Cloud Computing and Data Science
http://ojs.wiserpub.com/index.php/CCDS/

Research Article

An Improved Fast and Secure CAMEL Based Authenticated Key in Smart Health Care System

Syed Khasim[1*], **Shaik Shakeer Basha**[2]

[1]Department of Computer Science & Engineering, Dr. Samuel George Institute of Engineering & Technology, Markapur, Prakasam Dt, 523316, Andhra Pradesh, India
[2]Department of Computer Science & Engineering, Avanthi Institute of Engineering & Technology, Gunthapalli, Abdullahpurment Mandal, Hyderabad, 501512, Telangana, India
Email: khasim716@gmail.com

Received: 23 March 2022; **Revised:** 09 June 2022; **Accepted:** 01 July 2022

Abstract: Seeing as Smart Healthcare Systems provide cloud services for storing patient health records, data security and privacy are critical to the company's success, and patients do not want their identities to be revealed. The authentication procedure requires disclosing users' personal data, such as a username and password, on the authentication server in order to protect their identities. The patient's privacy may be invaded if the patient can be observed or linked to by the patient's unfortunate foes. As a result, we propose in this paper a system that gives patients anonymity, protection, and privacy of sensitive healthcare data from the Authorization Service and enemies. A camel-based rotating panel signature program was used in our proposed work to provide anonymity to health records while also adding extra security to the network layer. The effectiveness of the programs was assessed using theoretical analysis, which revealed that the program has a range of security characteristics and is resistant to multiple attacks.

Keywords: Smart Healthcare Systems, anonymous authentication, Camel algorithm, anonymity

Abbreviations

ECC	Elliptic Curve Cryptography
RSA	Rivest-Shamir-Adleman
PCs	Personel Computers
SAGE	Scheme Against Global Eavesdropping
WBANs	Wireless Body Area Networks
CLS	Certificate less Signature
PKI	Public Key Infrastructure
VLR	Verifier Local Revocation
CSP	Cloud Service Provider
RS	Registration Server

DOI: https://doi.org/10.37256/ccds.3220221423

1. Introduction

With cloud computing expanding in popularity, many healthcare institutions are turning to it for a variety of reasons. Healthcare practitioners with substantial savings and computations are motivated to utilize cloud-based servers since cloud computing offers several benefits such as scaling and cost savings [1]. Many advancements in embedded systems, biosensors, and wireless networks have resulted in the outstanding development of wearable sensors in the human body to collect all health records such as blood pressure and heart rate in recent years. Hospitals offer their services via cloud servers, where data are evaluated in order to improve the data quality and the health of the sensors that are delivered here for data processing [2]. Figure 1 shows an example of a smart cloud-based healthcare system for patient identification and anonymous service access in smart healthcare systems. At the same time, we must solve some of the difficulties associated with sharing data on unreliable cloud servers, such as losing patient control over data, health, and privacy violation, and putting patient privacy and the cloud system for health care [3]. We need to create mechanisms to preserve users' privacy, eliminate the risks of losing physical control over data, and secure access to patients' data in a virtual environment from harmful users while maintaining their confidentiality and integrity. Due to the higher processing power, traditional techniques of safeguarding an individual's privacy may not be sufficient. Users' online actions are extremely risky since they can be used to examine cloud servers or eavesdrop on surfing histories and location footprints. Our solution includes an authentication procedure that allows patients to be identified across all health services [4].

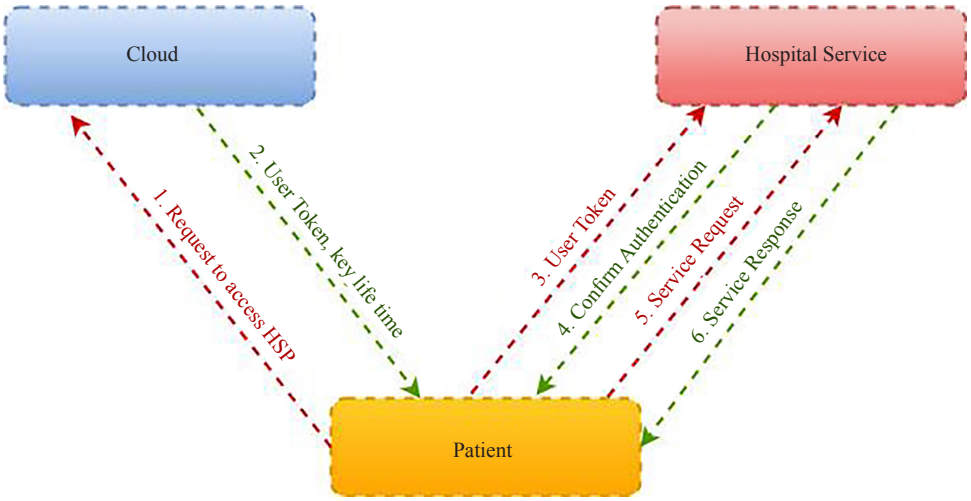

Figure 1. Smart Healthcare Systems for Patient authorization and anonymous service access. The operation of the proposed scheme is strong and attractive on cloud servers to store and hide the identities of patients giving priority to their privacy.

In recent years, a slew of privacy protection accreditation methods has been presented. Cloud servers, on the other hand, are incapable of safeguarding users' personal or sensitive data. When using internet services, offers a number of risks. When using cloud services in health systems, patients do not want to divulge their identities. Patients are hesitant to trust such apps unless the system guarantees complete privacy and security. Data that has been saved could be useful [5]. As a result, the program must be trustworthy and secure. Personal information, such as usernames, histories, and biometric traits, may be used to compromise a patient's identity and extract information from concealed forms, such as evaluating patient preferences or Internet traffic. The following is a list of goals for our work that we would like to attain [6].

