assist in reputation calculation for recruitment of *CC*s at CSP, where it can be the symbol of trustworthiness. Situation may become more critical when multiple CPSs get services from each other to fulfill requests [22]. To quantify the user reputation in MCS, an approach is presented in [15]. Approaches based on the analysis of data for authorised access from internal nodes and role based access on reputation aware fine grained access are proposed in [4] and [5].

In general perspective trust and reputation are same. Reputation can lead to trust between entities like in our presented scenario good reputation of *CC*s can be a reason of their recruitment by CSP. Trust based systems can be in the form of a numerical value, whereas the systems for reputation can be categorized based on community or on the acceptance at public level [6]. Two fundamental aspects need to be considered for reputation based systems. 1) Engine which calculates the reputation/rating in the perspective of feedback. 2) Propagation, which is a mechanism that can provide reputation on demand.

In [23] sensory reports generated by sensors are considered, where sensors are the source of data collection. We presented an exemplary application scenario, where the requested task by *DR* requires the *CC/CC*s to report some health conditions to CSP. Furthermore, it requires processing of collected data into useful and authentic information before delivering to *DR*. In this kind of situation, services taken from the users may not be fully trusted, while on the other side due to exploitations of outsources, *DR* may also concerned about privacy [3], [24]. The same situation does exist for *DO/CC* too, who do not want to expose their private information (location and identity).

In the view of our proposed scenario, *DO*s/*CC*s can be seen as Mobile Workers (MWs) or data contributors in Mobile Crowd Sensing (MCS) environment. On successful completion of sensing tasks, MWs can be assigned some rewards [24], [25]. Many mechanisms and mechanism design games have been proposed to provide services to the requesters [24], [26]. Requester in MCS is analogous to *DR* in our designed scenario. Game theoretic setting has been adopted in some literature to represent the selfish behavior of MWs. As recruited mobile sensing workers may report maliciously, *DO/CC* can also submit fake information [26]. So trust on reports is doubtful as they can report dishonestly or intentionally can contribute inaccurate data to misguide the platform in our case to misguide CSP. Incentive mechanism based approaches in MCS stimulate the mobile workers by paying monetary rewards [27]–[29]. The situation can be same in our presented case but here in this work incentive mechanism is not our priority. In next section, we have presented some work on privacy preservation in MCC.

B. PRIVACY PPRESERVATION IN MCC

Privacy in MCC have turned into more severe problem than others because of several reasons like: insecure open air transmission medium, resource-constraint cellular devices, cloud storage and processing in heterogeneous environments [1], [30]–[33], [34]. Several outsource based schemes have been proposed in literature. Some of them offer outsource services to store data at CSP and later on provide access to *DR*s with proper access management procedures. As in this process original data is not available to *DR* so verification problem of provided data occurs. With this motivation some approaches in literature proposed verifiable outsourcing where the extensive computing tasks are outsourced at CSP without exposing the more critical private data [35], [36]. An approach for privacy based access on cloud in crowdsourcing is presented in [37]. In this kind of approaches, access policies play important role, as access to particular storage should be granted to authorised user/users only. Solution to this problem brought the era of access policies. Initially, identity and later on attribute based schemes were proposed [38]. Attribute based schemes were proposed to provide the authorised access. Based on unique attributes, access domain can be verified.

The ABE schemes can be categorized as Cipertext-policy or the Key-policy based schemes. The former schemes utilize is considered to be more suitable and widely used where ciphertext is associated with the access policy. Problem with ABE technique is that complexity grows linearly with increase in number of attributes. In the perspective of Ciphertext-policy based ABE (CP-ABE) [36], the outsourced constant ciphertext policy (OCCP) [39] improves the communication overhead and reduces the computation cost. Moreover, ABE schemes also suffer from variable ciphertext length, incorrect transformation by outsources [39],

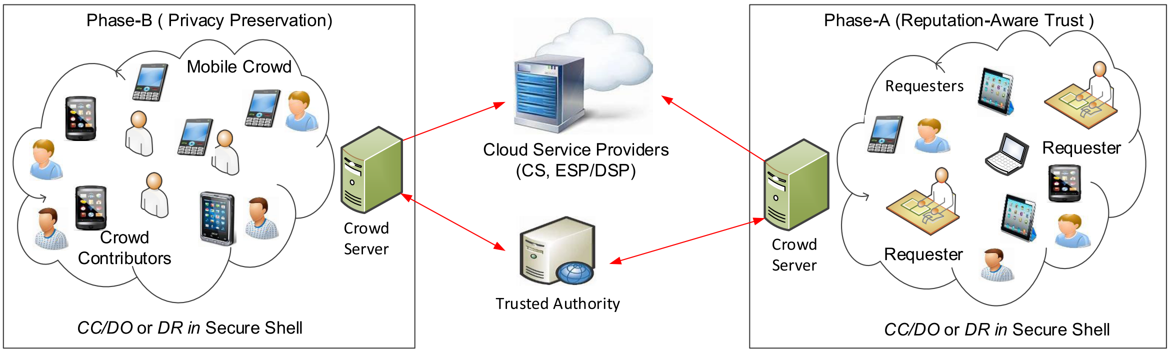


FIGURE 2. Proposed *RTPP* architecture in MCC.

communication overhead [40], need to rely on the service providers, and last but not the least is expensive pairing operation [41]. Like ours proposed work, another scheme [34] addressed privacy issue in sensing domain with cloud based approach still is a different from our exemplary application scenario. To deal with accuracy of transformation, some approaches proposed to get services from other service providers as well like [8]. Schemes like this may require extra monetary incentives. In our proposed approach services from CSP are also exploited by keeping the minimal computations and key control at end devices. Attribute based schemes are efficient for cloud computing but they are not suitable for MCC due to large ciphertext size and computation cost.

Solutions to limited computation and storage capabilities of mobile devices are provided by effectively utilizing cloud computing and MCC in [23], [36], [39], and [42]. Zhou *et al.* [40] presented efficient and secure data storage approach with constant size of ciphertext. They have presented an application scenario where sensors are attached with patient's body and doctor investigates the generated reports. They dealt two main aspects: first was to maintain privacy by ABE scheme. Secondly, efficient storage and constant size of ciphertext is managed. Expensive bilinear pairing operation is outsourced to *DSP*s. Leveraging outsource in MCC is a solution to some of the problems but at the same it gives rise to other issues. These issues can be like, servers cannot be fully trusted, data security and privacy are also important considerations. A *DR* desires to have trust on correctness and authenticity of contributed data by *CC*s, which is neglected in most of the literature approaches. On the other hand privacy of *CC*s must be taken into account too. Correctness of decryption and integrity of data during transmission remained prominent issues as original data is not available in most of the cases to verify the accuracy.

In outsourced ciphertext policy (OSCP) based scheme Zhao *et al.* [43] have proposed a verifiable scheme based on outsources. Their scheme is efficient as it can verify the accuracy of decrypted ciphertext provided by the *CSP*s. They also presented hybrid access policy tree to ensure authorised access. Scheme is tested and found to outperform some of the literature approaches in memory consumption and time take to encrypt and decrypt the messages. We have adopted the prime order bilinear approach as used by [43]. In contrast to this, we have considered different implementation scenario by involving MCS domain, trust and privacy issues in MCC perspective. We have also presented access tree which is more generic as compared to OSCP. The work in [44] is our prior work related to the ideology of this article. The main objective was to ensure the privacy of requester (*DR*) by exploiting the outsources. Concept of secure shell is also there but at one end only. This work can be considered as the extension of [44]. Focus of this work is on dealing with trust and privacy concerns of *CC* and *DR* in MCC both at the same time.

IV. SYSTEM MODEL

In this section, we have presented the proposed framework/model. As the Figure 2 shows that proposed scheme is divided in two phases. In Phase-A, we deal with the scenario where DR requests some services and CSP needs to hire some DOs/CCs, who may report incorrectly so ignorance on trust cannot be tolerated. In case requested data/information is already stored at CS, authorised access to DR is enforced by CSPs. To deal with the issue of trust we proposed to use some mechanism which can ensure truthfulness of reported results. In Phase-B, we proposed solution to *DO*'s/*CC*'s privacy at the time of contribution to the request from the DR and vice versa. For secure communication between end devices and *AS*s, we have introduced the concept of secure shell as shown in Figure 2.

In the proposed approach, though encryption/decryption service providers are exploited, still they will not be able to get the original message even they collude. It is because of generating critical ciphertext fully at end-devices with low computational capabilities. This makes the proposed scheme very efficient as privacy can be achieved for mobile devices without exposing the original message. Trusted authority (TA) is responsible for generating the keys. We assumed that channels between *TA* and *AS* are secure. To secure the channel between AS and end devices, we introduced the concept of secure shell.

At CSP platform, $T = \{\tau_1, \tau_2, \tau_3 \ldots\}$ are the set of tasks announced by the platform as a part of data collection process for *DR*s query. Each task would have some task completion requirements like: average reputation of *CC* (should not be less then a threshold value) and dead line. Selection of *CC*s from set $U = \{u_1, u_2, u_3 \ldots\}$ would be on the base of reputation score in previously completed tasks. For new *CC*, average trust level can be calculated by the historical observations. Number of *CC*s to be recruited may depend upon task requirements. Reputation score can indicate expected task completion quality of reporting. To calculate and analyse the quality of sensing, mechanism is based on the feedback of *DR*s.

A. ACCESS POLICY TREE

Zhou [40] have presented the access policy tree, where the attributes (*Att*) are placed at leaf nodes and internal nodes represent logical operators including AND ($\wedge$) and OR ($\vee$) as illustrated in Figure 3(a). For the AND operator threshold value is $k_x = num_x - 1$, where num_x represents child nodes of a node x. On contrary for OR ($\vee$) operator, the threshold value $k_x = 0$. Moreover, k_x is used to select the degree of polynomial used for outsourcing the computations of encryption and privacy preservation of data. Each leaf node contains an attribute that is used for encryption and can only perform decryption as per assigned attributes for encryption. A *DO* has to select a policy tree $\tau = \tau_{ESP} \wedge \tau_{DO}$, which is a hybrid tree of τ_{ESP} and τ_{DO}. Sub-tree for data access policy of τ_{DO} contains less number of attributes as compared to *ESP*. Zhao [43] have further included another option for hybrid tree $\tau = \tau_{ESP} \wedge \xi$ that enables the encryption with any policy as illustrated in Figure 3(b). In that case τ_{E-CSP} represents policy sub-tree at Encryption-Cloud Service Provider (E-CSP). We have proposed an additional feature for the policy tree by maintaining a set of client side attributes in the default policy tree at *DR* that is presented in Figure 4. During the key generation request, *DR* randomly chooses an attribute $Attr_m$ from a set of $Attr_1$, $Attr_2$,..., $Attr_m$ where m = $\{1, 2, 3, \ldots\}$. The value of m is changeable as per security level of the system. Reputation calculation, it's updation and privacy preservation in MCC are presented in the next sections.

