Protecting Medical Data Over Cloud using an Effectual Authentication Model

C. Raghavendra[1] and R. Raja[2]
[1]Assoc. Professor, CVR College of Engineering/ CSIT Department, Hyderabad, India
Email: drraghavendra@cvr.ac.in
[2]Assoc. Professor, CVR College of Engineering/ CSIT Department, Hyderabad, India
Email: r.raja@cvr.ac.in

Abstract- Tele-medicine provides better on-demand service from various places. This technology is modelled to get rid of the distance based barriers and to enhance service accessing process in various rural communities. With cloud computing advancements, Medical based on-demand services (MoDS) in tele-medicine system are offered by Cloud Service Providers (CSP). CSP associates patients and medical personalities from various places with fidelity and confidentiality. However, healthcare data outsourcing over public cloud offers certain novel confronts on security. Even though, attribute based encryption process provides flexible access control, huge amounts of subscribed or unsubscribed patients are connected with cloud based medical services; offering membership management is expensive. Here, Secure-MoDS based protocol (S-MoDS) is anticipated to acquire dynamic authorization and authentication with improved efficiency and flexibility for medical services over telemedicine system. Subsequently, when patients intend to change their ordering service, it does not require any parameter updating for those patients. Here, a secure authentication mechanism has been constructed for distributed tele-medicine system that attempts to update patients' private key separately. As well as, multiple authorities are involved to handle this system even in real time environment. However, private healthcare data, distributed database that are placed in cloud should show protection integrity. This may eliminate accidental misdiagnosis from inappropriate electronic health records that are circumvented by malicious users of internal cloud. Here, simulation is performed in MATLAB environment. The anticipated S-MoDS provides better trade off in contrary to prevailing attribute based encryption model in key generation and protocol performance.

***Index Terms*- Telemedicine, authentication, medical services, integrity, public cloud**

I. Introduction

When population grows higher, medical resource requirements may increase drastically in various healthcare systems [1]. Patients' who resides in under-developmental regions, where traffic is considered to be more inconvenient, extreme mobility lack and access authority towards high quality healthcare are complex for disabled and aged persons [2]. Tele-medicinal services may facilitate a way for fulfilling the gap [3]. This system may consumes huge information technological and telecommunication advantages to provide remote healthcare resources that resolves distance barriers to enhance medical services in remote rural communities [4], and may saves life in emergency and critical situations.

On demand, medical services are aroused with advancements in telemedicine system [5]. As depicted in fig. 1, patients are provided to communicate with most available specialists or doctors in distance devoid of visiting them directly [6]. In accordance to medical certificate from specialist of very large scale hospitals, patients may undergo certain laboratory based tests and physical examination with needed demand in community or local hospital, whose major role is to upload electronic health care records to database in cloud [7]-[8]. After receiving the consultation reports, remote doctors may perform accurate diagnosis for them. With this modelling, telemedicine system provides prescription verification and remote diagnosis that may save prior medical resources and diminish overall healthcare cost for poverty stricken individuals [9]-[10]. However, this system may facilitate healthcare consultant in various location to share information and examines predictive outcomes as remains in meeting room. In case of diverse serious illness, this may avoid infectious disease transmission or parasites among medical staffs and infectors[11]-[12].

Telemedicine system is generally provided with cloud service providers who offers virtual platform that facilitates patients and doctors to function together with complete health and wellness and assisted with home care services [13]. With this, it may construct communication link between storage server and medical staff. Patient may be subscribed with certain medical services over demand for superior quality care accessibility and enhancing their experiences [14]-[15]. Cloud servers are accountable for storing electronic records and health related data. For research specialist, they may access physical data that are provided in cloud to carry put appropriate diagnosis and perform certain scientific researchers. Cloud computing may also changes conventional model for medical care in digital format.