Without giving any personal information, the patient is unanimously approved by the authorization server.

• Multiple requests from the same patient cannot be linked through an authorization server, but the patient can be identified through auditory, for example.

• The user in the middle, the computer, is immune to attacks such as back attacks and auditory attacks.
• Sending communications can be verified by the recipient.

The rest of the paper is organized as follows: Section 2 discussed a literature review of previous authentication secure health care system models. Section 3 discusses the proposed method. Section 4 shows and describes the test results of the proposed work. Finally, Section 6 completes the conclusion of proposed work.

2. Related work

This section elaborates on the various issues using different techniques of secure health care modules. In bunch signature, without uncovering the partial character, any substantial gathering part permits to sign quite a few messages in the interest of the gathering. Though, the bunch supervisor has rights to uncover the personality of the endorser when made trouble. Most of the gathering marks depend on customary cryptography like ECC, RSA, and discrete logarithm. On the off chance that quantum PCs arise, these plans would be effectively broken. The new character puts together, gathering marks based on respect to bilinear guides with some security properties. In this plan, the length of the marks is free and the size of the gathering pubic key on the size of the gathering. The plan was appropriate for huge gatherings where the gathering part can sign many messages utilizing a similar key pair. This plan has downsides. The personality based validation frameworks experience the ill effects of the key escrow issue. The key expected to encode or decode is held, and retained so that under particular conditions, an approved party might access the key. As the escrow specialist holding all the cryptographic keys, the key escrow frameworks are considered a security hazard and may spill data or a single disappointment point. Additionally, when a client's private key is compromised, it turns out to be exceptionally difficult to renounce the client [7].

The e-Health framework is imagined as a promising way to deal with further developing medical services through data innovation, where security just as protection is essential for an enormous scope organization and its prosperity. This paper tended to on a solid protection saving Scheme against Global Eavesdropping, named SAGE, for e-Health frameworks. The proposed SAGE can accomplish the substance situated security additionally the logical protection against a solid worldwide enemy. The SAGE has been exhibited effective as far as transmission delay. This plan had a significant disadvantage that it was unreasonable because of substantial computational overhead when straightforwardly applied to the conveyed medical care frameworks. The plan couldn't bear the weight calculations [8].

The proposed mysterious confirmation conspires in cloud climate for s-wellbeing. The reception of an e-Health Cloud has various advantages, particularly sharing, putting away, permitting, and trading data between different clinical establishments, decreasing expense, accessibility of data, lessening costs, quick administrations, and so on Furthermore, saving character protection is a critical test of safety in all conditions just as establishes especially an intense worry in cloud conditions. It puts to the main goal of the client while utilizing administrations. Without a doubt, a significant boundary to the reception or utilization of cloud clients is dread of security misfortune in the cloud worker, especially in an e-Health cloud where clients show restraint toward touchy information or data. Clients/patients may don't have any desire to reveal their characters to the Cloud Service Provider when utilizing its administrations. An approach to secure them is making them unknown to the workers. This paper proposed a versatile and adaptable methodology for patients' personality security to ensure an e-Health Cloud through a mysterious verification plot. This plan depends on blind marks which permit patients to devour cloud benefits namelessly over the world. The framework slacked to give any insights concerning client enlistment and denial. Conversation insights concerning security investigation are not given [9].

In research on application, arranged plan about Wireless body region organizations (WBANs). That is generally utilized telemedicine, which can be used for home medical care and continuous patients checking. In WBANs, the sensor hubs assemble the customer's physiological information. Send it to the clinical focus, the customers communicate it to the clinical focus, the customers' very own information/data is touchy and there are a lot of safety dangers in the additional body corresponds. Henceforth, the security and security of customers' physiological information should be ensured and guaranteed first. Many existing validation conventions for WBANs neglected to consider the key update stage. This paper proposes proposed a proficient verified key arrangement conspire for WBANs in addition to adding the key update stage in improving the security of the plan. In the confirmation stage, to decrease the calculated cost, meeting keys are produced during the enlistment stage and kept covertly. The plan was more productive and dependent

on bilinear pairings yet the repudiation cycle was not plainly characterized if there should arise an occurrence of debate [10].

Wireless Body Area Networks (WBANs) is assistance, which is proficiently utilized at present for giving productive and got medical care administrations. This paper included Certificate less over the remote organization plot for the security reason. Furthermore, a couple of safety conventions are being utilized in both end client and specialist organizations. This plan was proposed to carry out the mysterious light-weight confirmation convention. A WBAN client can without much of a stretch access the telemedicine framework through this convention. Utilizing WBAN administrations, the doctor gets refreshed and the constant data of the patient. The Certificate less Signature (CLS) conspire is nearly used to exceptionally satisfying the security saving needs in WBAN by certificate less encryption likewise intended to dispense with the downsides of the PKI based plan and it doesn't need personality based encryption and computerized authentication, i.e., no key escrow issue. CLS allocated the security by giving private keys to the patient due to that it is inconceivable for the outsider or the aggressor to get to the private data of specific meetings that occurred during validation measure. The plan additionally gave enormous disadvantage of denial method itemizing inappropriately [11].

An unknown verification conspires for remote organizations utilizing Verifier Local Revocation (VLR) bunch signature plot. In the progression of information driven advancements and the Internet of Things in gathering and dispersing tangible information, security and protection turn out to be generally significant and helpful needs. This worry is a direct result of tactile information ordinarily communicated on remote organizations to-ward server farms which is effectively or for the most part noticed for the objective l of organization traffic investigation. Also, the gathered information in server farm can be handily gotten two from different clients, programmers too, if the framework doesn't manage any legitimate security system. In this proposed unknown validation arrangement of blending bases verifier-nearby disavowal bunch signature plot that confirms remote hubs (i.e., sensor hubs) of a specific advantage gathering to the door hub in communicating information. An extra accomplishment is a mysterious verification for getting information to the server farm. Where the plan helpless against replay assaults additionally a noxious Group Manager can imitate a client [12]. The Table 1 shows the various smart health care secure systems comparisons between 2018 to 2022, due to its impact this proposed work has been started to implement.

