IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON HEALTHCARE INFORMATION TECHNOLOGY FOR THE EXTREME AND REMOTE ENVIRONMENTS

Received March 15, 2019, accepted March 29, 2019, date of publication April 2, 2019, date of current version April 15, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2908664

Privacy Ensured *e*-Healthcare for Fog-Enhanced IoT Based Applications

RAHUL SAHA[1], (Member, IEEE), GULSHAN KUMAR[1], (Member, IEEE), MRITUNJAY KUMAR RAI[2], REJI THOMAS[3], AND SE-JUNG LIM[4]

[1]School of Computer Science and Engineering, Lovely Professional University, Phagwara 144 411, India
[2]School of Electronics and Communication Engineering, Lovely Professional University, Phagwara 144 411, India
[3]Division of Research and Development, Lovely Professional University, Phagwara 144 411, India
[4]Honam University, Gwangju 62399, South Korea

Corresponding authors: Gulshan Kumar (gulshan3971@gmail.com) and Se-Jung Lim (limsejung@korea.ac.kr)

ABSTRACT The progress in network technology and hardware in conjunction with the Internet-of-Things (IoTs) has provided the comfortability for an easier human life at present. Apart from the so-called ''smart'' environments, including smart homes, smart city, smart agriculture, IoTs have been included recently in e-healthcare systems as well for real-time diagnosis and medical consultancy. To enhance the capabilities of IoT-based healthcare systems, fog layers have been employed and that have shown its worth by providing fast response time and low latency. However, such development is posing a severe challenge in preserving the privacy of the users which further addresses the security/privacy issues to some extent. Being in an infant stage, such technology has invariably run into fewer privacy controls. Therefore, our present work is about an *e*-healthcare framework dealing with electronic medical records (EMRs) which preserves the privacy issues. Moreover, we have experimented the proposed work with respect to response time and delay and have compared with recent works. The results show that the proposed work is efficient in providing privacy along with standard network parameters.

INDEX TERMS Privacy, fog, healthcare, IoT, framework, consensus, view, access control.

I. INTRODUCTION

Advanced networking and fast-growing digital processing technologies have paved the way for the emergence of various online services. Such services use Internet of Things (IoTs) as medium to connect with people, process and things, thus ensuring more comfort to social life of humans [1]–[3]. These online services have shifted technologists and researchers from centralized environment to more distributed one. As a result, smart wearables, smart home, smart mobility, smart cities and even smart healthcare have been emerging at present [2]. Consequently, current internet technology undoubtedly has been enhanced to data technology for the proliferation of smart devices, and that generates huge amount of data. Cisco, Google, Amazon, Microsoft and many other leading Information Technology (IT) companies have already deployed cloud Data Centres (DC) to store and compute the data generated by various applications and services on a paid-usage model basis [4]. Though the model is successful as per the usage, but it is only applicable for latency tolerant devices and is not best suit for real time applications. With the present pace and accumulation of data, forecast of 92% data workload in the coming years is predicted and that have urged the deployment of a control layer for Fog Computing (FC) near the end-devices to support mobility and data locality [4], [5]. In fact, the term 'Fog Computing' has been introduced by Cisco in 2012 and this domain is receiving good attention for various applications by researchers, academia and industries. The main idea for deploying FC is to take advantage of the end devices, at the edge, rich in various resources including storage, compute, and bandwidth to process the real-time data of neighbouring nodes in one-hop manner to reduce the latency [1], [6]. The Cloud and Fog are interdependent and mutually beneficial. It is proved beyond doubt that cloud coordinates with the fog nodes can handle heavyweight data. For comparison, the delay-sensitive data are processed by fog nodes in the proximity of the IoT end devices.

As we have discussed earlier, IoTs have opened the door of many applications and e-health application is one

The associate editor coordinating the review of this manuscript and approving it for publication was Tai-Hoon Kim.

among them that recently has received immense interest of the researchers [7]. An e-health system is nothing, but a radio-frequency based wireless networking technology that uses ubiquitous functionalities. Various tiny sensor nodes and actuators are placed around the human body and are interconnected to accumulate data. The real-time data generated by these sensors and actuators are stored and used by the physicians or medical consultants in real time. For example, world's first tele-robotic surgery is performed on the patient from a remote location using robotically controlled instruments in India [8]. Medical and pharmaceutical researchers may also require the patient data for research tasks. The recent advances in cloud-fog-edge technologies are further enhancing the capabilities of such e-healthcare services. However, storing and retrieving such sensitive health records, also called as 'Electronic Medical Record (EMR)' from clouds impose severe privacy concern, especially on the identity of patients [9]–[11].