Based on confidentiality and access authority over cloud, the predominant cryptographic model is attribute based encryption model that offers encryption and decryption in accordance to user attributes [16]. In this model, it is executed in one to many bases. Anyone who possesses the ability of decrypting protected data with data owner attribute, partial elements of encrypted data are fixed with private key component. With these characteristics, data holder may upload information to server devoid of doubt. With respect to various relationships among access

Received on 12-11-2021, Revised on 04-03-2022, Accepted on 28-04-2022.

structures, private keys and cipher texts are related to secure authentication. Here, Secure-MoDS is anticipated for performing data encryption and decryption. Here, users' private keys are related to designed policies and cipher texts are labelled using various attribute sets. This may facilitates users to decrypt cipher text whenprivate key access standardization is fulfilled by embedded cipher text may eliminate user permissions. Therefore, this authentication is generally used to safeguard outsourced data confidentiality. With secure MoDS- cipher text is connected with certain standards and private key is depicted by attribute set. Users may decrypt cipher text with access tree iff attributes are related with private key to fulfil access structure, that may rejects certain decryptors requirements. This provides ability to medical service tagging by telemedicine attributes and private key distributionduring tagging user subscription. Subsequently, secure MoDS is superior for offering access confidentiality and authority of MoD than ABE.

II. Related Works

Lightweight based mutual authentication protocol for sensor and IoT devices and application is anticipated in [17]. This protocol is used among two lightweight models that work on key encryption strategy. It may utilize response and challenge strategy for mutual authentication by encryption. This kind of strategy is specified as n-pass protocol for security and encryption factors may describe various rounds. This protocol may consider participants who are previously aware of public key identities respectively. This protocol is provided to carry out when comparing with ECC, RSA and other protocol version as in contrary to optimal scheme.

There are various investigations that some efforts are provided to attribute based cryptography to blockchain. In [18], EHR's system, utilized attribute dependent signature strategy with multi-authority to validate blocking facility. It is stored with individual patient data. With this protocol, patient may provide physical data block anonymously, and provide access policy for appropriate personals to acquire those data. In [19], author used ABE approach to provide encrypt and secrete key shared data over cloud. In this approach, block chain technology may facilitate keyword search function on cipher text can be executed. In [20]-[21], author merged IBS, IBE, ABE and blockchain over crypto-system to offer system management. To facilitate privacy and data sharing, author [22] anticipated block chain dependent privacy preserving distribution for EMRs, that are stored in cloud indexes are reversed in tampered consortium proof based block chain. In [23]-[24], author offered an access control factors for block chain EMR exchange that eliminated gate way to authorize individuals access with block chain granularity. In [25], author provided a novel verification strategy for patient authentication among node database and enrolment devices. Blockchain approach may fulfil traceability and integrity of medical data.

III. Methodology

The mutual authentication operation includes two communication parties that may establish two protective authentication and communication server to start various processes. It may fulfil confidentiality with public key encryption usage; one directional has function integration and authentication using mutual agreement among communication parties for determining last session key for communication. System identity is essential for validating accuracy of transmitted message, where time stamp may fulfil message that works on current function. Every public key may be placed in server that assists in authentication and system registration.

A. Secure MoDS protocol

1) Each end user wants to establish protected communication with cloud server, may request for public key from server authority. Here, C is client, AS is service authority, P is public key, I is request, S is storage in cloud, t is time, E is encryption and D is decryption.

$$C \rightarrow AS: I_c, PK_c \qquad (1)$$

2) The authority may consider the end user as valid client and responses with public key request for cloud server.

$$AS \rightarrow c: PK_s \qquad (2)$$

3) Client may generate pseudo random number and timestamp XOR. Client then computes session key using $K_{c,s} = H\,(t_c \otimes R_c)$.These factors are then encrypted with cloud server based key provided by cloud authority. It is given as input to lightweight encryption process. Here, t_c, R_c, PK_c are provided for computation of $k_{c,s}$ and validating corresponding identity.

$$C \rightarrow s: E_{PKs}\left((t_c, R_c), K_{c,s}, PK_c\right) \qquad (3)$$

4) When receiving encryption from client, cloud server decrypts with private key D_{SKs} and validate computation of $K_{c,s} = H(t_s \otimes R_s)$. Cloud server network address and validation message is also used here. All these factors are encrypted with client public key and transmitted to end users.