Table 1. Comparison of Smart Health Care Secure System

Reference	Year	Description
[13]	2018	The need for a dependable end-to-end communication process it-based healthcare applications are discussed, as well as the development of communication technologies that can meet these requirements. Bacterial infections, heart disease, musculoskeletal injuries, and neuromuscular disorders are all represented in the study.
[14]	2019	A comprehensive examination of IoT-based software and systems in smart medical systems is offered. To provide meaningful insight into modern healthcare systems, various apps and services is explained in terms of their major goals and fields of application.
[15]	2021	A table summarizes the standards, specs, benefits, and drawbacks of the most recent WBAN-based healthcare applications. At the end of this paper, open concerns and major obstacles are tackled after mentioning it-based health care services and applications.
[16]	2021	The design of smart health systems is discussed, as well as the main requirements for these systems. Future directions and open topics are discussed at the conclusion of this study to ensure that smart healthcare systems evolve enough and quickly.
[17]	2022	Traditional healthcare system needs are discussed, as well as an overview of the smart healthcare infrastructure and the current state of new technologies employed in smart healthcare systems. The primary applications and services, as well as the obstacles of smart healthcare, are explored to provide a thorough understanding of the system's requirements and functions.

3. Proposed methodology

The camel-based system was utilized in the suggested anonymous authentication scheme to prevent users from acting as unreliable authentication servers in smart cloud-based healthcare applications.

In the event of harmful activity, the suggested approach provides a means for detecting privacy violations with the least amount of risk. Each group has an expiration date and members are reminded to update their keys on a regular basis to speed up the authorization process. When a member's key is returned, they must reveal their previous credentials. Furthermore, anonymous authentication techniques are commonly seen as lonesome. By connecting to a physical location or a person, a cloud service provider operating on the Internet can connect subsequent requests through an IP address. As a result, the software used Camel, which gives network-level anonymity to users while reducing the amount of data available to the cloud service provider. Camel's hidden service cannot be reached anonymously.

It completes anonymous authentication processes with minimum information, allowing neighboring links to be connected to the service provider. Instead of using a direct connection, Internet users connect a series of virtual tunnels to shield the camel network from traffic analytics attacks, which can be used to infer who is talking to whom on the public network.3 The camel, which is connected to the middle relay terminals via a relay terminal, transports traffic from the middle relay terminals to the exit terminals, preventing the entry and exit terminals from becoming acquainted.

The exit nodes, on the other hand, route traffic to the customer's desired destination. The encryption key for encryption is known by each node. We engaged Camel to work on the server side of our project, and there is a plan to run two secret services, which points to a strategy that uses elements of the CSP and RS protocols. The camel on the customer page can be used to encrypt internet traffic as a proxy application. It can cover the entire world by jumping via a succession of computers.

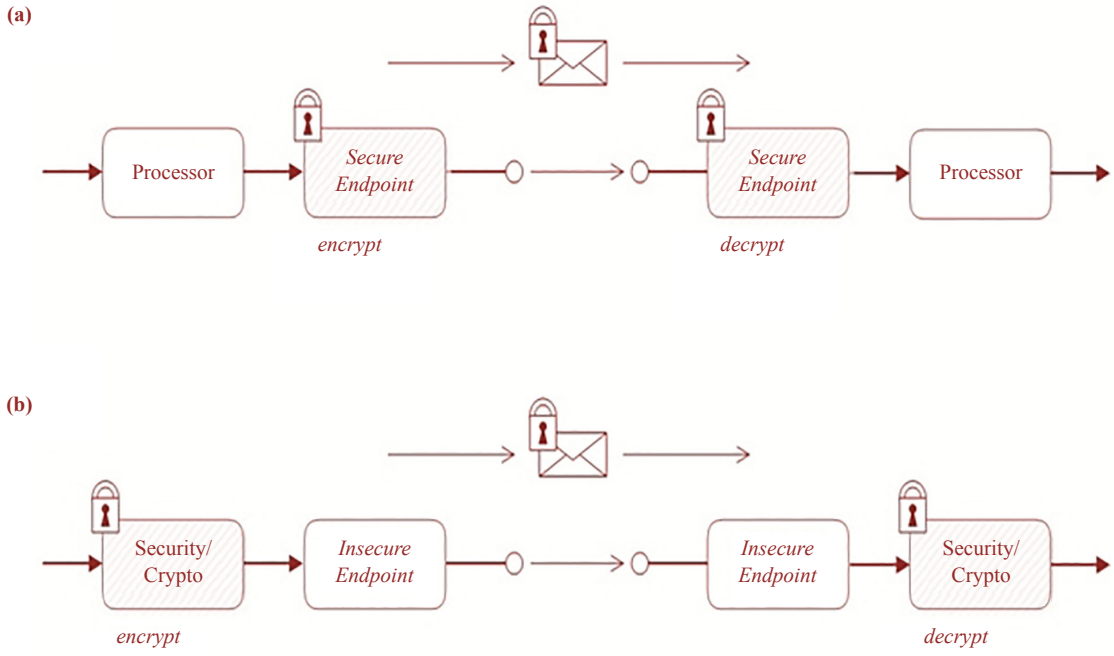

Figure 2. (a) and (b) Apache Camel Security Architecture [18]

Figure 2 The Camel algorithm provides a variety of security options and levels that can be used on Camel routes. These many types of security can be employed in conjunction with one another or on their own. It is simple to create Digital Signatures for Exchanges using Camel cryptographic endpoints and Cryptographic extension. Camel provides a pair of customizable endpoints that work together to establish an exchange signature in one part of the workflow and

then verify the signature in another section of the workflow [18].