The privacy is of four types; i) privacy of personal information also referred as data privacy, ii) privacy of personal behaviour, iii) privacy of personal communication and iii) privacy of the person [12]. The privacy of EMRs in clouds can be compromised accidentally or deliberately and hence the disclosure of data is respectively beneficial for the attacker and harmful for the user. Various methods have been considered to solve the issue of privacy in clouds. Encryption techniques, trusted computing, efficient private information retrieval, intention hiding techniques are the few tested methods [13], [14]. But with the abundance of data, the processes are getting mis-managed due to cost factors, limitation of query support, computation overhead, improper key usage. Therefore, the development of a mechanism that can be used for accessing the EMRs without jeopardising the privacy or identities with a proper access control method is the need of the hour.

II. RELATED WORK

As fog computing and its privacy concerns in e-healthcare are at infancy, a concise literature survey on the privacy preservation in fog-cloud environments extended with IoTs is discussed in this section. To preserve, anonymity and privacy, a data aggregation approach is initially considered [14]. In this approach, anonymity and authenticity of the devices are ensured first by pseudonym and pseudonym-certificate. A local certification authority has been used by fogs at the network edge to manage pseudonym tasks and data aggregation is generally done by Paillier algorithm. However, multilayer authentication process increases the latency which is a bottleneck for this approach. Further, as Paillier algorithm allows multiplication of encrypted values, under some restriction an untrusted party can homomorphically evaluate a circuit that entails multiplication under some threshold value. Another scheme providing integrity and privacy for data storage in fog-to-cloud based IoTs is public auditing approach [15]. In this scheme, bilinear mapping technique is used for converting the tags generated by mobile sinks to the ones used by the fog nodes in the phase of proof generation. Experimental results show that the scheme protects privacy and reduces the communication and computational costs in the verification phase. Zero-knowledge proof mechanism is used to verify the integrity of IoTs' data from various sources. Slow computation and requirement of additional machinery are the drawbacks of this method. Also, the bilinear mapping leads to undesired homomorphic encryption. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is the third approach and that provide security and privacy for the orchestration and delivery of IoT based services [16]. It is proved to be advantageous by reducing the latency of the service access, but ABE methods suffer from problems including non-existence of attribute revocation, key coordination and key escrow. Another scheme for e-health privacy is the 'fusion approach' [17]. In this approach authentication is performed between patient and medical nodes using IoT group key in encrypted format. The designed match based policy update mechanism enables flexible access policy updating without privacy leakage. The main drawback of this approach is that when a comprised patient or a spoofing process has been initiated with a query, the update mechanism in server retrieves the queries of the patients with health records. A more recent approach has considered the privacy concerns in healthcare using cloud and IoTs framework differently [18]. The concerns are included at the user level, application model and even intermediate results.

Various techniques are employed for the privacy in e-healthcare are reviewed recently [19] The pairwise key establishment, multibiometric key generation, hash function, chaotic maps, attribute-based encryption, hybrid encryption, Number Theory, Dynamic Probability Packet Marking, Tri-Mode Algorithm and Priority-Based Data Forwarding are the available techniques at present [19]–[22]. A real-time oriented hybrid privacy preserving clinical decision support system (HPCS) in conjunction with fog-cloud interface is also emerged [23]. The framework includes a fog server that uses a lightweight data mining method. A new secure outsourced inner-product protocol for achieving secure lightweight single-layer neural network is used in the work. For privacy, piecewise polynomial calculation protocol is used by cloud server to securely perform any activation functions in multiple-layer neural network. Another new protocol called privacy-preserving fraction approximation protocol is also used to solve the computation overflow problem. A privacy-preserving deduplication protocol with ownership management in fog computing is an interesting approach [24]. It uses user-level key management and update mechanisms to achieve the access control. Data-invariant user-level private keys are used by the data owners with a constant number of keys without considering the number of outsourced data files. The user-level public keys are updated at the remote storage which reduces communication overhead but generates the risk propagation for man-in-the-middle attacks. The OpenIoT platform with multiple IoT-cloud data is an earlier framework [25]. End-to-end security provisioning has been

obtained through homomorphic encryption and authentication process. Slow computation is a problem in this process. A secure sharing of health data is also available these days [26]. The work uses AES algorithm in conjunction with Elliptic cryptosystems. The confidentiality of the health records is ensured but the privacy and reliability are the points of question. Bio-cryptography based technique can also provide users' the privacy they are looking for [27].