$$s \rightarrow c: E_{PKc}\left(K_{s,c}, (t_s, R_s), a_s, v\right) \qquad (4)$$

5) User decrypts message with private key D_{SKc} and verification for re-computation of session key using hashing, stores timestamp message and network address validation by v. Absolutely, user may re-computes session key using $K_{c,s} = H(t_c \otimes R_c)$. In initial message part, new session key is encrypted using cloud server public key E_{PKs}, where next message is encrypted in public key E_{PKs} comprising plain text message clustered with clients' timestamp, network address, random number which is validated with cloud server by evaluating hash $H(t_c \otimes R_c)$ with user's session

key $k_{c,s}$. With message encryption and key are attained and transmit as single message to server.

$$c \rightarrow s: E_{PKs}(K_{c,s}), E_{PKs}(M, (t_c, R_c), a_c) \quad (5)$$

Assume that pseudo random variables are generated with above discussed number. This protocol considers ransom values as input, therefore encryption is not usually with similar parameter.

B. S-MoDS in Tele-medicine

Telemedicine holds various informational and communicational benefits to get rid of geographical constraints and enhances access to various healthcare services. Telemedicine execution is measured as specific benefits for enhancing client experience and protecting constrained medical cost and resources. Merging various cloud computing technologies, data distribution in telemedicine model assists physicians to provide appropriate prediction in proper time and offer superior quality to all individuals.

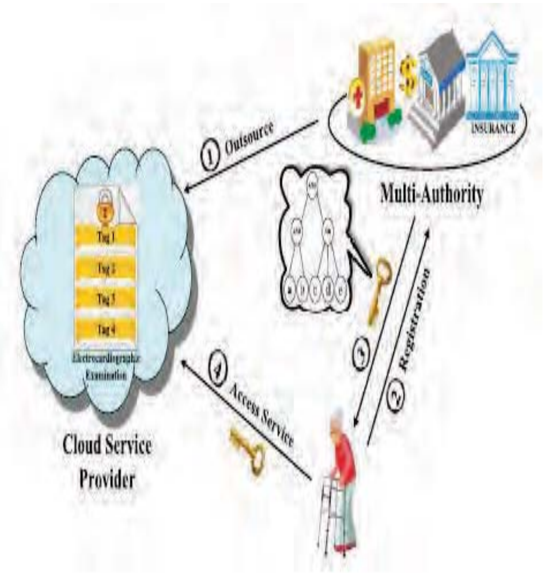

Figure 1. Generic Medical on Demand protocol

Healthcare data over telemedicine system comprises sensitive and personal information that are more attractive to cybercriminals. Henceforth, huge confronts for certain system to depict how to share, store and use data to privacy divulging server. However, integrity and privacy of healthcare data are safe guarded from external malicious users, however also from unauthorized access from insider cloud users of this system, for instance, (CSP and authority). They may assist in developing protected telemedicine system to provide integrity and privacy of healthcare data to various medical resources and fulfil data confidentiality. As depicted in Fig. 2, medical service is labelled with certain attribute in tag formats like examination of electrocardiographic tagging in heart disease, arrhythmia, angina pectoris, and price and so on. Various telemedicine authorities may merge with distributed keys with diverse standards to every patient. For example, cloud authorities