Part (a) of the endpoint security diagram depicts a message exchanged between two routers with secure endpoints. The producer endpoint on the left establishes a secure connection with the consumer endpoint on the right (usually using SSL/TLS). In this instance, both endpoints provide security. With endpoint security, it is typically possible to perform some form of peer authentication and sometimes authorization.

The payload security part (b) depicts a message transmitted between two routers with vulnerable endpoints. Use a payload processor that encrypts the message before transmitting and decrypts it after it is received to secure the communication from unauthorized spying in this situation.

3.1 *Proposed design architecture*

3.1.1 *Architecture description*

a) Trento: Trent introduced as a facility, is confided in the party that re-appropriated its foundation to CSP. Liable for introduction, disavowal, key age, and evaluation.

b) Cloud Service Provider: CSP offers types of assistance to clients of key trading. It is an unbelieved element that can acquire a lot of data of the client during confirmation measure where data given by Trent and RS. The client may be ready to conceal their personality from CSP.

c) Registration Server: RS just does the enrollment interaction of the client to start framework entrance. It trades data to Trent and CSP according to mentioned.

d) User/Patients: User gets to the cloud administrations from CSP with approved records to RS. Client solicitations to CSP for administrations without revealing their personality with trading some keys given from Trent (Figure 3).

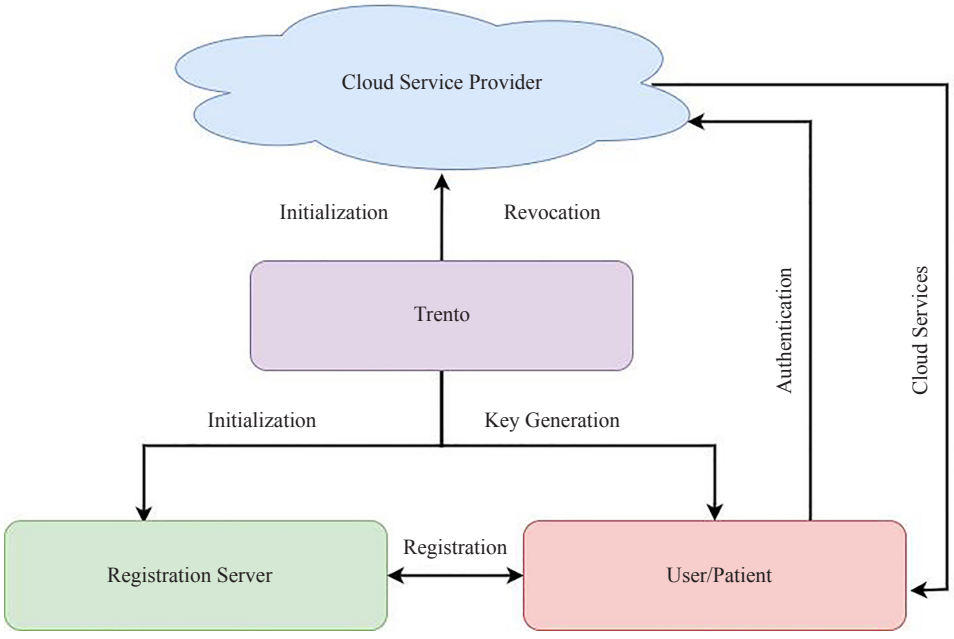

Figure 3. Proposed Design Architecture

3.2 *Proposed design architecture*

Anonymous Authentication scheme includes 5 phases [19]:

1. Initialization
2. Key Generation

3. Registration
4. Authentication
5. Revocation

Initialization: Trent creates a private-public key pair and gives public half to CSP and RS. With a scope of pairings clients should utilize concurred pairings. When Trent sets up the framework, reinstatement is finished.

Key Generation: Trent produces bunch key that substantial for quite a while, ace gathering key and from that infers public gathering key which is somewhat arbitrary and some degree got from bunch chief key. Trent produces a marked endorsement containing data. Trent encodes and sends that endorsement to CSP and RS by utilizing its public key. CSP and RS unscramble and confirm that the authentication is really from Trent with the assistance half open key given past. Trent needs to refresh bunch keys each season of the same key age measure.

Registration: RS presently does the enrollment interaction of the client to start framework entrance. It trades data to Trent and CSP according to mentioned.

Authentication: A user wishes to demand assistance from CSP and starts the verification interaction. The client associates with CSP over an unknown organization and sends the gathering key to verify. CSP checks the gathering key matches a put-away authentication sent by Trent and ought not to be terminated. CSP produces an irregular number and sends it to the client. Client and CSP play out a zero information convention. The client produces a signature and sends it and solicitation to CSP. CSP proceeds to the subsequent stage if the balance remains constant/substantial mark in any case ends the association. CSP additionally makes sure that the client didn't play out the convention with the renounced key. CSP encodes and plays out the mentioned administration with an encryption key and saves it in the review log so that lone Trent might understand.

Revocation: When Trent tracked down that a client has been manhandling the administrations, he disavows the client's vital. Key disavowal fundamentally permits untrusted CSP who keeps a decoded log to interface the entirety of clients' associations and ought not to be utilized essential not by ending a customer's administration. Trent demands the enrollment log and review log from RS and CSP separately and decodes it to get demands. Trent utilizes bunch signature ace key and the rundown of record of interaction to separate which bunch part held marking key to mark the message and burned-through which administration. Trent tests for each record in enrollment log, if a match is discovered, Trent figures the relating boundary and adds it to renouncement log. Trent shares the following data for clients with CSP to disavow client's participation key. To permit CSP to get confirmations of participation made by client and deny offering administrations to him. RS eliminates clients from the rundown of adequate customers when Trent sends the client's character to it.