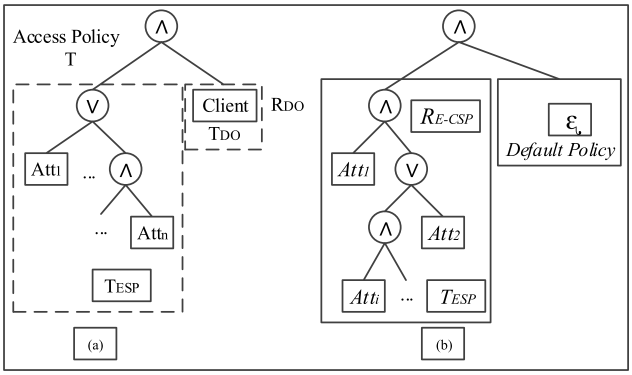


FIGURE 3. Access policy tree for (a) Hybrid tree and (b) Hybrid tree with default policy support.

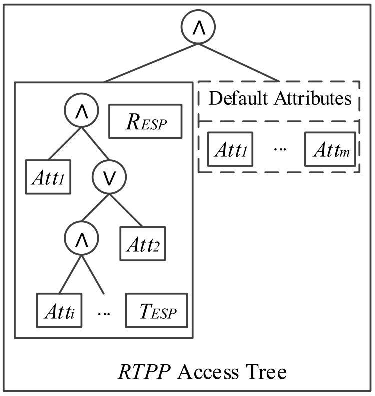


FIGURE 4. Hybrid tree with dynamic attribute selection.

V. REPUTATION-AWARE TRUST AND PRIVACY PRESERVATION (RTPP) SCHEME

This section presents system model and methodology that is used for the reputation aware trusted sensing and privacy preservation in MCC. *DR* (sensing device like body sensors) may requests some sensing services about health issues from CSP and in turn *CC*s take part in data collection process initiated by CSP, can be one of the possible application scenario. *DR* desires for trusted reporting while keeping the privacy of query details (location and identity). Whereas *CC* also does not want to expose privacy when making contribution. As being the owner of mobile devices it is not feasible for *DR* and *CC/DO* to apply complex cryptographic techniques to achieve privacy. Proposed scheme is capable of providing trusted reporting to *DR*s. Privacy of resource constrained mobile devices is achieved through CP-ABE based scheme by effectively applying outsources in data retrieval/storage process. In case to grant access to the stored data at data center, proposed scheme employs policies to ensure authorized access. End devices may require complex computations to be performed or data to be stored, all this can be done at CSPs. In this work, we interchangeably used *DO/CC* so they should be considered as the same entity until mentioned.

For privacy preservation of end nodes in MCC, we proposed verifiable outsourced ABE scheme based on the bilinear group of prime order. The designed system for this part is known as the Anonymous Secure-shell Ciphertext-policy Attribute-Based Encryption (AS-CABE). CP-ABE scheme is constructed based on [40], in which at the root node AND logical gate is implied to grant access. To improve verification, key-encapsulation mechanism is exploited. Hash function is applied at the concatenation of ciphertext from *ESP* (Encryption Service Provider) and *DR*. Critical computations at final ciphertext are also applied which keeps the key control at end device. The second hash value is then used to affirm the correctness of the outsourced decryption. Computational complexity of our proposed schemes is expected to be constant. With the aim to provide privacy, another approach for local business is also presented in [43].

After the completion of registration phase, *AS*s remove participant's private sensitive information. At the same time

*AS*s mask their identities. Information from *AS*s is later on removed to avoid correlational attack. There are different attacks that are possible in our proposed model like: denial of services, collude attack, passive attack, correlation and identity theft attack. In the analysis section these attacks are analysed.

In next two subsections, we have presented trust development phase and work flow of privacy part. Frequently used notations in this paper are presented in Table 2.

TABLE 2. Some of the important notations used in this work.

Notation	Description
λ	History removing factor
α, β	Agent rating weightage, constant factors (In Phase-A) and random integers in (Phase-B)
CC	Crowd contributors/ Mobile users/ Sensor
DR	Data requester
DO	Data owner
AS	Anonymity Server
TA	Trusted Authority
EU	End Users(*DR, DO/CC*)
ESP	Encryption Service Provider
DSP	Decryption Service Provider
CS	Cloud Storage
TS	Set of Attributes
AP	Access Policy
M	Orignal Message
R	Reputation Score
P	Set of Parties
T	Task
C_M	Ciphertext Message
SK, K_s	Private Key/ Secret Key, Key Space
U_k	Unique Verifier
A_L	Attribute List
ID_{cc}	Identity of Crowd Contributor
PK	Public Key
MSK	Master Key
ID	Identity
PS	Total number of participants
P_Ψ	Probability that *DO* is compromised
P_{DRC}	Probability of not compromising
P_A, P_B	Probability of getting node A's information, Probability of getting node B's information
Ψ	Number of compromised participants
$Attr_m$	Attribute
Z_p	Finite field
H	Hash Function
k	Security credential
T_i	Time stamp
n_i	Random nonce
S_{SK}	Symmetric secret key
I_T	Intermediatory token
T_{DRi}	Policy tree of D_{Ri}
H_{Attrm}	Hash of $Attr_m$

A. PHASE-A REPUTATION-AWARE TRUST

This subsection is devoted to overcome the trust issue of *DR* on *DO/CC*. A central authority is there that manages trust and offer services to *DR* when requested. *DR* may be a mobile device/a body sensor with limited power, so cannot perform complex computations to ensure trust by its own. For this we have used "Beta reputation" [10] which is a reputation management system from economics to ensure the trust using historic observations. This reputation system can be managed at a central or in a distributed environment, in our case we adopted it for a central authority, which is CSP.

CSP calculates and maintains the trust score of *DO*s//*CC*s and *DR*s at the same time which makes our scheme a unique one to provide correctness and authentic information to *DR*s. CSP is assumed to calculate and maintain the trust score, which will represent the *DO*'s/*CC*'s reputation in previous data contributing tasks. It is also crucial for CSP to achieve computations efficiently as availability of alternative CSPs is not an issue. This factor also stimulates the CSP to perform selection of *CC*s in a very careful manner as *DR*s would be much more conscious about truthfulness and accuracy to the contribution.

Reputation system work by calculating two variables based on previous contributions. To apply this scheme, we assumed that CSP maintains record of the *DO*s/*CC*s. This assumption seems to be logical as CSPs are expected to have enough storage and computation power. The main objective of the Phase-A is to provide a platform which builds its trust towards *EU*s.

Our rating scheme is of two types, one for *DR*s and the other for *DO*s/*CC*s. First, we will presents reputation mechanism for *DR*.

1) *DR*'S REPUTATION

DR requests services from CSP and after necessary processing, desired output is delivered in response. In our designed approach *DR* is supposed to grade/benchmark the quality of response. Reported quality may vary from person to person depending upon the expectations of response. Expertise, experience and interest may be required to analyse the response to assign fair rating. To judge the real quality of response provided to a *DR*, CSP should investigate the reply with the perspective of quality. Especially, when requests for same kind of tasks are accomplished for different *DR*s. Below we present a mechanism to judge the quality of response by rating the *DR*s themselves and to assign more accurate ratings to *CC*s.

$$R_T = \alpha_1 {R_1}^T + \alpha_2 {R_2}^T + \ldots \alpha_N {R_N}^T \tag{4}$$

Where $\alpha_1, \alpha_2 \ldots \alpha_N$ are the calculated weights from history of task completion. ${R_1}^T, {R_2}^T \ldots {R_N}^T$are ratings given by *DR*s after receiving the requested task from CSP. From (4)

$$R_T = \sum_{i=1}^{N} \alpha_i {R_i}^T \tag{5}$$

$$\alpha_T = \sum_{i=1}^{n} \frac{1}{n} \alpha_{n-i} \tag{6}$$

Where N is the number of *DR*s, who had assigned ratings and n is the history parameter, α is calculated from the previous value of α in history and T represents task. Previous values are considered until the value of α becomes zero. This represents the end of effective history for *CC*s selection. Next we presented, how the weightage will be updated on the feedback of *DR*.

a: WEIGHTAGE (α) UPDATION

Weightage is a kind of voting power, we have adopted a dynamic approach to update it. Feedback from the *DR* to rate the *CC*s can be in positive or negative. Positive represents the good satisfaction level of *DR* and vice versa. As we have considered ratings from different *DR*s, we set average reporting for tasks to get optimum value as standard deviation. If feedback on a tasks is accumulatively at satisfactory level, then rating given by *DR* in correspondence with the majority will increase its weightage otherwise decrease. If (R) given by *DR* is within the acceptable standard deviation ($R \rightarrow [\mu_R - \sigma_R, \mu_R + \sigma_R]$), then $\alpha = \alpha_T + \beta\alpha_T$, where $\mu_R = \frac{1}{N}[R_1 + R_2 + \ldots R_N]$, $\sigma_R = \sqrt{\frac{\sum_{i=1}^{N}(R_i-\mu_R)^2}{N-1}}$ and β is the constant factor.

Using (6).

$$\alpha_T = \sum_{i=1}^{n}\frac{1}{n}\alpha_{T-i} + \beta\sum_{i=1}^{n}\frac{1}{n}\alpha_{T-i}(Positivefeedback) \qquad (7)$$

If Rating (R) is not within the acceptable standard deviation ($R \not\rightarrow [\mu_R - \sigma_R, \mu_R + \sigma_R]$), then $\alpha = \alpha_T - \beta\alpha_T$.