Now it is very clear there exist some serious shortcomings with e-healthcare. Therefore, there is a requirement to develop a mechanism to preserve the privacy for medical records in e-healthcare systems attached with cloud-fog-edge architecture in IoT applications. The proposed framework discussed in the present article uses:

1) Data aggregator at the fog level to restrict the authentication point to one - reduce communication overhead at each level.
2) Elliptic cryptographic approach - ensure confidentiality.
3) Consensus algorithm - enhance reliability and trust in the EMR transactions.

We have considered privacy issues as our problem definition and have provided suitable solution for them. The rest of the paper has been organized as follows. Section 3 describes the proposed framework with system model and analyses the privacy of the proposed system. Section 4 shows the experimental results and Section 5 concludes the paper.

III. PROPOSED APPROACH

The proposed framework in the present work addresses the privacy issues in e-healthcare. The framework uses various end-user devices such as health monitoring systems, mobile devices and laptops, a layer of fog comprised of fog accumulators as data aggregators, fog devices such as access points, servers, switches and routers and cloud servers. The architecture used for the study is shown in Figure-1. The layer of fog is also conjugated with query handler, key centre and identity verifying manager.

The specific functioning of each modules are as follows.

Fog Accumulator: All the data from the fog nodes are aggregated by the fog accumulator and then outsourced to the public cloud. The cache in fog accumulator helps in reducing the latency.

Key Centre: Key Centre is responsible for generation and verification of keys.

Query Handler: Handles and responses with a query which is beyond a specific view request.

Identity Manager: Maps the identity to a pseudo-identity to hide the patient details as required.

The basic functioning of the proposed framework with all its modules is explained herewith. Edge devices or terminal devices gather data (EMRs) from patients and submit them to the identity manager. The identity manager then maps the patient details with pseudo-identity and store them in the cloud servers. In the basic architecture, each device executes a cryptographic exchange that ensures the security of

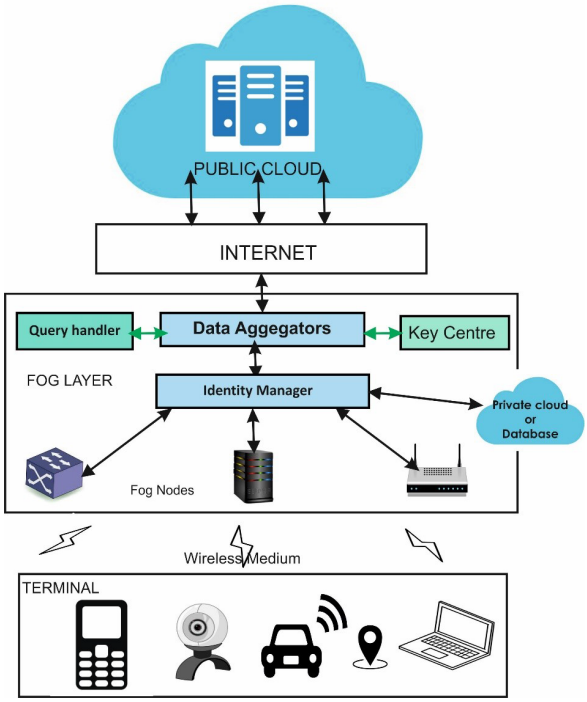

FIGURE 1. Proposed framework for the privacy ensured e-healthcare network.

these services. However, in this proposed approach we have additionally included a fog accumulator layer as a check point before sending data to cloud. Also, in this modified process, two more modules are added in the framework: a key centre and a query handler. The generated EMRs must have individual identity which are mapped with a pseudo-identity generated by the identity manager and stored in private cloud server rather than public one. Along with the identities, when any fog device request for any service in or from cloud through fog accumulator, the key centre provides security keys for cryptographic processes such as authentication, confidentiality, integrity and non-repudiation. Further, a consensus protocol is also executed to obtain a logical decision/conclusion about the view of the requested EMRs. The above said approach provides the following benefits.

1) Single point of cryptographic exchange for privacy preservation of EMRs.
2) Consensus to agree to control the view of EMRs.
3) Query handler handles the queries based upon the consensus to access the view of EMRs.

A. SYSTEM MODEL

In this sub-section, a system model used for the experimentation is described. However, following assumptions were considered during entire process.

- The data aggregator device is secure and trusted with enabled intrusion detection process.
- Identity Manager module is working in conjunction with private cloud to protect the identities of the EMR.