3.3 *Proposed algorithm*

3.3.1 *Key generation*

Public key and private key generated.
The public key generation equation: $Q = d \times P$
Where k and d is random number selected within the range of (1 to n − 1),
P is the point on the curve and Q public key and d is the private key.

3.3.2 *Encryption*

Input
1. String = message M (plain text)
2. Public key = key Literal types as Plain text, encrypted text Output
1. START
2. Init = (ENCRYPT MODE, key)
3. Plaintext = Input message
4. Encrypted Text-do Final (plaintext)
5. Encrypted String = cipher text cipher text 1 = $k \times P$ cipher text 2 = $M + k \times Q$
6. Return encrypted String.

3.3.3 *Decryption*

Input
1. String = cipher text
2. PrivateKey = key Literal types as Ciphertext, decrypted text Output
1. START
2. Init-(DECRYPT MODE, key)
3. Ciphertext-cipher text
4. Decrypted Text-do Final (cipher text)
5. Decrypted String-message (plain text) M = cipher text 2 d × ciphertext1
6. Return decrypted String (Figure 4)

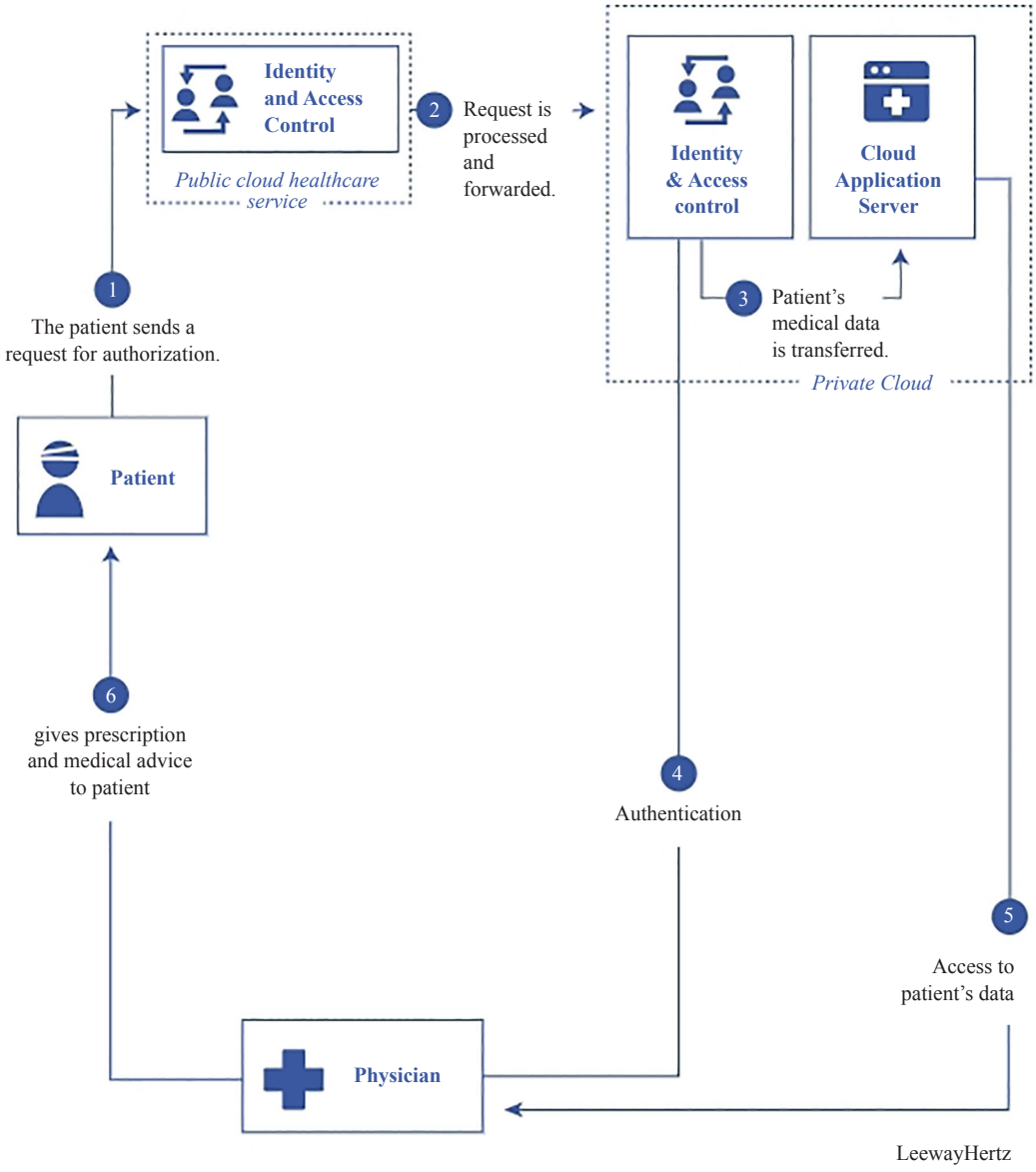

Figure 4. Architecture of private and public cloud communication scenarios [20]

3.4 *Requirement specification*

1. Software Requirements Microsoft Windows 7 and Above Net Beans IDE 8.
2 Java Development Kit (JDK) 1. 7 MySQL 5.5 onwards Application server, Tomcat 5.0
The following steps of cloud-based architecture gives a complete idea of the overall workflow process.