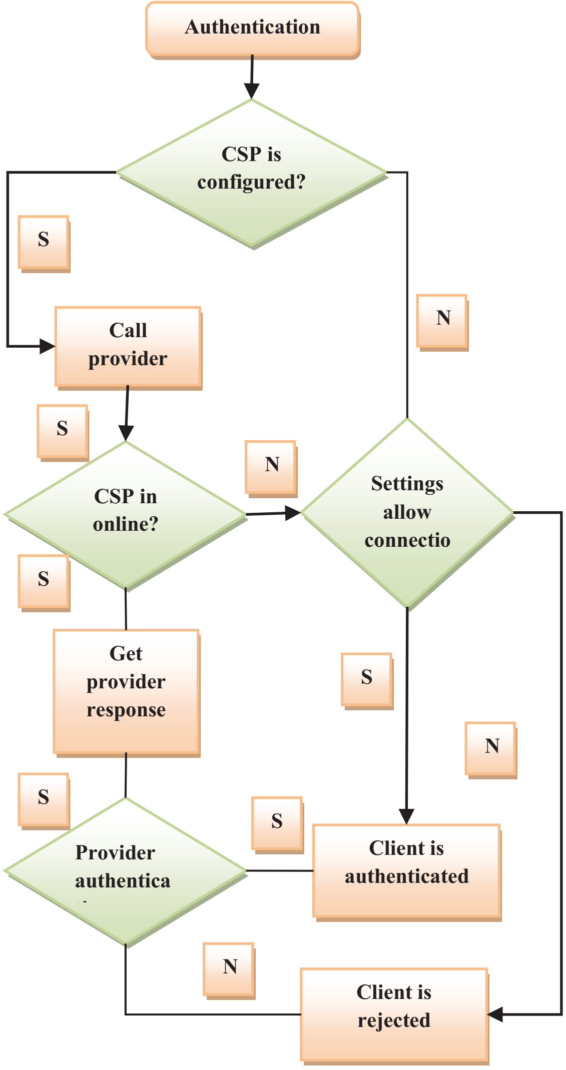

Figure 2. Flow diagram of proposed model

are accountable for registration, e-payment, and healthcare subsidies. They construct key for decrypting protected on demand services as the attributes are fulfilled with cardiology, heart disease, pectoris and arrhythmia. Therefore, Secure MoDS protocol may offer data confidentiality and access control in telemedicine system.

While considering integrity consortium based block chain is used for managing these multiple authorities as in fig. 2. More specifically, after performing private key, users may perform electrocardiographic analysis with wearable medical devices by their own in house or more sophisticated professional equipment in community care taking centre nearby. After performing this, analysis results of Electrocardiograph (ECG), physical status video, ultrasound, colour Doppler are uploaded CSP to database and data were indexed by keywords and abstracts of outcomes that are provided in block. For specialists and doctors, analysis was downloaded and provide medical certificate to user with CSP. Services may vary in diverse days; it may produce block chronologically to save indexes of associated healthcare data when appropriate data is placed. Blocks that are available in MoD services are associated with series into block chain that belongs to user. As smaller size of index, it will not exceed storage space limitation in all blocks. Based on this model, changes concerning original healthcare information in cloud may cause due to appropriate index in block chain that are altered and every entity comprising all authorities may discover corresponding variations. This approach may acquire global perspective in medical history in verifiable, efficient and permanent methodology. Therefore, block chain approaches is beneficial for offering protection integrity on healthcare data in cloud.

C. *Security evaluation*

This section provides a detailed security analysis on the proposed model. The S-MoDS model provides secure mutual authentication and key agreements. The trust relationship is established via the authentication process. The following are the security related steps:

1) Generate pair-wise private and public keys;

2) Randomly select the prime numbers;

3) Generate encrypted medical file or records;

4) Make the essential medical information to be encrypted;

5) Compute the cipher text;

6) Perform proxy re-encryption;

7) Compute the complexity of the private and public key;

8) Decrypt the hospital data;

9) Evaluate the essential information.

IV. Numerical Results and Discussions

The ultimate objective of this work is to examine the prevailing and the anticipated protocol model experimentally, where mutual authentication efficacy is dependent on pseudo random functionality and key exchange among cloud server. From this, experimentation is carried out using various factors. Execution time of anticipated model is demonstrated at various time instances. Simulation was carried out in MATLAB environment and key size, execution time is considered to be a major performance metrics. Here, Intel core i3 processor with 3.10GHz RAM and 16 GB internal memory.

TABLE I.
Order of Computation

Encryption cost	Decryption cost	Registering	Updating	Revoking
$O(m_c)$	$O(m_c)$	$O(m)$	$O(n\ X\ m)$	$O(n\ X\ m)$
$O(m_c)$	$O(m_c)$	$O(m)$	$O(n\ X\ m)$	$O(n\ X\ m)$
$O(m_c)$	$O(m_c)$	$O(m + m_u + n)$	$O(m + m_u + n)$	$O(\ m)$
$O(m_c)$	$O(m_c)$	$O(m_u)$	$O(n\ X\ m_u)$	$O(n\ X\ m)$
$O(m_c)$	$O(m_c)$	$O(m + m_u + n)$	$O(m + m_u + n)$	$O(\ m)$
$O(N\ X\ m_c)$	$O(N\ X\ m_c)$	$O(N\ X\ m)$	$O(N\ X\ m)$	$O(\ n\ X\ m)$
$O(m_c)$	$O(m_c)$	$O(m)$	$O(n\ X\ m)$	$O(\ n\ X\ m)$
$O(N\ X\ m_c)$	$O(N\ X\ m_c)$	$O(N\ X\ (m + m_u + n)$	$O(m + m_u + n)$	$O(\ m)$