- Cloud servers are trusted and secured with shared public key of the server with fog accumulator.

Additionally, the model functions are categorized into different phases and is explained in the following sub-sections.

1) IDENTITY MANAGEMENT PHASE

This phase deals with the mapping of original identity of an EMR such as patient name, address, contact, GPS location and other personal information. In this mapping process, a token is generated first by parsing the EMRs with an EMR parser and relevant personal information are segregated and abstracted with lightweight mapping technique. Subsequently, an attribute-based encryption is used and a public key pub_str is derived by the hash (SHA-512) on the parsed information of EMR concatenated with timestamp str. The output token is generated by applying Elliptic Curve Cryptography [28] with EMR and pub_{str}. The token T_{EMR_i} is made available for public access as required. The process is summarized in Algorithm-1 and is executed by the private cloud servers only. For any purpose or to update any information, if decryption is required, we follow the decryption method shown in Algorithm 2, where pv_{str} is the private key for decryption.

Algorithm 1 Identity Token Generation

Input EMR
Output Mapped token T_{EMR_i}

1: str = [parsed(EMR) || timestamp]
2: pub_{str} = SHA - 512(str)
3: T_{EMR_i} = ECCEncrypt (EMR, pub_{str})

Algorithm 2 Token Decryption

Input T_{EMR_i}
Output EMR

1: $pv_{str} = \sum_{i=1}^{n} h_i\,(str)str_i$
2: EMR = ECCDecrypt(T_{EMR_i}, pv_{str})

2) KEY DISTRIBUTION PHASE

The keys going to be discussed here is not the same mentioned in the preceding phase. Previous keys are only for storing the EMRs in the private clouds by the heterogeneous sensors where original identities are tokenized. These keys are utilized by the public cloud servers or service providers and the file requester. Whenever, a user is requesting for an EMR, Cloud Service Providers (CSPs) must provide them a public key for the access of the required data and is provided after the verification from Key Centre. The user first sends a Request message (REQ) with its identity {REQ,u_i}. Data aggregator forwards the request to Key Centre (KC) along with its own certificate d_{i_cert}. and KC responses back with public-private key pair {$u_{i_{pu}}$ $u_{i_{pr}}$} of u_i. Data aggregator then responds back to the user as: {REQ_i^{ACK}, $u_{i_{pu}}$, $u_{i_{pr}}$ }. Next, the user sends a message containing the EMR to be accessed and the user's certificate by generating a random nonce and encrypting it with the private key $u_{i_{pr}}$. On receiving and verifying the certificate, the EMR, the corresponding transactions of the EMR and the new public key of the new request are sent for the consensus process. Figure-2 shows the process in summary with the help of sequence diagram.

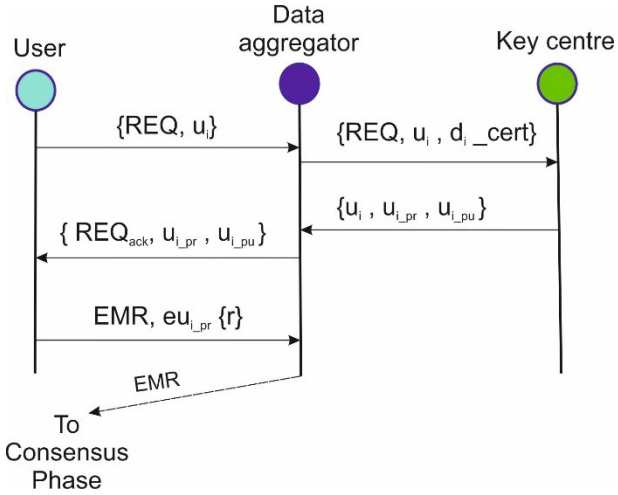

FIGURE 2. Sequence diagram for key distribution phase.

3) CONSENSUS PHASE AND VIEW ACCESS

Consensus is performed by the data aggregators in the network. When the data aggregator receives request of EMR, all the transactions corresponding to that EMR and EMR containing CSP are verified and validated using the Paxos consensus [29]. Use of Paxos ensures durability of the storage as it requires replication. Once the validation is successful, the data aggregator that receives the EMR request sends a SUCCESS message to the public CSP. Data aggregator then records the message and update its database or private cloud accordingly. Once the consensus is a success, the query handler parses the requested query and checks for its sanity and role of the user. Depending upon its verification, view of the EMR is determined and data aggregator sends back the requested EMR as response in an encrypted form with the public key $u_{i_{pu}}$. For this process, a query handler is pre-configured with role-based access control [30] and query parsing technique [31], [32].