Using (6).

$$\alpha_T = \sum_{i=1}^{n}\frac{1}{n}\alpha_{T-i} - \beta\sum_{i=1}^{n}\frac{1}{n}\alpha_{T-i}(Negativefeedback) \qquad (8)$$

Where α presents updated weightage value. When feedback from *DR*s for some specific task is positive, α is updated using (7), whereas for negative feedback α is updated using (8).

Although CSPs are assumed to have enough storage and computation capacity but nothing can be unlimited as large amount of data may have to be managed. So to make the scheme efficient with respect to memory utilization, we have used ageing factor from [10]. This feature will reduce the impact of previous reputation score of *DO*s on future selection to be a data contributor. With ageing factor, storage space can be saved and efficiency in terms of time required to traverse the records can also be achieved. By reducing the search space, CSP can offer real time services to some extent. This factor makes the list of effective reputation scores shorter and shorter. After every contribution, CSP updates the list of R for *CC*s. Ageing factor can be considered as the sliding window concept, presented in Figure 5 which is taken from [10] and enhanced to adopt the multiple reputation updating scenario. Figure 5 represents the reputation and trust management of *DR* and *DO/CC* in our designed approach.

To save storage space and required computations, (9) presents the procedure. Equation (4) to (15) includes the computation for *CC*s selection and updation of reputations after getting feedback from *DR*s in the reputation system. Feedback from *DR*s is a kind of rating the legitimateness of provided information.

$$R^T_{n,\lambda} = \sum_{i=1}^{n} R^T_n \lambda^{n-1} \qquad (9)$$

Where $\lambda \in [0, 1]$ determines the history maintained.

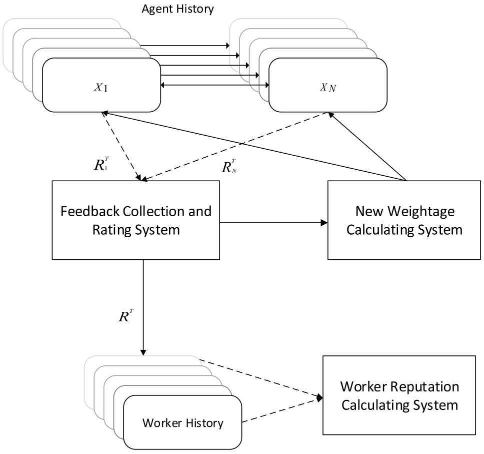

Agent History
x_1
x_N
R_1^T
R_N^T
Feedback Collection and Rating System
New Weightage Calculating System
R^T
Worker History
Worker Reputation Calculating System

FIGURE 5. Ageing factor and updating reputation system.

$\lambda \rightarrow 1$ means no forgetting at all and $\lambda \rightarrow 0$ represents history is not maintained at all.

Selection of well reputed *CC* is important to ensure trust of *DR*. The basic purpose of reputation system is to select the most suitable *CC* on the base of their R score. Better R means more chance of selection to be the *CC* and ultimately on successful completion of task, *CC* may get reward from CSP. After every successful completion of task and getting feedback from *DR*s, R is updated at CSP. Next, we present reputation mechanism for *DO*s.

2) RATING OF *CC*s

For the completed tasks, rating of *CC*s will be calculated on the feedback of *DR*s. (From (4)) $R_T = \alpha_1 {R_1}^T + \alpha_2 {R_2}^T + \ldots \alpha_N {R_N}^T$

$$R = \sum_{i=1}^{n} \alpha_n R^T_n \qquad (10)$$

where R is the rating of a single task.

For m tasks,

$$R_T = \frac{1}{m}[\sum_{i=1}^{n}\alpha_n R_n^{T_1} + \sum_{i=1}^{n}\alpha_n R_n^{T_2} + \ldots \sum_{i=1}^{n}\alpha_n R_n^{T_m}] \qquad (11)$$

By combining (10) and (11)

$$R_T = \frac{1}{m}[\sum_{j=1}^{m}\sum_{i=1}^{n}\alpha_n R_n^{T_m}] \qquad (12)$$

where R_T is the reputation of currently completed task set.

$$R = \gamma_1 R^T + \gamma_2 R^{T-1} + \ldots \gamma_n R^{T-n} \qquad (13)$$

Here R is final reputation calculated on the base of current and effective history reputation value. γ decreases as move deeper in the history of task completion where $\gamma_1 > \gamma_2 > \gamma_3 > \ldots > \gamma_n$, eventually becomes 0 (zero). When value of γ decreases upto zero then history is removed further from that point to free the storage space. From (13)

$$R = \sum_{k=1}^{n} \gamma_k R_k^{T-k} \tag{14}$$

For m tasks $R = \gamma_1 \sum_{i=1}^{n} \alpha_i R_i^T + \gamma_2 \sum_{i=1}^{n} \alpha_i R_i^{T-1} + \ldots \gamma_m \sum_{i=1}^{n} \alpha_i R_i^{T-n}$

$$R = \sum_{j=1}^{m} \sum_{i=1}^{n} \gamma_j \alpha_i R_i^T \tag{15}$$

To achieve trust of *DR*, selection/recruitment of *CC*s should be done very carefully. For this ageing factor plays an important role.

B. PHASE-B PRIVACY PRESERVATION BY OUTSOURCING IN MCC

To preserve privacy of resource constrained mobile devices, we presented AS-CABE in this section. We briefly explained methodology of proposed scheme to achieve privacy in cloud oriented mobile computing, which is the Phase-B of the proposed framework as shown in Figure 2. Bilinear mapping, access policy based on CP-ABE scheme and outsourced encryption technique is presented.

The proposed model is shown in Figure 2 in which crowd contributors can be mobile participants, who generate, gather or request data. To achieve participant's privacy and anonymity for crowd (contributors and requesters), the proposed system has crowd servers to gather *CC*s/*DR*s data and keep it by masking their identities. To fulfill privacy and security requirements, encrypted data is sent to cloud storage by crowd server, it also gathers and stores participant's data anonymously.

For end users, outsourced encryption/decryption service providers perform computations without exposing original data, by this, end-to-end user's data privacy and anonymity is achieved. Trusted authority is responsible for: authenticating end-users, ensuring privacy preservation and to play a vital role in outsourced encryption/decryption by issuing keys. By having anonymity server and secure shell, we will be able to secure participants location and identity. In our proposed scheme, we have access policies to grant authorised access to end users. Next we presented the details to achieve aforementioned objectives.

To present methodology briefly, firstly, we assumed that there is an efficient algorithm Ψ to generate bilinear group who's input parameter is $\tilde{\alpha}$. This algorithm gives output G = $\{g, G, G, G_T, p\}$ where generator of G is g, is of prime order p. We considered G as a bilinear group for all x,y belongs to G, where a, b belongs to Z_p under the bi-linearity condition and bilinear map $s : G * G \rightarrow G_T$. For further details on bilinear maps, we refer to preliminaries section of this article. Secondly, both group operations and bilinear map are computed efficiently. An access structure is also defined to represent a set of parties P, where $P = \{p_1, p_2 \ldots p_n\}$ with the collection of monotone and non-monotone subsets of $\{p_1, p_2 \ldots p_n\}$. The access structures belong to parties for authorized and unauthorized set. Thirdly, a symmetric encryption scheme consisting of two polynomial time algorithms: symmetric encryption (SE) and ciphered message C_M took part in the encryption process. The original message M is constructed using a key (K) from key space K_s. A pseudorandom generator using one-time padding encryption process makes proposed scheme secure from adversary, for the case when malicious party takes advantage within polynomial time.

1) KEY GENERATION BETWEEN *DR* AND *ESP*

As the proposed scheme is based on ciphertext attribute policy so the participant's security mechanism is related with a set of attributes based policy tree. These attributes can be descriptive or may be some numeric representation that are common between end users. A participant can decrypt data if and only if there is an assignment of the private key according to access rights, whereas accuracy of attributes is also ensured. During the setup phase, *TA* receives a security credential k from the *DR* and then selects a bilinear group G with a prime order p and a generator g. *TA* also selects two random integers α and β from the finite field Z_p. *TA* computes $h = g^{\beta}$, hash function $H : \{0, 1\} \rightarrow G$, prepares the public key as $PK = \{G, g, h, T_{TA}, e(g, g)^{\alpha}, H\}$ and master key $MSK = \{\beta, T_{TA}, g^{\alpha}\}$. *TA* keeps the *MSK* as a secret, transmits the (ID_{TA}, C_1) containing *PK*'s parameters to the *DR* and encrypt using DR_i's public key as given in (16). Where ID_{TA} is identity of *TA*, T_{TA} represents the timestamp at *TA* and ID_{DR_i} represents the identity of receiver DR_i.

$$C_1 = E_{PK_{DR_i}}(ID_{TA}, G, g, h, e(g, g)^{\alpha}, H, T_{TA}, ID_{DR_i}, MAC(g||h||e(g, g)^{\alpha})||T_{TA}||ID_{DR_i}) \tag{16}$$

DR_i receives the message and decrypts using its private key to get the message parameters and then calculates the difference of T_{TA} with the receiving time at DR_i to verify the freshness of message. If the difference is larger than a threshold value then the message will be discarded. If the message is within time constraint then DR_i calculates the $MAC'(g\|h\|e(g, g)^{\alpha})\|T_{TA}\|ID_{DR_i})$ and compares it with the *MAC* sent by *TA*. If both values are same then it is verified that message is not altered by any middle-man and can be used for further operations. Otherwise the message is discarded even at this stage. After successful integrity check, the public parameters are saved in the repository. DR_i prepares a request message to *TA* for establishing new session key between DR_i and *ESP* that can be the crowd server in our scenario. DR_i randomly selects an attribute $Attr_m$ out of m attributes in the DR_i's policy tree T_{DR_i}. The request message is encrypted using public key of *TA* which contains H$(Attr_m)$ that is Hash of attribute $Attr_m$, timestamp T_i at DR_i and a random nonce value n_i as given in (17). DR_i transmits the message (ID_{DR_i}, C_2) to *TA*.