3.4.1 *Stage 1: Patient requests authorization*

Public cloud administrations are tended to exclusively by other clients like patients and outsiders like insurance agencies, drug stores, research medical services organizations, and drug producers. A patient is additionally expected to be an outside client. Thus, the signs on utilizing (username and secret word) addressing public personality and access control cloud administrations to put a solicitation for approval [20].

3.4.2 *Stage 2: Request is prepared at public cloud and sent to private cloud organization*

In light of the solicitation type for capacity, access, or preparing wellbeing information, it is handled at the public cloud level and is sent to the character and access control administration from the private cloud.

3.4.3 *Stage 3: Request is either acknowledged or dismissed*

On the off chance that a private cloud worker acknowledges the solicitation, it is sent to a medical care private cloud application worker. Unexpectedly, if the solicitation is dismissed, an advising message is sent indicating the solicitation's dismissal.

3.4.4 *Stage 4: Physician demands approval*

The doctor is viewed as an inner client. In this way, he signs on to the private cloud benefits and sends an approval demand containing the client and secret phrase to personality and access control.

3.4.5 *The doctor's solicitation is prepared to get the information from the cloud application worker*

When the confirmation is effective, private cloud administrations measure the solicitation, and doctors can get the information from the public cloud application worker.

3.4.6 *A clinical exhortation is straightforwardly shipped off the patient*

A doctor can straightforwardly send criticism as far as clinical counselor medicine to the patient.

Growing such kinds of cloud-based medical care answers for provincial wellbeing and in case of debacles is significant. Also, caregiving organizations and clinical experts should start utilizing cloud-based clinical records and clinical picture chronicling administrations. This sort of arrangement's principal objective is to lessen the difficult undertaking of the specialists and clinical staff worked on clinical frameworks and successful patient consideration [21].

4. Results and discussion

This section discusses the performance evaluation of the implementation of proposed work and compared various algorithms with different features and parameters. In a hospital setting, all of the patient's health information will be gathered. We have created a patient health information form which should be filled out by a nurse or doctor in our suggested job. A table named the health status record will have a complete collection of data (PHR). The PHR is consolidated in the cloud architecture to offer the necessary health data for detection alerts and therapies based on medical professional analysis. IoT is used to integrate networking elements, displays, actuators, sensors, and other healthcare devices and equipment in a multidimensional system. This contributes to the primary trends on the Internet of Things-based medical industry, which focuses on wearable gadgets, robotic surgery, and other cutting-

edge technologies. Experimental results presented in the machine learning field frequently utilize statistical tests of significance to compare learning algorithms. These tests provide a sound response to the issue of whether one machine learning algorithm is superior than another at a given learning task. However, in machine learning contexts, determining the significance statistically is not always simple. Precision is a common metric in many software toolkits for general data analysis and machine learning. Utilizing qualified doctors, pathologists, or radiologists to review medical imaging and identify the underlying causes of clinical diseases is the current clinical standard.

Table 2. Comparison of Features

Features	KG [22]	ECA [23]	H [24]	E_M [25]	Proposed
Anonymity	√	√	√	√	√
Mutual Authentication	√	×	√	√	√
Forward Unlink ability	√	√	×	√	√
Traceability	√	√	√	√	√
Revocation	×	×	√	√	√
Efficient Credential Update	√	√	√	×	√
Communication, Integrity	√	×	√	√	√
Resistance to Modification Attacks	√	×	√	√	√
Resistance to MitM Attacks	√	×	√	√	√
Resistance to Replay Attacks	√	×	√	√	√

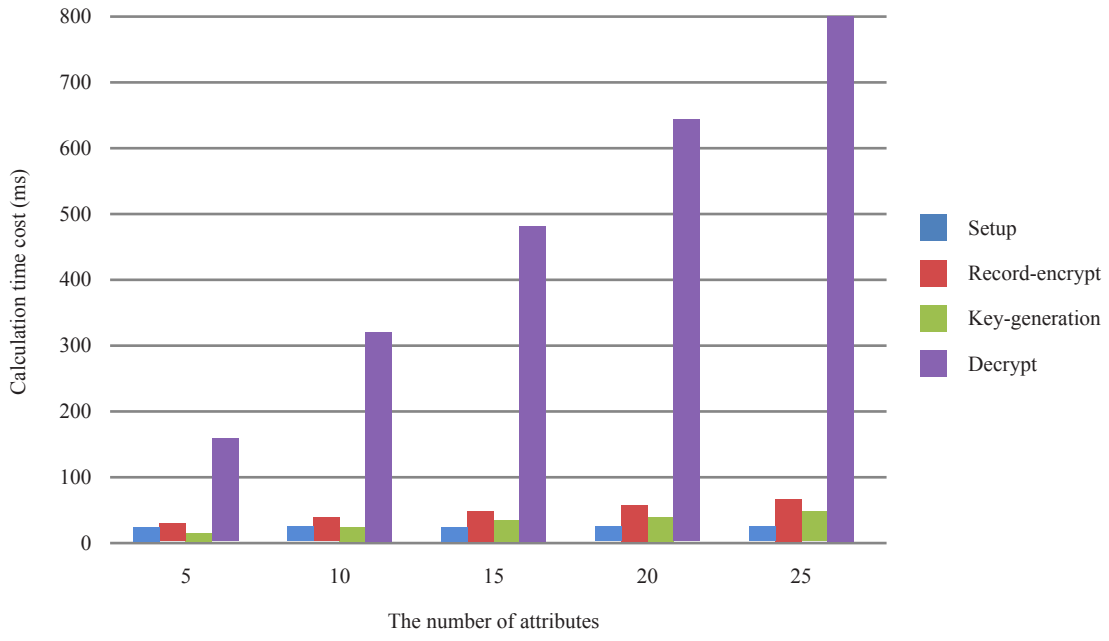

Figure 5. Higher efficiency of all attributes graph for health care system

• KG- Generate public/private key pair
• ECA- Elliptic Curve Addition
• H- Hash Operation
• E_M- Modular Exponentiation