TABLE II.
Encryption Time

Number of experiments	Secure data sharing scheme	S-MoDS
1	3428	3400
2	3505	3500
3	3420	3350
4	3381	3280
5	3306	3200
6	3346	3246

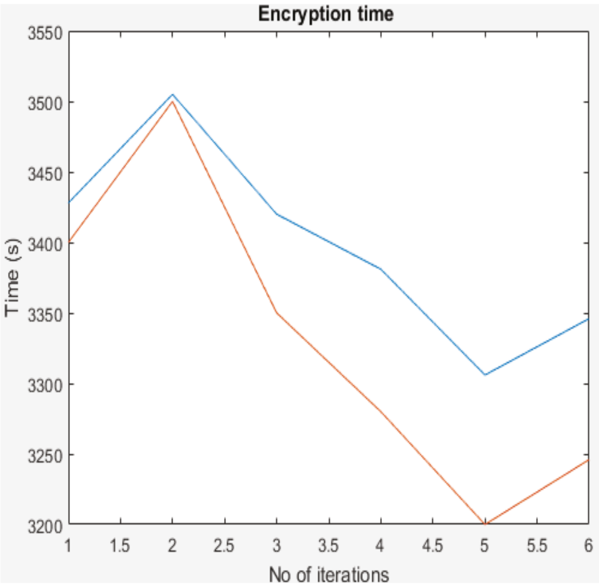

Figure 3. Encryption time

TABLE III.
DECRYPTION TIME

Number of experiments	Secure data sharing scheme	S-MoDS
1	113	110
2	104	100
3	156	150
4	189	180
5	145	140
6	108	103

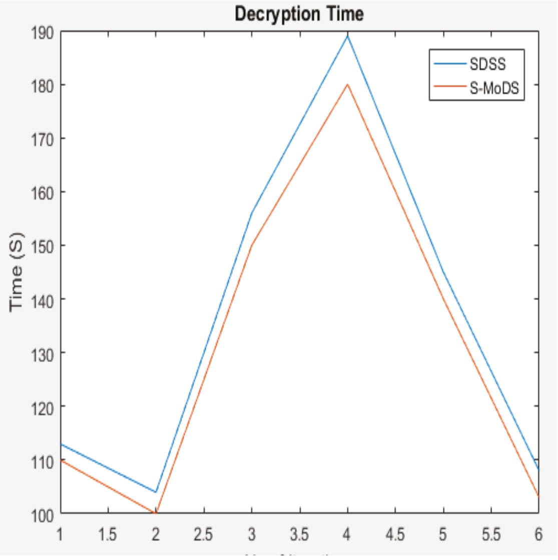

Figure 4. Decryption time

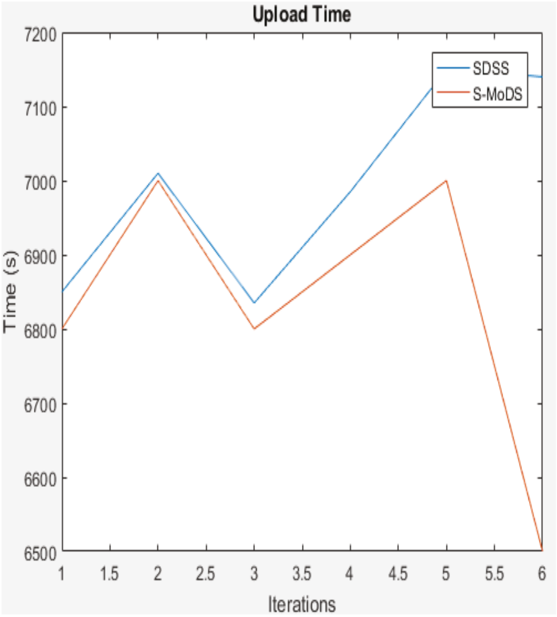

Figure 5. Uploading time

TABLE IV.
UPLOAD TIME

Number of experiments	Secure data sharing scheme	S-MoDS
1	6850	6800
2	7010	7000
3	6835	6800
4	6985	6900
5	7150	7000
6	7140	6500