$$C_2 = E_{PK_{TA}}(ID_{DR_i}, H(Attr_m), T_i, n_i, ID_{ESP}, MAC(H(Attr_m)\|T_i, n_i, ID_{ESP})) \tag{17}$$

TA receives the message and decrypts it using its private key to extract the parameters. Then it checks the freshness of message using timestamp and verify the integrity of message using *MAC*. After that, *TA* extracts the master secret key *MSK* for DR_i, choose a random number and calculates $\omega_1 = H(ID_{DR_i} \| n_i \| e(g, g)^{\alpha})$ and $\omega_2 = H(ID_{DR_i} \| T_i \| g^{\alpha})$ and generates a symmetric secret key as given in (18).

$$S_{SK} = H(ID_{DR_i}) \oplus \omega_1 \oplus \omega_2 \oplus H(Attr_m) \oplus H(ID_{ESP}) \quad (18)$$

TA prepares a ciphertext of message containing $\omega = \omega_1 \oplus \omega_2$ and *MAC* as given in (19). Where T_{TA_E} is timestamp generated for this message to ensure message freshness. Moreover, a ciphertext of ω_2 is also attached in message for transmission to DR_i. *TA* transmits the message (ID_{TA}, C_3) to *ESP*.

$$C_3 = E_{PK_{ESP}}(ID_{TA}, T_{TA_E}, \omega, H(Attr_m), ID_{DR_i}, MAC(T_{TA_E} \| \omega \| H(Attr_m) \| ID_{DR_i}), E_{PK_{DR_i}}(ID_{TA}, \omega_2)) \quad (19)$$

On receiving the message, *ESP* first decrypts it to ensure message freshness and then verifies its integrity. After successful verifications, *ESP* prepares the key as $S_{SK_E} = H(ID_{DR_i}) \oplus \omega \oplus H(Attr_m) \oplus (ID_{ESP}, C_4)$ to transmit to DR_i, where timestamp at *ESP* is represented as T_E as given in (20).

$$C_4 = E_{PK_{DR_i}}(ID_{ESP}, T_E, n_E, MAC(T_E \| n_E), E_{PK_{DR_i}}(ID_{TA}, \omega_2)) \quad (20)$$

DR_i receives the message, checks its freshness and integrity by T_E and *MAC* values. After that, DR_i obtains ω_2 by decrypting $E_{PK_{DR_i}}(ID_{TA}, \omega_2)$ using its private key. It also calculates the value of $\omega_1 = H(ID_{DR_i} \| n_i \| e(g, g)^{\alpha})$ to prepare the secret session key for securely communication with *ESP*.

When a *DR* requests some computations or query for legitimate information that can be processed at a CSP, without the need of further outsourcing even in that case interests were exposed. If the required/necessary information to respond the request explicitly exists at CSP then it is easy to fulfill it. Different from most of the literature, we have assumed the scenario that a particular request can not be satisfied directly rather it may require some prior processing. It may be the case that CSP does not have required data to be processed to provide the service. In this case, we proposed the selection of *DO*s/*CC*s to make contribution then after getting the desired answers, information can be saved at cloud storage for future use as well. Access to stored information at data centers can be only provided when access rights are satisfied. Data service manager strictly ensures the implementation of *AP*s to avoid unauthorized access to the stored data. This kind of situation may seems to be similar with crowd service providers but in our case CSPs not only collect requested data from *DO/CC* but also process, store contributed data and information for future queries. Further, more information can also be generated by the stored data, instead of simply providing access to data repository. Whereas in crowdsourcing applications, services are simply provided by recruiting the workers. In that situation, platform just acts like an entity that makes proper match of jobs and job seekers. In this way the proposed approach is different from crowd service providers.

Access rights of users are deployed by adopting the concept of access tree where some threshold is defined according to the domain of participants in the network. In the proposed model, cloud storage is a semi-trusted platform, which is responsible to provide storage and computational facilities to the participants.

Proposed methodology in this phase is divided into two main parts, secure bonding and authentication between end users and *AS*s. Instead of using search engines Phase-B consists of data collection from crowd, where the objective is to utilize human intelligence. This part also ensures the secure data gathering, storage to cloud and to perform security and integrity of data decryption when requested by *DR*.

2) ANONYMOUS SECURE-SHELL BETWEEN END USERS AND CROWD SERVER

Proposed scheme enhances [40] in terms of efficiency and secure data storage to make it suitable for mobile cloud computing by introducing anonymity server and ultimately by building secure shell in crowd contributing network. Now we presents the construction of secure shell. Inputs for protocol-I are privacy policy, secret key, end user query/task and ciphertext. Every *CC* needs to be registered with *AS* and should be authenticated by *TA*. As we have proposed set of default attributes, which can provide authentic access to any new entity. $H(Attr_m)$ is an attribute which is randomly selected from default attributes list. Within the secure shell, *CC* at first transmits its details like identity by encrypting the text with the public key of *TA*. *TA* validates *CC* attributes, ensures that it belongs to the member's list, then a key for secure communication is generated and shared with *CC* and *TA*.

Protocol-I Anonymous Secure-Shell

```
$CC \rightarrow TA : E_{PK_{TA}}(ID_{cc}, \eta, T_{cc}, n_{cc}, H(\eta \| T_{cc} \| n_{cc}))$

$TA$: Generate Key $K_{cc \rightarrow AS}$ using $Attr_m$ in policy tree $T_{cc}$ for $CC$
    Verify $ID_{AS}$ in Membership-List
    Share key with $CC$ and $AS$

$TA \rightarrow AS : E_{PK_{AS}}(ID_{AS}, \omega, H(Attr_m), H(\omega || H(Attr_m))), E_{PK_{cc}}(ID_{TA}, \omega_2)$

Setup Anonymous Secure-shell between Contributor and Crowd Server

$CC \rightarrow AS : E_{K_{CC-AS}}(ID_{CC}, Concatd_{Data_{String}}, T, MAC(Concatd_{Data_{String}})$

$AS$: Save Credentials and $ID_{CC}$ as Mask($ID_{CC}$) for anonymity
    Remove all security parameters for this session
```

Protocol-II Out Sourced Data Encryption and Decryption

Part-I: Secure Data Storage by *DO DO*: Generate s_1 and s_2 and performs $Encrypt_{DO}$ $(s_2, Attr_m)$ to generate cipher credentials C^O_{DO} like [38] and transmits to ESP

DO: Set I_T as intermediate Token and calculate verifier $V_x = H(I_T)$ and cross verifier $CV_x = h\left(V_x \| C^O_{DO}\right)$

DO: Calculate symmetric key $S_{KDO} = V_x \oplus H\ (Attr_m) \oplus H(h(I_T) \oplus H(C^O_{DO}))$

DO: Calculate ciphertext C^S_{DO} as $E_{S_{KDO}}(ID_{DO}\|M)$

DO→ ESP: $E_{PK_{ESP}}(ID_{DO}, n_{DO}, T_{DO}, s_1, I_T, C^O_{DO}, C^S_{DO}, H(s_1\|C^O_{DO}\|C^s_{DO}\|T_{DO}\|I_T\|n_{DO}))$

ESP: Verifies message freshness and integrity using T_{DO} and Hash $H(.)$

ESP: Perform $Encrypt_{ESP}(s_1, T_{ESP})$ to generate ciphertext credentials C^O_{ESP} like [38]

ESP: Calculate ciphtetext as $CT = \left\{C^O_{DO}, C^S_{DO}\right\}$

Part-II: Decryption and Data Recover at *DR*

DR: Calculates Blind Key $SK' = H(SK)$ and a recovery key RK

DR→ *DSP*: $E_{PK_{DSP}}(ID_{DR}, SK', Attr_m, T_{DR_1}H(SK'\|T_{DR_1}))$

DR→ *ESP*: $E_{PK_{ESP}}(ID_{DR}, REQ, T_{DR_2}, H(SK'\|T_{DR_2}))$

$ESP \rightarrow DSP : E_{PK_{DSP}}\left(ID_{ESP}, T_{DO}, CT', H\left(T_{DO}\|CT'\right)\right)$

DSP: Perform $Decrypt_{DSP}\left(CT', SK'\right)$ to get the partial decryption ciphertext (PDC)

$DSP \rightarrow DR : E_{PK_{DR}}(ID_{DSP}, T_{DSP}, PDC, H(T_{DSP})\|PDC))$

$ESP \rightarrow CSP : E_{PK_{CSP}}(ID_{ESP}, T_{ESP}, CT, I_T, H(T_{ESP})\|CT\|I_T))$

$CSP \rightarrow DR : E_{PK_{DR}}(ID_{CSP}, T_{CSP}, CT, I_T, H(T_{CSP})\|CT\|I_T))$

DR: Perform $Decrypt_{DR}(PDC, RK, C^O_{DO})$ to get temp ciphertext C_T

DR: Calculate $V'_x = H(I_T)$ and $CV'_x = h(V_x\|C^O_{DO})$ to verify else discard

DR: Perform Decrypt (C^S_{DO}, S_{KDO}) to get message M

TA encrypt text with the public key of *AS* and transmits it to *AS*. Ultimately *AS* encrypts the text with public key of *CC* and transmits the message to *CC*. On receiving the message from *AS*, *CC* concatenates the data string, text with its identity, take *MAC* and in response sends ciphertext to *AS*. This completes the creation of secure-shell between *CC* and *AS*. To handle anonymizer's single point of failure, *AS* deletes participant real identities after masking their location and identity attributes. *TA* is responsible for generating secret key as explored above using policy tree with dynamic attribute selection (*TS*). It is done to control access and to store collect data at cloud storage. Due to this we will be able to avoid correctional attacks.

In this case, *TA* also prepares a secret key *SK* using *MSK* as in [38] and [40] but we have variation in random attribute selection from default attribute set in our *RTPP* policy tree. The *SK* is transmitted to *DO* on a secure channel.