B. PRIVACY ANALYSIS

The privacy and robustness against the threats are of outmost importance for e-healthcare systems with network employing cloud-fog interface. The present model uses LINDDUN framework for privacy analysis [33]. This framework negotiate any network born threats targeting the privacy of the data during storage or transmission. In this section, how the proposed model robust against threats is explained, in terms of linkability, identifiability, non-repudiation, detectability, information disclosure,content unawareness, and Policy and Consent Noncompliance. A brief description about these seven points are given below

TABLE 1. Implementation metrics.

Consensus protocol	Paxos
Geographic distribution of nodes	Campus area network (CAN) environment, 10 nodes
Hardware environment of all peers	3.3 GHz, 16 GB RAM, Octa-core, 2 TB HDD
Network model	We implemented with three firewalls, three access points, 10 routers
Number of nodes involved in the test transaction.	5
Test tools and framework	Hyperledger composer (smoke tests)
Type of data store used	CouchDB

- *Linkability:* An adversary may attempt to distinguish whether two or more EMRs such as blood report, heart monitoring data and other medical data are related to the same user. It may also try to correlate those sensitive information and infer a logical access provisions for the user who has accessed the service with a device at a particular location, thus reveals the habits of the patient. Therefore, unlinkability need to be guaranteed in this kind of information processing. The proposed model ensures a solution by introducing 'unlinkability' with pseudo-identity and view based access.
- *Identifiability:* An adversary may attempt to correlate and identify a patient from the types of messages or EMRs retrieved or exchanged. Thus, the introduced pseudo-identity and identity token in the model preserves 'identifiability' in the proposed approach.
- *Non-repudiation:* Non-repudiation can be used preserve patients' privacy. An adversary may attempt to collect EMRs stored and exchanged within the cloud-fog infrastructure and be able to infer some information about a patient or patients' habit or medical consultancies. Therefore, 'non-repudiation' is done by using the signatures in the proposed work.
- *Detectability:* An adversary may tend to correlate and infer statistics about the type of EMRs with the messages exchanged amongst CSPs entities. For instance, an adversary detects to identify the timing factors for heart patient when the monitoring system continuously sends monitored data to the private health cloud. Therefore, the patients' undetectability and unobservability must be guaranteed by the system. The proposed approach ensures these by using cryptographic processes with ECC.
- *Information disclosure:* An adversary may eavesdrop and passively collect information exchanged within the infrastructure aiming at profiling patients which may lead to disrupting the location privacy and/or personal data for dynamic health monitoring systems. These data are further used for inferring the patients' health records and patients' activities by analysing the history of service access from the device. In this way profiling causes a potential risk for the patents' privacy. Thus, confidentiality of information must be ensured. The proposed approach uses pseudo-identity, cryptographic procedures and consensus to control the access of the requested data.
- *Content Unawareness:* A compromised or misbehaving data requester or CSP may try to gather more patient information than it is necessary. Hence, the content awareness of patients is a requirement of the framework. The proposed privacy framework ensures this by using the role-based access control mechanism on the requester and view consensus before granting the access.
- *Policy and Consent Noncompliance:* A compromised CSP may try to obtain sensitive information about users such as their device controls and location. It may also use such information with data brokers for economic advantages without users' consent, and can even access the personal data stored on a health monitoring device such mobile-based health monitoring applications. The proposed framework provides solution by using proper cryptographic mechanism and identity hidden mechanism with identity token.

TABLE 2. Average EMR Transaction time (milliseconds).

No. of EMRs	Masood et. al. [20]	Menaka et. al. [26]	Omotosho et. al. [27]	Proposed Approach
100	20.433	20.133	23.500	18.543
200	20.633	22.500	25.667	19.023
300	23.176	24.017	26.333	21.777
400	24.500	27.433	26.919	21.500
500	24.337	27.237	27.000	22.334
600	25.474	31.717	28.133	23.003
700	26.333	32.333	29.500	25.933
800	28.777	35.767	30.377	27.333
900	30.011	37.000	31.808	27.886
1000	32.500	39.977	32.617	29.717
Time Complexity	O(n2) + O(C)	O(n2) + O(C)	O(n) × O(C) × O(n logn)	O(n) + O(C) + O(d)
n is the number of EMRs and C is the cryptographic timings, d is the data aggregators consensus time				

IV. RESULTS AND DISCUSSION

The aforementioned model is tested in practical scenario involving cloud-fog infrastructure in the network for e-healthcare services and is discussed in this section. A Paxos consensus is implemented with the hyperledger composer. A SQL data querying system is also used for the convenience

TABLE 3. Comparison of features.