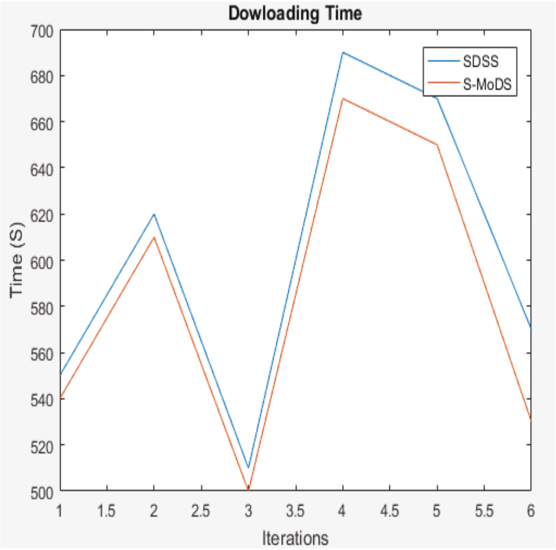

Figure 6. Downloading time

TABLE V.
DOWNLOAD TIME

Number of experiments	Secure data sharing scheme	S-MoDS
1	550	540
2	620	610
3	510	500
4	690	670
5	670	650
6	570	530

TABLE VI.
KEY GENERATION TIME

Number of experiments	Secure data sharing scheme	S-MoDS
1	1010	1005
2	1110	1100
3	1150	1130
4	1200	1100
5	1180	1080
6	1200	1050

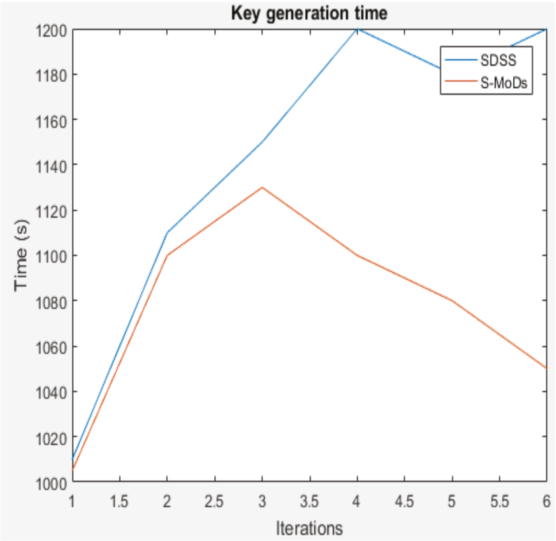

Figure 7. Key generation time

D.

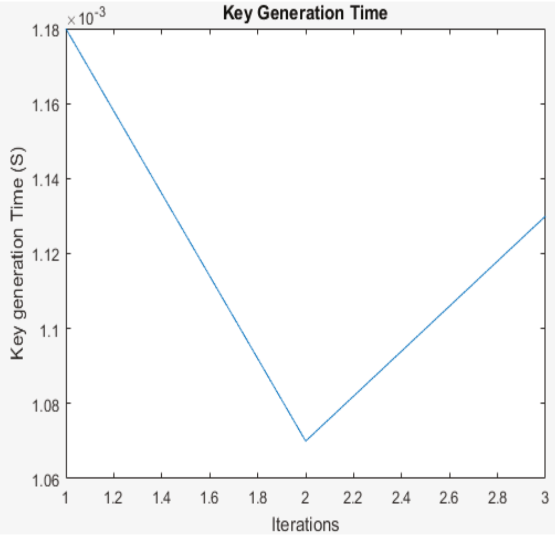

Figure 8. Key generation time

TABLE VII.
KEY GENERATION TIME(S)

256 bit hash	Key generation time (s)
Session Key S_{k1}	0.001180
Session Key S_{k2}	0.001070
Session Key S_{k3}	0.001130

TABLE VIII.
COMPUTATIONAL TIME

Protocol	MPAKE	S-MoDS
Computational Time (s)	9.30	5.90

From figure given above, the performance analysis was performed with various parameter sets. Time needed for 100 key generation with available system is quite complex. Therefore, generation of millions of keys are measured to be a standalone factor for examining server that is done with reduced amount of time. Table I depicts various order of computation and complexity for performing various computation. Generation of more keys are more appropriate for time needed for all devices. Generation of session keys as in Table VI is provided 'H' timestamp.