3) OUTSOURCED ENCRYPTION AND DECRYPTION

Data access policies are defined at *TA* by running access policy algorithm which takes *MSK* as input and generate keys to communicate within secure shell, among *ESP* and *DSP*, and *CS* service providers. To avoid heavy computations of attribute based access policies at mobile node, the *ESP* is used for extensive encryption operations for *DO/CC*. On the other side *DSP* is exploited for complex decryption operations for *DR*. At first, *DSP* only decrypts ciphertext in an intermediate format then final decryption is performed at the receiver for actual message. The subset of selected attribute oriented access policy runs at *CC*s to compute as per proposed *RTPP* access policy. The detailed protocol and work flow for secure data sharing, data access policy, outsourced encryption, and decryption are illustrated in Protocol-2.

It consists of two parts, Part-I deals with the secure data storage at *CSP*. To do so it generates s1 and s2, which are the data strings. *DO* perform encryption with s2 and its attributes from *TS* (set of attributes) to generate cipher credentials then transmits it to *ESP*. Then *DO* generates an intermediatory token (I_T) for the calculation of verifier and cross verifier to ensure the correctness of ciphertext at final stage in this protocol. *DO* calculates symmetric session key, produces ciphertext from original message based on its identity and then transmits it to *ESP* with security credentials. On receiving the message from *DO*, *ESP* verifies the freshness and integrity with hash function. It then generates cipher credentials and calculates the ciphertext represented at *CT*.

Part-II deals with the decryption and recovery of the stored data at cloud. For this, *DR* calculates blind key and recovery key. Then it takes hash on blind key, perform encryption based on its attributes and identity with the public key of *DSP*, finally transmits message to *DSP*. *DR* also sends request to *ESP* by using the public key of *ESP*. *ESP* takes hash on the ciphertext with its identity and encrypts the message with the public key of *DSP*. *DSP* then perform decryption on the ciphertext with blind key of *DR* to obtain partially decrypted text as the final decryption on plain ciphertext is to be performed at end device. *DSP* sends partially decrypted text to *DR*. Whereas *ESP* send its identity, ciphertext, token and calculated hash on these credentials, to *CSP*. *CSP* in response sends ciphertext to *DR*, which is generated using public key of *DR* and includes token and its identity. Recovery key is used by *DR* to perform decryption on partially decrypted ciphtertext. By this *DR* obtain temporary ciphhertext represented by C_T in this protocol. Now on the behalf of *DR* the most important step is to ensure the correctness of decryption. Verification is justified if the verifier and cross verifier are same otherwise message would be discarded.To overcome unfeasibility (requires high communication bandwidth) due to *CC*s frequent join/leave, and continuous monitoring by *TA*, proposed scheme get benefits by induction of *AS*. Outsourced encryption and decryption is secure as final critical computations are performed by end users.

VI. ANALYSIS

To provide trust in our designed approach we utilized reputation updating system by enhancing it to make suitable for our scenario. Computations of reputation system are assumed to be done at CSP. Novel approach in our model is that we maintained the reputation of *CC* and *DR* both at the same time. Purpose of this was to give well calculated reputation score by keeping the rational human behavior in mind. Assigning *R* is a very responsible task and requires some judgment capabilities of particular reported phenomena. Humans can also be biased depending upon different factors. Calculating reputation can be tricky as the level of understanding of *DR*s to give reputation score may vary. Different *DR*s may assign different ratings to the same task, which is handled in our proposed approach. Although *CSP*s are expected to be powerful devices but to reduce space and to decrease traversing time, ageing factor is introduced. This will also help to effectively utilize data storage capacity at *CSP* by removing unnecessary part. Few limitations of the proposed work are: outsource services are exploited especially the assumption of CSP to maintain trust as a central authority. In that case if CSP became compromised then trust cannot be ensured for end users. This scheme is efficient in producing constant ciphtertext length, in providing verification of correct decryption of ciphtertext and also in ensuring the authorised access. These processes may require frequent communication which can be a difficult situation for low power end devices.

Some of the important assumptions in the proposed work are: end devices are assumed to be the mobile devices with known resource constraints (limited computation and storage capacity). *CC*s are assumed to participate in sensing tasks because proposed approach is able to deal their one of the most important concern of privacy. In this approach third party (Trusted Authority) is assumed to be trustable. TA is also responsible for key generation to secure communication. We assumed that channels between *TA* and *AS* (Anonymous Server) are secure. Among outsourced entities, CSP is jobbed for the calculation and updation of trust score. In privacy part (Phase-B), we have assumed that there is an efficient algorithm to generate bilinear group. An important assumption is that a particular request cannot be satisfied directly rather it may require some prior processing, which may need contribution from crowd. We have assumed that answer to data requester's query may need human intelligence and skills not just search engine as conventional. For simulation purpose, every new user is assigned the value of 0.5 as reputation score R.

A. TIME COMPLEXITY

Reputation (*R*) is parameter that holds a numeric value representing trustworthiness of *DR* on *CC/DO*. Time complexity analysis for the major portion of reputation-aware trust (Phase-A) is presented below.

1) WEIGHTAGE (α) UPDATION

To analyse the ratings, updation of weightage is compulsory. On average, whenever a task is delivered to *DR*, rating is expected to be received in response to the service. There will be increase in the value of *R* for that crowd contributor, who would have done satisfactory level contribution. On the other hand for some task when bad rating will be assigned on collective basis, *R* score of *CC* will drop down as well. Fair dealing has been ensured in this work so one good or bad rating will not make drastic increase or decrease in *R* value of *CC*.

For $i = 1$ to n, $\alpha_T = \sum_{i=1}^{n} \frac{1}{n}\alpha_{T-1}$ calculates reputation weightage of each *DR* so time complexity would be $n*m$, where m is history and n is number of users. History is constant so time complexity is n. $R_T = \sum_{i=1}^{n} \alpha_n R_n^T$, its time complexity is n (here n is the number of ratings).

2) HISTORY AGEING FACTOR

A unique feature of this work is that management of storage space is done in a very effective manner. Usually, servers at cloud have plenty of storage capacity. But it may be impossible to preserve and traverse all the records by effectively minimizing the latency. As we may have to deal with a large number of *CC*'s tasks completion details. For this reason ageing factor was utilized. The purpose was to free unnecessarily occupied storage, as the records of *CC*s get older and become useless. Equation (9) $R_{n,\lambda}^T = \sum_{i=1}^{n} R_n^T \lambda^{n-1}$ presents the history. As history is to be maintained for some specific time limit so time complexity is represented as c, whereas overall time complexity is n.

3) *CC*s RATING

Time complexity to calculate *CC*s rating = $m*n$, where n is number of ratings (*DR*s) and m is the number of tasks, as m and n both posses some constant so time complexity = c. Equation (15) $R = \sum_{j=1}^{m} \sum_{i=1}^{n} \gamma_j \alpha_i R_i^T$ gives the rating so complexity of calculating *R* is *3n+2c*, which means that overall complexity is *n* (number of user).

B. SECURITY ANALYSIS

The security analysis of scheme is on Discrete Logarithmic Problem (DL) because the multiplicative group and group generator are hard. We have evaluated major security portion of the proposed approach. To handle accessibility and consistency threats, it is essential to validate data contributors formally, who want to make contribution. To overcome accessibility with authorization confirmation problem, storage at cloud is provided by authorized access along efficient access policy tree with "AND" logical gate at root node. *AS*s are installed at both ends so efficient task recommendation and distribution can also be managed. In the presence of *AS*, *DO*s/*CC*s can be authenticated to provide trusted and consistent contribution for data requesters by preventing denial of service, which is a dynamic approach. Whereas *DR*s transmissions are also encrypted to prevent active and passive attacks. Trusted authority is responsible for distributing secret keys by applying authentication policy. Message integrity is performed using one-way hash function which is unforgeable during node authentication and cryptographic key sharing. All channels between encryption and decryption service providers are secured.

1) INTEGRITY PROTECTION

To provide integrity in the proposed scheme several measures have been taken. Hash, *MAC*, ω, A_{H_M} are used to transmit secret message over channel. By computing Hash, *MAC* and timestamp at *ESP*, designed approach proves message integrity. Even after taking the necessary measures to ensure integrity, if an adversary node becomes successful in polynomial time then what can be compromised is being presented below. If we consider, a hash function **h(.)** with collusion resistance and one-way cryptography, it can be defined as $h : \{0, 1\}^m \rightarrow \{0, 1\}^k$ then collusion on hash can appear with the some probability, i.e $x' \neq x$ in a way that $h(x) = h(x')$, for some values of x and *h(x)*, in (21):

$$Pr\left[(h(x) = h(x')(x' \neq x))\right] = 1 - (1 - \frac{1}{2^k})^{m-1} \quad (21)$$

we consider the length of binary s_1 string as l. If any node A in the designed model is compromised then adversary can get the information of other nodes in the network with the probability of $Pr\left[Attacker\frac{(K_B)}{K_A}\right] = \frac{l}{2^l}$, where l is $log(p)$ bits which is representing any bit string of a random order. In the system model, outsources at least will have some information about *CC*s/*DO*s and *DR*s that can be compromised. There are some common attributes for the nodes in the network that can be used to give access to any entity. Memory contents of any two nodes in the system model differs in random and unique bit strings within their free spaces. If an adversary node remaines successful against any single node in the network, some contents of other entities in the network can also be disclosed. Memory contents P_A of any node A are disclosed, therefore: $Attacker(P_A(\neq P_B)), Attacker(K_B), Attacker(P_B = (P_A)) \vee Attacker(P_B), Attacker(P_A = (P_B)) \vee False$

When node A is compromised, key of node B can be computed as $K_B = h(P_B)$. Adversary can get only that information of Node B which is common in node A and B. Even when one bit difference is considered, probability of getting node B's information is $P_B = \frac{1}{2^l}$.

In the following section, we have performed security analysis for some of possible attacks on our proposed scheme.

2) DENIAL OF SERVICE

It happens when malicious data contributor may accept tasks at first stage but later on refuse to provide valid results. In proposed scheme, the *AS* overcomes this issue by validating crowd member's presence and by defining their domain. The second type of DoS attack is possible when honest participants may delay results for the sake of more reward. *AS* maintains request/response list to handle this problem. In case *AS* is compromised, reverse engineering is not possible, as identities were kept by masking. On the other side, *DR*s do not want the service providers or any other participant to explore their requested tasks and response on them. As the *DR*s can also be a mobile user with known resource constraint problems, decryption service provider is employed to handle their computations. As decryption is verified by second hash function so there is no issue of incorrect decryption. Along with, the integrity of communication is also ensured. The defined access policy and attribute-set based encryption restrict participants not to overlap the boundary of privileges. Anonymity server oriented bilinear pairing attribute based scheme is secure, reliable and computationally less complex for *CC*s and service seekers.