	Data aggregator	View controller	Consensus	Unlink-ability	Non-identifiability	Non-repudiation	Undetect-ability	Information non-disclosure	Content unawareness	Comp-liance
Masood et. al. [20]	no	no	no	yes	no	yes	no	yes	no	yes
Menaka et. al. [26]	no	no	no	no	no	yes	no	yes	no	no
Omotosho et. al. [27]	no	no	no	no	no	yes	no	yes	no	yes
Proposed Approach	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes

of query parsing. The implementation parameters are shown in Table-1.

The results obtained using proposed model are compared with the other recent works described in [20], [26], [27]. For that performances are analysed in two basic measurable aspects: time consumption and memory consumption. For Paxos to be implemented, 1 TB of memory is used in overall with L1-L2 cache for the experimentation. The use of cache helps the data aggregators to reach consensus with the minimum delay. The delay in EMR transactions are measured in milliseconds and is shown in Figure-3. Average time of EMR transactions are shown in Table-2. Time complexity is also shown in the last row of the table. In this work all experiments are performed for all the algorithms with 1000 EMRs.

The results depicted in the Table-2 shows that the proposed work is having significantly less transaction time which is statistically 13.84% less as compared to other algorithms shown in comparison. This effect is due to the one-point cryptographic exchange with data aggregators in the fog-enhanced framework. The comparison results shown in Figure-3 shows reduced delay which is approximately 23.6% with the proposed algorithm. If one correlates the data of average EMR transmission and overall delay, the delay is almost twice due to multiple cryptographic exchanges between nodal points in other algorithms. In the proposed work, only one-time signature exchange is done which make the overall process less time consuming and hence faster processing of information can be achieved. A new parameter is introduced and compared to view utilization ratio with number of queries handled by the algorithms within a specific time duration. The parameter has been defined as:

$$\text{Query View Ratio (QVR)}\% = \frac{No.\ of\ allowed\ queries\ of\ EMR}{Total\ number\ of\ queries\ for\ EMR} \times 100$$

QVR values are measured for all the algorithms and have identified that the other algorithms possess almost 100% QVR whereas the proposed approach QVR is much less. This interesting result emphasizes the usage of consensus. This approach controls the access view of the EMRs and therefore obtaining less QVR. This less QVR also becomes advantageous with regards to privacy. The result is shown in Figure-4 and further signifies the working functionality of the query handler in the framework.

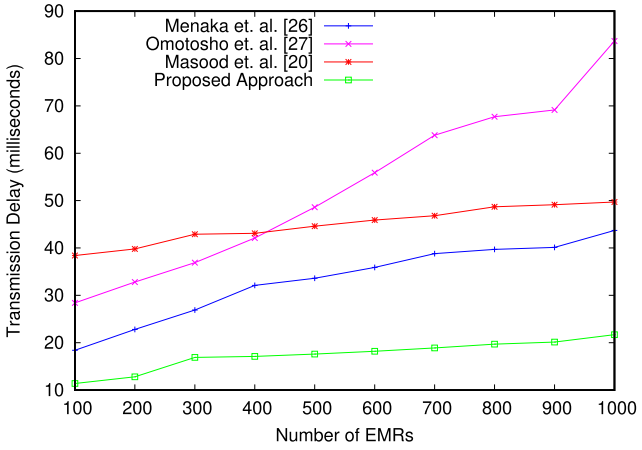

FIGURE 3. Comparison of time delay.

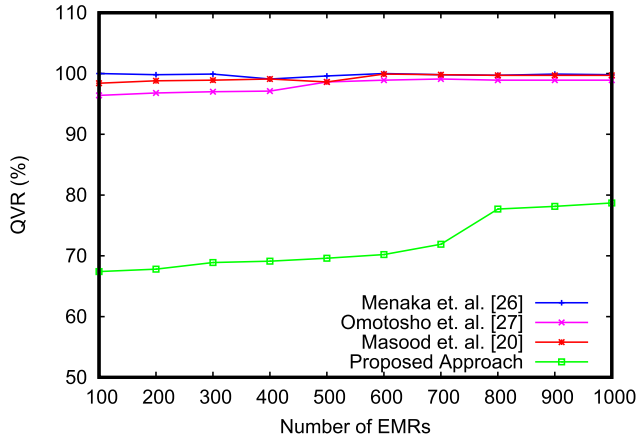

FIGURE 4. Comparison of query view ratio.