Table VII depicts computational time of proposed versus existing model. Here, S-MoDs is compared with MAPKE where computation time of MPAKE is 9.30 while in S-MoDs computation time is 5.90 seconds. From Fig 3- Fig 8 various computations has been performed for key generation, uploading time, downloading time, encryption time, decryption time. Performance is quite similar to key generation from various set of parameter values. Table II depicts the comparison of the encryption time of proposed S-MoDS with existing secure data sharing scheme. The encryption time is measured in seconds. The execution time of proposed model is 3400s, 3500s, 3350s, 3280s, 3200s and 3246s which is comparatively higher than secure data sharing scheme, i.e. 3428s, 3505s, 3420s, 3381s, 3306s and 3346s. Table II to Table VI depicts corresponding values associated with Encryption, decryption, uploading and downloading time. Some features are more essential in protocol design such as update, Authorities, Integrity, traceability. Update is specifically for revoking and updating with standardized policies. When users joins or leaves cloud network, service authority may be raised with version number. Each authority is accountable for managing various kinds of data associated with S-MoDS authentication protocol. In traceability, it merges cloud storage and blockchain for managing original data as it is stored in cloud. It protects medical data from distortion. It will also reduce medical disputes and accidents. By evaluating various factors, protocol has to fulfil revoking, updating, integrity, traceability and multiple authority management in cloud storage.

V. CONCLUSIONS

This research intends to model a novel approach for provisioning authentication to the medical data. S-MoDS protocol is appropriate for performing against diverse attacks and outcome session offers superior performance on huge amount of devices that are to be authenticated in reduced time. Here, Secure-MoDS based protocol (S-MoDS) is anticipated for establishing authentication over telemedicine system. A secure authentication mechanism has been constructed for distributed tele-medicine system to update patients' private key where multiple authorities are involved to handle this system. Private healthcare data is placed in cloud and gives protection integrity. It eliminates accidental misdiagnosis from inappropriate electronic health records. This is extremely appropriate for cloud architecture that included IoT that are used in various labs, universities, vehicles, industries where secured environment is extremely prioritized. Regrettably, this work has attained an effectual protocol model in contrary to benchmarks like RSA, ECC and so on. As future extension, this work may carry out experimentation with multiple high level end users from various channels for approximating resource availability. As well, authentication backup is offered to eliminate single point of failure in connected network.

REFERENCES

[1] Y. Karaca, M. Moonis, Y.-D. Zhang, and C. Gezgez, “Mobile cloud computing based stroke healthcare system," Int. J. Inf. Manage., vol. 45, pp. 250_261, Apr. 2019.

[2] O. Ali, A. Shrestha, J. Soar, and S. F. Wamba, “Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review," Int. J. Inf. Manage., vol. 43, pp. 146_158, Dec. 2018.

[3] M. Armbrust, A. Fox, R. Grif_th, A. D. Joseph, R. Kaz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50_58, 2010.

[4] V. Casola, A. Castiglione, K. K. Choo, and C. Esposito, “Healthcare-related data in the cloud: Challenges and opportunities," IEEE Cloud Comput., vol. 3, no. 6, pp. 10_14, Apr. 2016.

[5] S. H. Lee, J. H. Song, and I. K. Kim, “CDA generation and integrationfor health information exchange based on cloud computing system," IEEE

[6] Trans. Services Comput., vol. 9, no. 2, pp. 241_249, Mar. 2016.

[7] S. Sharma, K. Chen, and A. Sheth, “Toward practical privacy-preservinganalytics for IoT and cloud-based healthcare systems," IEEE InternetComput., vol. 22, no. 2, pp. 42_51, Mar. 2018.