3) COLLUDE ATTACK

Scheme is secure in collude attack, even all the external entities collude to fetch the original message, still they have to compromise some part of information. As critical computations are kept at *EU* devices, this is a certificate of not losing message in its original/whole form. In case even adversary will be able to get original data once, pseudorandom generator with one-time pad in encryption ensures the integrity of upcoming communication. For every session there is a key, which is changed so attacker is not expected to fetch it for upcoming sessions in polynomial time even succeeded once.

4) CORRELATION ATTACK

Some pieces of information about one or multiple entities may relate to each other. By knowing one attribute, others can also be found as discussed in sub section (integrity protection) of security analysis. In our proposed approach, if we assume that *AS* is compromised, even then private information of *EU*s cannot be exposed. This is due to applying masking to protect personal information. At the time when *EU*s are registered with *AS*, their sensitive information is kept by masking.

Scheme is secure in correlation attacks and reverse engineering is avoided.

5) IDENTITY THEFT ATTACK

The second part of proposed scheme also overcomes the participant's identity theft attack from intruders. During participant registration phase, public key of *AS*s is used to share secret information of *EU*s. The *AS*s keep hashed values of participant's identity with some random number function application to hide private data from intruders. Secondly, a blind algorithm runs at anonymity server to encrypt and decrypt data, which provides anonymous data services to the participants.

VII. RESULTS AND ANALYSIS

We have analysed existing and proposed schemes for MCC based reputation aware trust management and privacy preservation. We have developed web services to perform *ESP* and *DSP* functionality by interacting with the Amazon cloud. We have implemented client side encryption code using C Sharp to transmit the part of data to *ESP*. On *ESP* side, decryption code is implemented to receive the ciphertext from users and extract the credentials required for further extensive encryption on behalf of user and finally share with cloud servers. Web services are developed using using C# and then deployed on the amazon cloud to perform these operation for proposed and existing scenarios in a distributed and secure manner. On client side, Javascript based encryption and decryption functions are also utilized during front end web page development that can be accessed using PCs, laptops and cell phones. In our case, we have opened our client side page at multiple devices ranging from 50 to 250 data requesters to initiate the request simultaneously. Moreover, the web services maintain record in MySQL database for *DO* to ensure reputation evaluation. In our scenario, number of attributes of data are also varied from 10 to 100. An android based web application is developed to act as *DR* and *DO/CC* to interact with the *ESP* and *DSP* by exploiting outsourced encryption and decryption. Trust values are also maintained by web services by receiving information regarding *DR*. We have compared our work with base schemes including CPE-ABE [36], OCCP [39] and OSCP [43].

A. REPUTATION EVALUATION

Figure 6 represents the impact of honest/dis-honest reporting from sensing reporters by increasing or decreasing in the value of reputation. Figure shows that system will response effectively with respect to the quality and honesty of *CC*. In Figure 6 there is rapid decrease in reputation due to dishonest contribution this can also lead to de-regeneration of *CC*. The graph does not show the quality of reporting but it indicates an urge for the *CC*s to report good of quality of data and discourage to report fake data to misguide the platform. On average for every new user, *R* score is assumed to be 0.5, that represents average expected quality at initial stage. Later on this value is calculated depending on the response of *DR* and on the history of previous tasks, here we have taken history with weights [0.2, 0.3, 0.5]. The maximum achievable *R* score is 1. The graph shows that *CC* will gets reward for quality reporting and would be punished by the decrease in reputation for fake reporting. In this way, the proposed reputation aware trust system offers fair dealing as well.

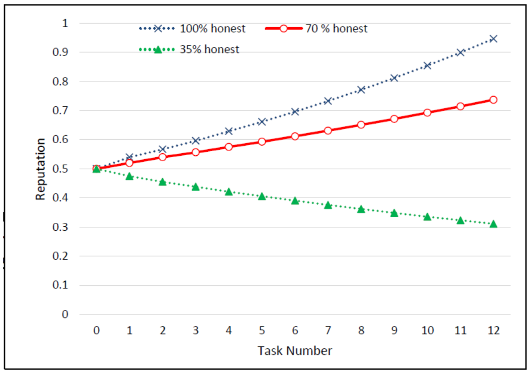
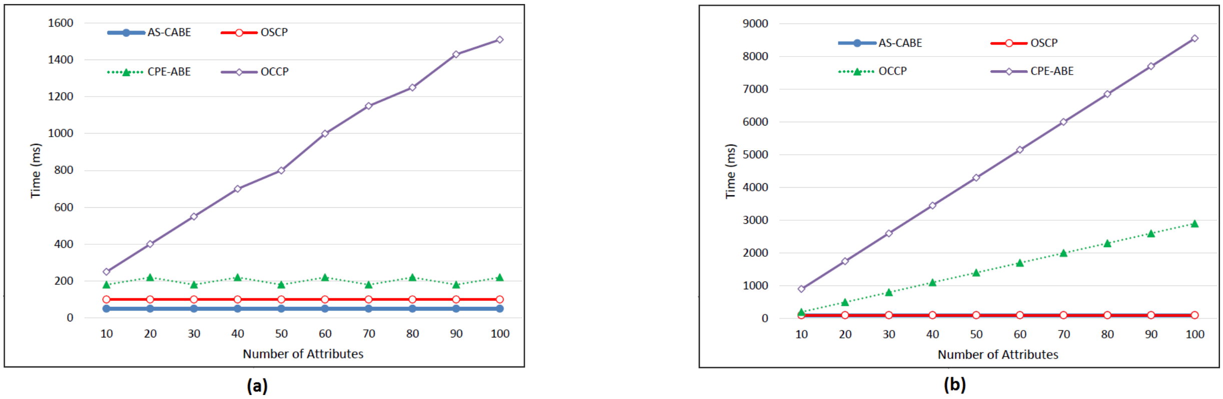


FIGURE 6. Reputation updation based on the completion of tasks.

B. ENCRYPTION AND DECRYPTION TIME

Figure 7(a) represents the time taken by one mobile device to encrypt the message in conventional approaches. In comparison with other approaches, our designed approach has constant computation time. This constant time is achieved mainly by outsourcing large amount of calculations to CSPs and *AS*s. Another reason of achieving constant computational time is that expensive bilinear pairing operation is outsourced as well. For the process of encryption, time taken by some of approaches from literature (OCCP, CPE-ABE) fluctuates. For example, when OCCP is considered there was exponential increase in the number of attributes such as for 70 attributes, 2000 ms were required and for CPE-ABE 6000 ms. OSCP [43] scheme is most similar to our proposed work's, when encryption part is concerned. In contrast to these approaches encryption time of our designed approach AS-CBAE remained constant. For example only 100 ms was taken for encryption at mobile node and all the other computations were done by the outsource entities. Figure 7(b) is showing the time required by the end node for the the process of decryption. Decryption process for previous techniques like (OCCP, CPE-ABE), time complexity increases linearly with the increase in the number of attributes. As it can be seen from the graphs that for 70 attributes OCCP needed 2000 ms and CPE-ABE required 6000 ms whereas for the decryption process OSCP [43] is almost same to the decryption process in AS-CABE, where decryption computational time remained constant. Same is the case with for 70 attributes, OCCP and CPE-ABE require 1150 ms and 180 ms respectively whereas AS-CABE requires constant time of 50 ms.



(a)

(b)

FIGURE 7. Impact of variations in number of attributes over (a) Encryption Time and (b) Decryption Time.

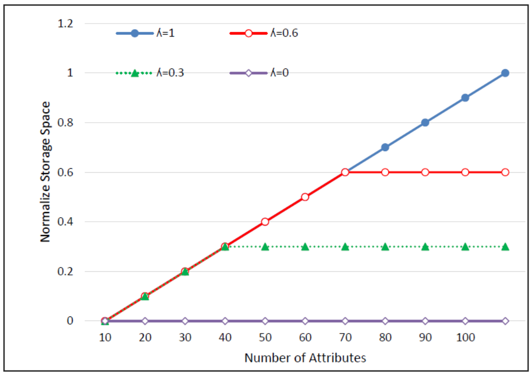


FIGURE 8. History size for different λ values.

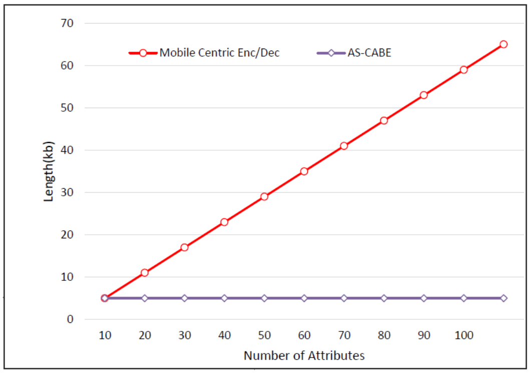


FIGURE 9. Effect of increase in number of attributes.

C. STORAGE OVERHEAD

Proposed scheme is efficient with respect to storage overhead. For end devices only legitimate computation is kept, which is expected not to require large storage space. Storage overhead is also very minimal for *DR*s as they are not required to save any information about *DO*s/*CC*s, because this is done by CSP. To save the storage space at CSP ageing factor in Phase-A is utilized which helped to reduce storage overhead as history is only maintained for limited number of *DO*s/*CC*s. As a result CSP just needs to consider effective history for selection of credible *CC*s/*DO*s. Figure 8. elucidates the effect of ageing factor when $\lambda = 0$, history is not maintained at all. Whereas when $\lambda = 1$, system keeps track of or store all the values and history size increases gradually for λ between 0 and 1, history is maintained upto certain size depending on value of λ. Both of the extreme situations are not favorable. For the case when history is not maintained at all, CSP cannot make assumptions on the expectation of tasks completion or on the quality. For the case when history is maintained for every performed task, time complexity increases exponential with the increase in *CC*s and tasks.