As shown in Table 2, our calculation gives the entirety of the ideal provisions and insurances against assaults. The calculation that comes nearest is that of which needs forward-unlink capacity. It very well may be found in that the pseudo personality created in enlistment is given as a piece of each validation bundle utilized, making the exchanges inconsequentially linkable. Additionally, for a few of the calculations recorded, the issue of accreditation renouncement isn't expressly tended to; nonetheless, in the event that it seems conceivable that the convention could give qualification repudiation, the plan is given to acknowledge for giving denial also. The Figure 5 shows a graphical representation of comparison of a number of attributes with time costs, for the effectiveness of higher efficiency of all attributes of the health care system.

Table 3. Comparison of Execution Time

Cryptographic Operations	Execution Time in ms
KG [22]	625
ECA [23]	496
H [24]	326
E_M [25]	126
Proposed	30

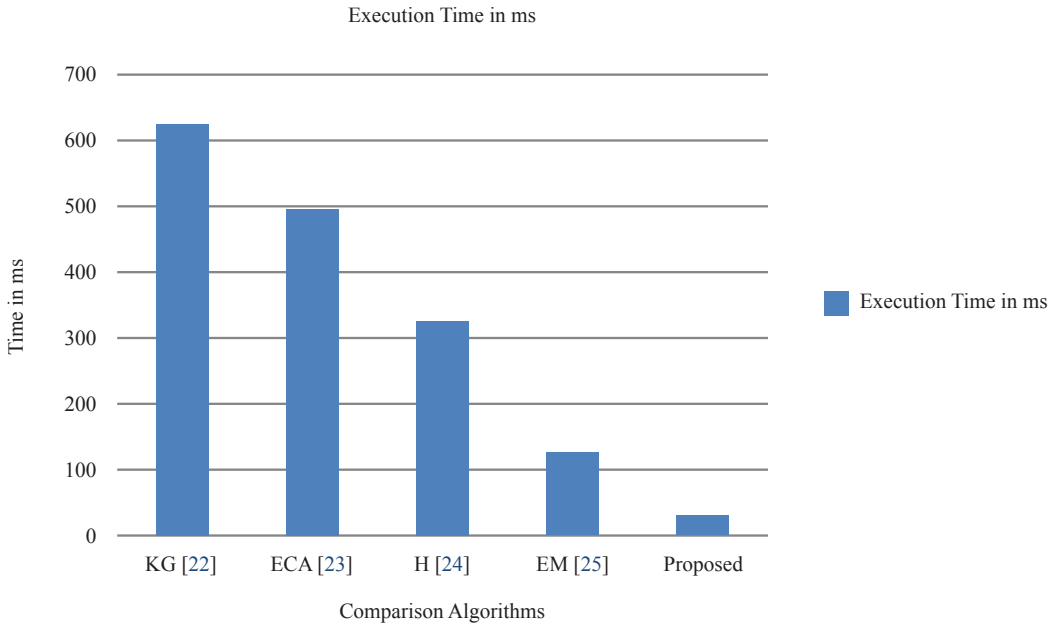

Figure 6. Comparison of Execution Time

Table 3 provides the execution times for each method, which can be used to evaluate the relative complexities.

In the start up and authentication phases, it can be seen that our approach is considerably faster than other algorithms, which is the only other algorithm that has the ability to unlink. In the revocation phase, however, it is slower. The Figure 6 shows a graphical representation of different algorithms execution time's from the reference [22] to [25] compared with proposed algorithm. The Figure 6 shows the effectiveness of proposed algorithm execution time has less than the previous algorithms.

Table 4. Communication overhead for Each Algorithm

Algorithms	Initialization (bits)	Registration (bits)	Authentication (bits)	Revocation (bits)
KG [22]	0	2592	7045	N/A
ECA [23]	544	1952	6914	N/A
H [24]	376	864	1856	N/A
E_M [25]	368	768	1056	N/A
Proposed	1480	576	2368	1024

Then we compare (see Table 4 and Table 5) the algorithms we've looked at based on how many one-way communications are required for each step of the protocol. Table 4 displays the results. The number of patient records to be packaged in a single transmission from the database of physicians is denoted by the integer t in Lin's scheme. For the sake of initialization, it is assumed that each message publication necessitates a single transfer. The Figure 7 shows a graphical representation of different algorithms, communication overhead from the reference [22] to [25] compared with proposed algorithm. The Figure 7 shows the effectiveness of proposed algorithm communication overhead has higher than the previous algorithms.