[8] V. Goyal, O. Pandey, A. Sahai, and B.Waters, “Attribute-based encryptionfor _ne-grained access control of encrypted data," in Proc. 13th ACMConf. Comput. Commun. Secur., Alexandria, VA, USA, Oct./Nov. 2006,pp. 89_98.

[9] K. He, J. Chen, Y. Zhang, R. Du, Y. Xiang, M. M. Hassan, and A. Alelaiwi,“Secure independent-update concise-expression access control for video

[10] on demand in cloud," Inf. Sci., vol. 387, pp. 75_89, May 2017.

[11] J. Garay, A. Kiayias, and N. Leonardos, “The Bitcoin backbone protocol:Analysis and applications," in Proc. Annu. Int. Conf. Theory Appl. Cryp-tograph. Techn.,So_a, Bulgaria, 2015, pp. 281_310.

[12] Y. Zhang and J.Wen, “The IoT electric business model: Using blockchaintechnology for the Internet of Things," Peer PeerNetw. Appl., vol. 10, no. 4,pp. 983_994, Jul. 2017.

[13] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and securesharing of personal health records in cloud computing using attribute-basedencryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1,pp. 131_143, Jan. 2013.

[14] J. Wei, W. Liu, and X. Hu, “Secure and ef_cient attribute-based accesscontrol for multiauthority cloud storage," IEEE Syst. J., vol. 12, no. 2,pp. 1731_1742, Jun. 2018.

[15] H. Wang and Y. Song, “Secure cloud-based EHR system usingattribute-based cryptosystem and blockchain," J. Med. Syst., vol. 42, no. 8,p. 152, 2018.

[16] C.-H. Hong and B. Varghese, “Resource management in fog/edgecomputing: A survey," 2018, arXiv:1810.00305. [Online]. Available:https://arxiv.org/abs/1810.00305

[17] S. Khan, S. Parkinson, and Y. Qin, “Fog computing security: A review ofcurrent applications and security solutions," J. Cloud Comput., Adv., Syst.Appl., vol. 6, no. 1, p. 19, 2017.

[18] S. Khan, S. Parkinson, and Y. Qin, “Fog computing security: A review ofcurrent applications and security solutions," J. Cloud Comput., Adv., Syst.Appl., vol. 6, no. 1, p. 19, 2017.

[19] M. V.Pawar and J. Anuradha, “Network security and types of attacks innetwork," ProcediaComput. Sci., vol. 48, pp. 503_506, 2015.

[20] K. Stouffer, J. Falco, and K. Scarfone, “Guide to industrial control systems(ICS) security," NIST, Gaithersburg, MD, USA, Tech. Rep., Jun. 2011.

[21] R. Mahmud, R. Kotagiri, and R. Buyya, “Fog computing: A taxonomy,survey and future directions," Internet Everything, pp. 103_130, Oct. 2017.

[22] N. Chen, Y. Yang, T. Zhang, M.-T. Zhou, X. Luo, and J. K. Zao, “Fog asa service technology," IEEE Commun. Mag., vol. 56, no. 11, pp. 95_101,Nov. 2018.

[23] A. Kattepur, H. K. Rath, A. Simha, and A. Mukherjee, “Distributedoptimization in multi-agent robotics for industry 4.0 warehouses," inProc. 33rd Annu. ACM Symp. Appl. Comput., Pau, France, Apr. 2018,pp. 808_815.

[24] K. Piotrowski, P. Langendoerfer, and S. Peter, “How public key cryptography in_uences wireless sensor node lifetime," in Proc. 4th ACMWorkshopSecure Ad Hoc Sensor Netw., 2006, pp. 169_176

[25] V. L. Shivraj, M. A. Rajan, M. Singh, and P. Balamuralidhar, “One timepassword authentication scheme based on elliptic curves for Internet ofThings (IoT)," in Proc. 5th IEEE Nat. Symp. Inf. Technol., Towards SmartWorld, Feb. 2015, pp. 1_6.

[26] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag,N. Choudhury, and V. Kumar, “Security and privacy in fog computing:Challenges," IEEE Access, vol. 5, pp. 19293_19304, 2017.

[27] C.-H. Hong and B. Varghese, “Resource management in fog/edgecomputing: A survey," 2018, arXiv:1810.00305. [Online]. Available:https://arxiv.org/abs/1810.00305