D. COMPUTATIONAL OVERHEAD

Computational complexity of *EU*s is reduced by getting services from CSP and typically in our proposed approach by

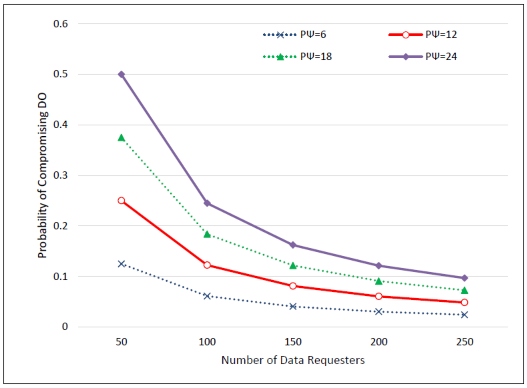
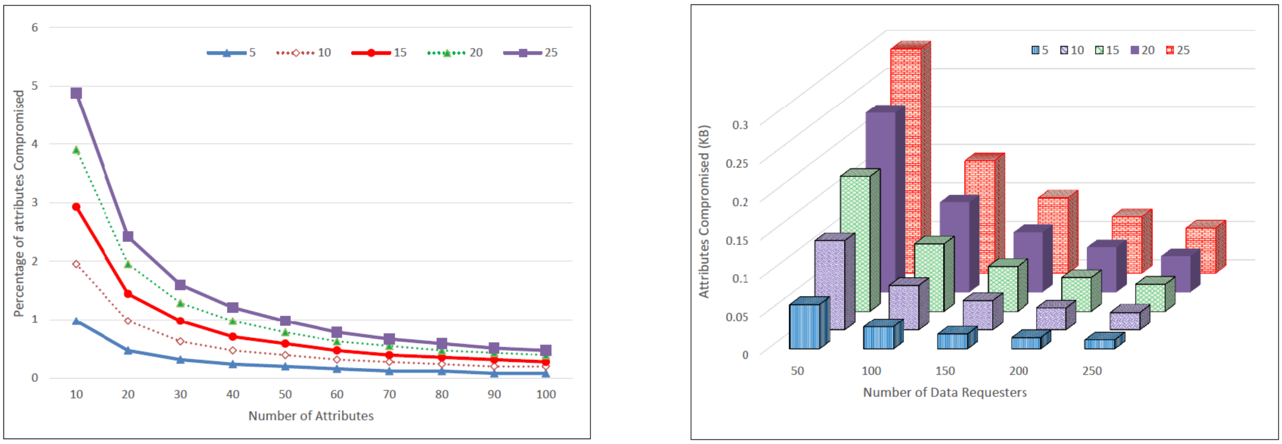


FIGURE 10. Probability of Compromising Data Requester.

*AS*s at both ends. Installation of *AS*s near end devices was due to the assumption of mobile devices. From the perspective of CSPs, scheme is efficient too, as taking the decision of *CC*s selection for data collection needs fix/certain portion of history to be traversed. So running time is low which also decreases response time/latency.

Proposed work has constant ciphertext length which can play it's part to reduce communication overhead. Critical part of computations is kept at end devices and only non-critical is transmitted to outsources, still due to need of frequent



(a)

(b)

FIGURE 11. Compromised nodes that cost fraction of communication to be compromised in (a) and by the compromised messages in (b).

communication for low power end devices it could be costly. To handle this almost every computation is assumed to be done by *AS*, *TA*, *CS*, and CSPs (*ESP*, *DSP*) so *DO*s and *DR*s can offload/generate complex tasks to these sources. Secure, anonymous and verifiable encryption/decryption is provided by the proposed approach. Figure 9 illustrates exponential increase in computational complexity with the increase in number of attributes at a mobile device. This was a drawback of some of the literature approaches in general, in which mobile devices were responsible for the enforcement of *AP*s. This was also one of the main disadvantages of CP-ABE based schemes in which mobile devices were responsible for the enforcement of *AP*s, same is the case with CP-ABE based schemes. In our scheme, it was done partly by outsources, computational complexity at mobile node is also constant as only the essential part of communication is done at the end node. For mobile devices there is negligible time overhead as most of the computations are done by CSPs. For the 50 number of attributes, the length in KB for the mobile centric encryption/decryption approaches in general is 30 KB. Whereas our proposed AS-CABE scheme consumes a constant amount and hence reduces the computational cost. The reason to achieve constant overhead is that most of the computations are performed at outsources and we have taken the average of multiple repetition.

E. RESILIENCE

As in the initialization phase, participants are required to send authentication requests. During the *DR*'s key establishment phase, attack can be launched to fetch the transmitted data. In this section we tried to cope this issue. The probability to be a compromised *DO* from total participants is presented below. The number of total participants or *DR*s is varied from 50 to 250. In (22), P_{DRC} is the probability that a *DO* is not compromised, where PS is the total number of participants and Ψ is indicating the number of participants that are compromised.

$$P_{DRC} = \frac{\binom{PS-3}{\Psi}}{\binom{PS-2}{\Psi}} \tag{22}$$

Term (*PS*-2) is presenting the two participants (sender and receiver) that are not among the compromised nodes. Whereas (*PS*-3) is the indication of *DO*, as a node if it is not considered to be compromised from the total set of nodes. In this scenario, we have to find the probability P_Ψ to predict that the *DO* is compromised. For this case, we have subtracted the probability of not compromising P_{DRC} from the total probability value of 1 that results in the remaining probability of *DO* being compromised, as given in (22).

$$P_\Psi = 1 - P_{DRC} = \frac{\Psi}{PS-2} \tag{23}$$

Due to exploitation of outsources, communication can be compromised with some fraction. Figure 10 illustrates the probability of compromising a *DO* varying as 0.040541, 0.081081, 0.121622 and 0.162162 when Ψ is varied from 6, 12, 18, and 24 respectively. If some intermediary node is compromised then adversary can get some data and other security related parameters from that device. Setup phase is secured as the presented scenario is distributed and security parameters are stored at different nodes. More than this, as the particular security credentials remained effective only for that session, so even if a node is compromised it will not affect the future communication.

Figure 11(a) elucidates the percentage when a certain number of attributes are compromised as 5 to 25 out of total attributes ranging from 10 to 100 for each *CC/DO*. For example, when there are 50 total attributes the percentages of compromised attributes are 0.195313, 0.390625, 0.585938, 0.78125 and 0.976563 when number of attributes compromised are 5,10,15,20 and 25 respectively. Similarly 11(b) represents the compromised message with the probability of 0.175781, 0.087891, 0.058594, 0.043945 and

0.0351563, when number of compromised attributes are varied from 10-25.

VIII. CONCLUSION

In MCC we deal with the scenario when a *DR* (Data Requester) requests some services from CSPs but concerned about disclosure of query details (like health matters and identity) and at last about authenticity of delivered information. In this scenario it is possible that a particular CSP does not have the required data or information to respond the request so need to get the data first from outsources (other CSPs, *CC*s/*DO*s). To be particular, we are dealing the case when outsource is a mobile device owner *DO/CC* (Data Owner/Crowd Contributor), who can contribute to data the collection process. These devices are well known for their limitations like: can not contribute legitimate information individually, have limited computational/storage power and at the same time also concerned about identity disclosure while being a participant (*DO/CC*). Reported data at CSP may not be trustworthy enough to deliver directly to *DR*. So the trust and privacy are the concerns of participants at both ends.

We have proposed a model with two phases: Phase-A deals with trust and Phase-B with privacy. Trust of *DR* is ensured by adopting and enhancing ''beta reputation'' to adjust with MCC scenario. To make contribution in data collection process, selection of *DO/CC* is done based on reputation maintained by CSP in Phase-A. Privacy is provided on both sides in Phase-B by outsourcing the complex CP-ABE operations, while keeping the critical but minimal computations at end devices. *AS*s are installed to provide anonymity by masking the participants identities and to shift most part of the complex computations from end devices. Concept of secure-shell is proposed between *AS*s and end devices to securely outsource the computations to/from *AS*s and end devices. Security analysis ensures that our proposed scheme is protected. DoS, correlational, collude and identity theft attacks are avoided. To validate our work, we have setup a testbed using web services on Amazon cloud and a mobile application for android phones to achieve *DSP*, *ESP* services for *DR* and *DR/CC*. Results explore the supremacy of our scheme in storage, trust, resilience, encryption and decryption time. In future, we shall analyze the annotations and semantic based relationship identification for the attributes in policy trees. We shall evaluate its impact for attribute based encryption and for identifying linkage for reputation as well. Further more, an efficient incentive mechanism in this domain can also be considered.

REFERENCES

[1] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," *Future Gener. Comput. Syst.*, vol. 29, no. 1, pp. 84–106, 2013.

[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Commun. Mobile Comput.*, vol. 13, no. 18, pp. 1587–1611, Dec. 2013.

[3] L. Ertaul, S. Singhal, and G. Saldamli, "Security challenges in cloud computing," in *Proc. Int. Conf. Secur. Manage.*, Las Vegas, NV, USA, 2010, pp. 36–42.

[4] J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, "A secure cloud-assisted urban data sharing framework for ubiquitous-cities," *Pervasive Mobile Comput.*, vol. 41, pp. 219–230, Oct. 2017.

[5] H. Lin, L. Xu, Y. Mu, and W. Wu, "A reliable recommendation and privacy-preserving based cross-layer reputation mechanism for mobile cloud computing," *Future Gener. Comput. Syst.*, vol. 52, pp. 125–136, Nov. 2015.

[6] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decis. Support Syst.*, vol. 43, no. 2, pp. 618–644, 2007.

[7] C. Zhu, H. Wang, X. Liu, L. Shu, L. T. Yang, and V. C. M. Leung, "A novel sensory data processing framework to integrate sensor networks with mobile cloud," *IEEE Syst. J.*, vol. 10, no. 3, pp. 1125–1136, Sep. 2016.

[8] T. Luo and L. Zeynalvand, "Reshaping mobile crowd sensing using cross validation to improve data credibility," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Singapore, Dec. 2017, pp. 1–7.

[9] D. Zhao, X.-Y. Li, and H. Ma, "Budget-feasible online incentive mechanisms for crowdsourcing tasks truthfully," *IEEE/ACM Trans. Netw.*, vol. 24, no. 2, pp. 647–661, Apr. 2016.