Finally, we have compared the features of the proposed work with the other algorithms and the summarization has been provided in Table-3. The comparison signifies that the proposed approach is efficient and possess the required features for any cloud-fog based e-healthcare.

V. CONCLUSION

The applicability of IoT and its related cloud-fog infrastructure frameworks in e-healthcare is tested to provide the maximum societal benefits. Privacy of personal records in

e-healthcare system is considered in this study. Data aggregator avoids multiple point cryptographic process and that has eased the timing constraints to some extent. Incorporation of the query handler and role-based access control mechanisms have handled the viewing aspect of the requested queries successfully. The novel consensus-based approach used in the framework ensured the reliability of the requester to view the EMR. In short, the experimental and comparative analysis confirm the method is efficient and beneficial for e-healthcare in cloud-fog network.

VI. AUTHOR CONTRIBUTIONS

G. Kumar, R. Saha and M.K. Rai conceived the idea, designed the experiments and analyzed the data; G. Kumar and R. Saha performed the experiments and conducted the analyses; G. Kumar, R. Thomas and Se-jung Lim interpreted the results and drew the conclusions; R. Thomas and R. Saha wrote the paper. All authors agree with the above contribution details.

VII. CONFLICTS OF INTEREST

All authors declare no conflict of interest.

REFERENCES

[1] O. Salman, I. Elhajj, A. Chehab, and A. Kayssi, "IoT survey: An SDN and fog computing perspective," *Comput. Netw.*, vol. 143, pp. 221–246, Oct. 2018.
[2] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019.
[3] P. P. Ray, "A survey of IoT cloud platforms," *Future Comput. Inform. J.*, vol. 1, nos. 1–2, pp. 35–46, 2017.
[4] M. Armburst *et al.*, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, p. 5058, 2010.
[5] *Cisco Global Cloud Index: Forecast and Methodology, 2016–2021*, Cisco, San Jose, CA, USA, 2018.
[6] L. Peng, A. R. Dhaini, and P.-H. Ho, "Toward integrated cloud–fog networks for efficient IoT provisioning: Key challenges and solutions," *Future Gener. Comput. Syst.*, vol. 88, pp. 603–616, Nov. 2018.
[7] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Gener. Comput. Syst.*, vol. 78, pp. 659–676, Jan. 2018.
[8] *Gujarat Doctor Makes History, Performs World's 1st Robotic Heart Surgery 30 km Away from Patient*. Accessed: Dec. 7, 2018. [Online]. Available: https://www.news18.com/news/india/gujarat-doctor-makes-history-performs-worlds-1st-robotic-heart-surgery-30-km-away-from-patient-1961729.html
[9] C. Zhao, J. Jiang, Z. Xu, and Y. Guan, "A study of EMR-based medical knowledge network and its applications," *Comput. Methods Programs Biomed.*, vol. 143, pp. 12–23, May 2017.
[10] A. S. M. Kayes, W. Rahayu, T. Dillon, E. Chang, and J. Han, "Context-aware access control with imprecise context characterization for cloud-based data resources," *Future Gener. Comput. Syst.*, vol. 93, pp. 237–255, Apr. 2019.
[11] N. A. Azeez and C. van der Vyver, "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis," *Egyptian Inform. J.*, vol. 93, pp. 237–255, Apr. 2019.
[12] R. Clarke. (2006). *What's Privacy?* Accessed: Dec. 2018. [Online]. Available: http://www.rogerclarke.com/DV/Privacy.html
[13] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & IoT," *Sustain. Comput. Inform. Syst.*, vol. 19, pp. 174–184, Sep. 2018.
[14] L. Malina, J. Hajny, P. Dzurenda, and V. Zeman, "Privacy-preserving security solution for cloud services," *J. Appl. Res. Technol.*, vol. 13, no. 1, pp. 20–31, 2015.
[15] Z. Guan *et al.*, "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, Jan. 2019.
[16] J. Lu, F. Nan, Y. Huang, C.-C. Chang, Y. Du, and H. Tian, "Privacy-preserving public auditing for secure data storage in fog-to-cloud computing," *J. Netw. Comput. Appl.*, vol. 127, pp. 59–69, Dec. 2018.
[17] A. Viejo and D. Sánchez, "Secure and privacy-preserving orchestration and delivery of fog-enabled IoT services," *Ad Hoc Netw.*, vol. 82, pp. 113–125, Jan. 2019.
[18] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving fusion of IoT and big data for e-health," *Future Gener. Comput. Syst.*, vol. 86, pp. 1437–1455, Sep. 2018.