[10] A. Jøsang and R. Ismail, "The beta reputation system," in *Proc. 15th Bled Electron. Commerce Conf.*, vol. 5, 2002, pp. 2502–2511.

[11] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *Proc. 2nd Theory Cryptogr. Conf.*, 2005, pp. 325–341.

[12] M. Chiregi and N. J. Navimipour, "A new method for trust and reputation evaluation in the cloud environments using the recommendations of opinion leaders' entities and removing the effect of troll entities," *Comput. Hum. Behav.*, vol. 60, pp. 280–292, Jul. 2016.

[13] J. Guo, R. Chen, and J. J. P. Tsai, "A survey of trust computation models for service management in Internet of Things systems," *Comput. Commun.*, vol. 97, pp. 1–14, Jan. 2017.

[14] S. Ozdemir, "Functional reputation based reliable data aggregation and transmission for wireless sensor networks," *Comput. Commun.*, vol. 31, no. 17, pp. 3941–3953, 2008.

[15] M. Pouryazdan, B. Kantarci, T. Soyata, L. Foschini, and H. Song, "Quantifying user reputation scores, data trustworthiness, and user incentives in mobile crowd-sensing," *IEEE Access*, vol. 5, pp. 1382–1397, 2017.

[16] M. Chiregi and N. J. Navimipour, "Cloud computing and trust evaluation: A systematic literature review of the state-of-the-art mechanisms," *J. Elect. Syst. Inf. Technol.*, to be published, doi: 10.1016/j.jesit.2017.09.001.

[17] V. V. Rajendran and S. Swamynathan, "Hybrid model for dynamic evaluation of trust in cloud services," *Wireless Netw.*, vol. 22, no. 6, pp. 1807–1818, 2016.

[18] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for VM-based cloudlets in mobile computing," *IEEE Pervasive Comput.*, vol. 8, no. 4, pp. 14–23, Oct./Dec. 2009.

[19] N. Aminzadeh, Z. Sanaei, and S. H. A. Hamid, "Mobile storage augmentation in mobile cloud computing: Taxonomy, approaches, and open issues," *Simul. Model. Pract. Theory*, vol. 50, pp. 96–108, Jan. 2015.

[20] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *J. Netw. Comput. Appl.*, vol. 84, pp. 38–54, Apr. 2017.

[21] M. Hussain and B. M. Almourad, "Trust in mobile cloud computing with LTE-based deployment," in *Proc. IEEE 11th Int. Conf. Ubiquitous Intell. Comput. IEEE 11th Int. Conf. Auton. Trusted Comput. IEEE 14th Int. Conf Scalable Comput. Commun. Assoc. Workshops (UTC-ATC-ScalCom)*, Dec. 2014, pp. 643–648.

[22] H. Takabi, S. T. Zargar, and J. B. D. Joshi, "Mobile cloud computing and its security, privacy and trust management challenges," in *Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications*, vol. 9, D. B. Rawat, B. B. Bista, and G. Yan, Ed. Hershey, PA, USA: IGI Global, 2014, p. 22.

[23] Y. Zhang, D. Zheng, X. Chen, J. Li, and H. Li, "Efficient attribute-based data sharing in mobile clouds," *Pervasive Mobile Comput.*, vol. 28, pp. 135–149, Jun. 2016.

[24] X. Chen, M. Liu, Y. Zhou, Z. Li, S. Chen, and X. He, "A truthful incentive mechanism for online recruitment in mobile crowd sensing system," *Sensors*, vol. 17, no. 1, pp. 1–79, 2017.

[25] X. Zhang, Z. Yang, Y. Liu, J. Li, and Z. Ming, "Toward efficient mechanisms for mobile crowdsensing," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1760–1771, Feb. 2017.

[26] D. Yang, G. Xue, X. Fang, and J. Tang, "Crowdsourcing to smartphones: Incentive mechanism design for mobile phone sensing," in *Proc. Mobicom*, 2012, pp. 173–184.

[27] D. Peng, F. Wu, and G. Chen, "Data quality guided incentive mechanism design for crowdsensing," *IEEE Trans. Mobile Comput.*, vol. 17, no. 2, pp. 307–319, Feb. 2018.

[28] M. Pouryazdan, B. Kantarci, T. Soyata, and H. Song, "Anchor-assisted and vote-based trustworthiness assurance in smart city crowdsensing," *IEEE Access*, vol. 4, pp. 529–541, 2016.

[29] T. Zhou, Z. Cai, K. Wu, Y. Chen, and M. Xu, "FIDC: A framework for improving data credibility in mobile crowdsensing," *Comput. Netw.*, vol. 120, pp. 157–169, Jun. 2017.

[30] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, Jan. 2017.

[31] X. Zheng, Z. Cai, J. Yu, C. Wang, and Y. Li, "Follow but no track: Privacy preserved profile publishing in cyber-physical social systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1868–1878, Dec. 2017.

[32] TZ. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 4, pp. 577–590, Jul./Aug. 2016.

[33] Z. He, Z. Cai, and J. Yu, "Latent-data privacy preserving with customized data utility for social network data," *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 665–673, Jan. 2018.

[34] G. Drosatos, P. S. Efraimidis, I. N. Athanasiadis, M. Stevens, and E. D'Hondt, "Privacy-preserving computation of participatory noise maps in the cloud," *J. Syst. Softw.*, vol. 92, no. 1, pp. 170–183, 2014.

[35] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.

[36] H. Wang, D. He, J. Shen, Z. Zheng, C. Zhao, and M. Zhao, "Verifiable outsourced ciphertext-policy attribute-based encryption in cloud computing," *Soft Comput.*, vol. 21, no. 4, pp. 7325–7335, 2016.

[37] D. Papamartzivanos, D. Damopoulos, and G. Kambourakis, "A cloud-based architecture to crowdsource mobile app privacy leaks," in *Proc. 18th Panhellenic Conf. Inform.*, 2014, pp. 1–6.

[38] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2005, pp. 457–473.

[39] J. Li, F. Sha, Y. Zhang, X. Huang, and J. Shen, "Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length," *Secure Commun. Netw.*, vol. 2017, Jan. 2017, Art. no. 3596205.

[40] Z. Zhou and D. Huang, "Efficient and secure data storage operations for mobile cloud computing," in *Proc. 8th Int. Conf. Netw. Service Manage.*, 2012, pp. 37–45.

[41] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 8, pp. 2201–2210, Aug. 2014.

[42] J. B. Abdo, T. Bourgeau, J. Demerjian, and H. Chaouchi, "Extended privacy in crowdsourced location-based services using mobile cloud computing," *Mobile Inf. Syst.*, vol. 2016, Jun. 2016, Art. no. 7867206.

[43] Z. Zhao and J. Wang, "Verifiable outsourced ciphertext-policy attribute-based encryption for mobile cloud computing," *KSII Trans. Internet Inf. Syst.*, vol. 11, no. 6, pp. 3254–3272, 2017.

[44] W. Ahmad, S. Wang, and Z. Mahmood, "Outsourced ciphertext-policy based privacy preservation for mobile cloud computing," *Procedia Comput. Sci.*, vol. 129, pp. 128–134, Dec. 2018.

WAQAS AHMAD received the B.S. degree in computer science from the University of Azad Jammu and Kashmir, Pakistan, in 2009, and the M.S. degree in computer science from International Islamic University at Islamabad, Islamabad, Pakistan, in 2012. He is currently pursuing the Ph.D. degree with Beijing Normal University, Beijing, China. From 2013 to 2015, he was a visiting faculty member in different institutions in Pakistan. His areas of interest are game theory, mechanism design, crowd sourcing, privacy preservation in mobile cloud computing, and mobile crowd sensing.

SHENGLING WANG received the Ph.D. degree from Xi'an Jiaotong University in 2008. After that, she did her post-doctoral research with the Department of Computer Science and Technology, Tsinghua University. Then, she was an Assistant Professor and an Associate Professor with the Institute of Computing Technology, Chinese Academy of Sciences, from 2010 to 2013. She is currently an Associate Professor with the College of Information Science and Technology, Beijing Normal University. She has published about 40 papers, including many international top journals or magazines, such as JSAC, TON, TPDS, the IEEE Wireless Communications, and the IEEE Network.

ATA ULLAH received the B.S. and M.S. degrees in computer science from COMSATS University Islamabad, Pakistan, in 2005 and 2007, respectively, and the Ph.D. degree in computer science from IIUI, Pakistan, in 2016, in the area of wireless network security. From 2007 to 2008, he was a Software Engineer with Streaming Networks, Islamabad. He joined NUML, Islamabad, in 2008, where he was an Assistant Professor/Head Project Committee Member of the Department of Computer Science until 2017. He remained faculty partner for the industrial collaboration in software development. He has been a Research Fellow with the School of Computer and Communication Engineering, University of Science and Technology Beijing, China, since 2017. He has published several papers in peer-reviewed ISI indexed impact factor journals and international conferences. He has programming expertise in C, C#, Java, PHP, and NS2. His areas of interests are WSN, IoT, cyber physical social thinking space, health-services, NGN, VoIP, and their security solutions. He has supervised 110 projects at under graduate level and won one international and 45 national-level software competitions. He received ICT funding for the development of projects. He is also a reviewer and a guest editor for conference and journal publications.

SHEHARYAR received the B.S. degree from the National University of Science and Technology, Islamabad, Pakistan, in 2014. He is currently pursuing the M.S. degree in computer science with the College of Information Science and Technology, Beijing Normal University, Beijing, China. His major research areas are machine learning and pattern recognition.

ZAHID MAHMOOD received the B.S. degree from the University of Baluchistan, Quetta, and the M.S. degree in computer sciences from International Islamic University, Islamabad, Pakistan, in 2007 and 2012, respectively, and the Ph.D. degree from the Beijing University of Science and Technology, Beijing, China. He was with International Islamic University, Islamabad. After that, he joined Mohi-ud-Din Islamic University, Nerian Sharif, as a Lecturer, until 2014. His major research areas are key management techniques in wireless sensor networks and lightweight cryptography techniques for Internet of Things, authentication, privacy, and secure communication for wearable devices.