[19] S. Sharma, K. Chen, and A. Sheth, "Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems," *IEEE Internet Comput.*, vol. 22, no. 2, pp. 42–51, Mar. 2018.
[20] H. Dawood, I. Masood, N. R. Aljohani, A. Daud, and Y. Wang, "Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure," *Wireless Commun. Mobile Comput.*, vol. 2018, Nov. 2018, Art. no. 2143897.
[21] M. A. Sahi *et al.*, "Privacy preservation in e-healthcare environments: State of the art and future directions," *IEEE Access*, vol. 6, pp. 464–478, 2017.
[22] K. Zhang, X. Liang, M. Baura, R. Lu, and X. Shen, "PHDA: A priority based health data aggregation with privacy preservation for cloud assisted WBANs," *Inf. Sci.*, vol. 284, pp. 130–141, Nov. 2014.
[23] X. Liu, R. H. Deng, Y. Yang, H. N. Tran, and S. Zhong, "Hybrid privacy-preserving clinical decision support system in fog–cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 825–837, Jan. 2018.
[24] D. Koo and J. Hur, "Privacy-preserving deduplication of encrypted data with dynamic ownership management in fog computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 739–752, Jan. 2018.
[25] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation," *Future Gener. Comput. Syst.*, vol. 76, pp. 540–549, Nov. 2017.
[26] C. Menaka and R. S. Ponmagal, "Patient-controlled personal health record enforcing patient privacy in cloud based healthcare system," *Int. J. Pure Appl. Math.*, vol. 119, no. 10, pp. 375–392, 2018.
[27] J. Emuoyibofarhe, "Ensuring patients privacy in a cryptographic-based-electronic health records using bio-cryptography," *Int. J. Electron. Healthcare*, to be published.
[28] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, Jan. 1987.
[29] L. Lamport, "The part-time parliament," *ACM Trans. Comput. Syst.*, vol. 16, no. 2, pp. 133–169, 1998.
[30] *What is Role-Based Access Control (RBAC) for Azure Resources?*. Accessed: Dec. 17, 2018. [Online]. Available: https://docs.microsoft.com/en-us/azure/role-based-access-control/overview
[31] *Query Processing Language*. Accessed: Jan. 5, 2019. [Online]. Available: https://www.searchtechnologies.com/search-query-parsing
[32] *SQL Processing*. Accessed: Jan. 22, 2019. [Online]. Available: https://docs.oracle.com/database/121/TGSQL/tgsql_sqlproc.htm#TGSQL175
[33] *Apply the LINDDUN Framework for Privacy Requirement Analysis*. Accessed: Jan. 25, 2019. [Online]. Available: http://tampub.uta.fi/handle/10024/100871

RAHUL SAHA received the B.Tech. degree in computer science engineering from the Academy of Technology, West Bengal, and the M.Tech. and Ph.D. degrees from Lovely Professional University, Punjab, India, with area of specialization in cryptography, position and location computation in wireless sensor networks, where he is currently an Associate Professor. He has many publications in well renowned international journals and conferences.

GULSHAN KUMAR received the B.Tech. degree in computer science engineering from the Amritsar College of Engineering, Amritsar, in 2009, and the M.Tech. and Ph.D. degrees from Lovely Professional University, Punjab, India, with area of specialization in position and location computation in wireless sensor networks, where he is currently an Associate Professor. He has many publications in well renowned international journals and conferences.

MRITUNJAY KUMAR RAI received the M.E. degree in digital system from the Motilal Nehru National Institute of Technology, Allahabad, India, and the Ph.D. degree from the ABV Indian Institute of Information Technology and Management, Gwalior, India. He was an Associate Professor with Lovely Professional University, Phagwara, India. He had published more than 50 research articles in reputed international conferences and international journals. His research interests include wireless networks, network security, and cognitive radio networks.

REJI THOMAS received the Ph.D. degree from IIT Delhi. He is currently a Professor with Lovely Professional University, Phagwara, Punjab, India. His research interests include logic, memory, and energy storage devices.

SE-JUNG LIM is currently with the Department of Computer Engineering, Chonnam National University. Her main research interests include wireless sensor networks, IT systems, and network security.