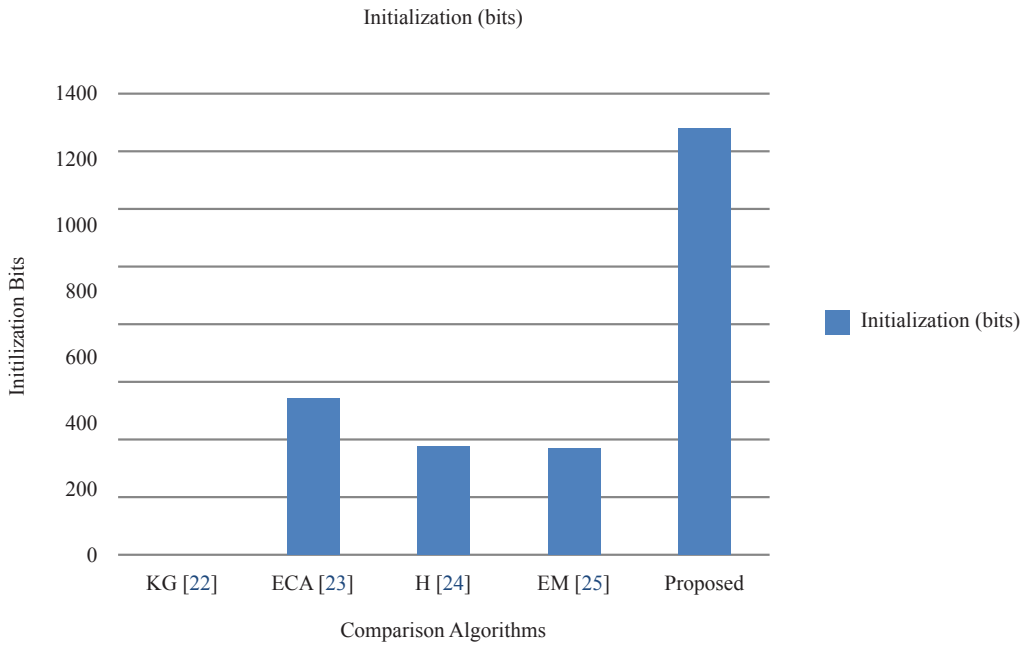

Figure 7. Communication overhead for Each Algorithm

Table 5. Performance validation of proposed with existing algorithm

Parameters	DES [26]	BLOWFISH [27]	AES [28]	Proposed
Network lifetime	150 s	155 s	168 s	195 s
Latency	0.622 ms	0.56 ms	0.5 ms	0.46 ms
Scalability	0.59 ms	0.89 ms	0.73 ms	0.92 ms
Security	87%	82%	95%	97%
Encryption Time	52 ms	43 ms	39 ms	38 ms
Decryption Time	85 ms	82 ms	78 ms	77 ms

Because of the more modest key sizes utilized in Camel, the security of the framework can be effortlessly increased by expanding the critical size without influencing the computational intricacy. The plan adds an additional layer of security against traffic investigation assaults by a snoop by giving secrecy at the organization layer by utilizing TOR. The plan shields patients' delicate information from a snoop and untrusted cloud workers. One notable element of our plan is that the clinical application or specialist organizations can't uncover the character of the patient consequently securing the protection. In this paper, we have planned a viable framework that is secure and proficient. The proposed verification plot guarantees that the patients can devour administrations without uncovering their personality at the hour of utilization or reflectively.

5. Conclusion

The success of smart cloud-based healthcare applications hinges on the protection of patients' privacy. We present an anonymous authentication mechanism for a smart cloud-based healthcare application in this work. Patients' privacy is protected under the proposed approach when they use Cloud services. The proposed work employs a rotating board signature pattern based on a camel. The system fails due to the camel's small key sizes without affecting the computational complexity. This application adds an extra layer of security against a deaf person's traffic analysis attacks by hiring a camel to provide anonymity in the network layer. This application safeguards critical patient information from a deaf person and unstable cloud services. One of the most important aspects of our program is that medical use or service providers are prohibited from disclosing patient identities, ensuring patient privacy. We have devised a realistic, safe, and effective method in this paper. Patients can access the services at the time of consumption or without revealing their identity under the suggested certification process.

Conflicts of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Sowjanya K, Disrupt M, Ray S. An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. *International Journal of Information Security*. 2020; 19: 129-146.

[2] Jain S, Gui Z, Ji S, Shen J, Tan H, Tang Y. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. *Network and Computer Applications*. 2018; 106: 117-123.

[3] Wei F, Vijayakumar P, Shen J, Zhang R, Li L. A provably secure password-based anonymous authentication

scheme for wireless body area networks. *Computers & Electrical Engineering.* 2018; 65: 322-331.
[4] Shim K. Universal forgery attacks on remote authentication schemes for wireless body area networks based on Internet of Thing. *Internet of Things.* 2019; 6(5): 9211-9212.
[5] Hussain SJ, Irfan M, Jhanjhi NZ, Hussain K, Humayun M. Performance enhancement in wireless body area networks with secure communication. *Wireless Personal Communications*. 2021; 116: 1-22.
[6] Rahmani AM, NguyenGia T, Negash B, Anzanpour A, Azimi I, Jiang M, et al. Exploiting smart e-health gateways at the edge of healthcare internet-of-things: A fog computing approach. *Future Generation Computer Systems*. 2018; 78: 641-658.
[7] Kuzhalvaimozhi S, Rao GR. An efficient scheme for anonymous authentication using identity based group signature. *Fourth International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom2012)*. The Institution of Engineering and Technology; 2012.
[8] Lin X, Lu R, Shen X, Nemoto Y, Kato N. Sage: A strong privacy-preserving scheme against global eavesdropping for ehealth systems. *Selected Areas in Commun.* 2009; 27(4): 365-378.
[9] Djellalbia A, Badache N, Benmeziane S, Bensimessaoud S. *2016 Conference on Internetinal Technology and Secured Transactions (IJITST)*. Anonymous authentication scheme in ehealth cloud environment. Barcelona, Spain: IEEE; 2016. p. 47-52.
[10] Li T, Zheng Y, Zhou T. Efficient anonymous authenticated key agreement scheme for wireless body area networks. *Security and Commun Networks*. 2017; 2017(1): 1-8. Available from: https://doi.org/10.1155/2017/4167549.
[11] Liu J, Zhang Z, Chen X, Kwak KS. Certificateless remote anonymous authentication schemes for wireless body area networks. *Parallel and Distributed Syst*. 2014; 25(2): 332-342.
[12] Sudarsono A, Al Rasyid MUH. *2016 Seminar on Intelligent Technology and Its Application*s. An anonymous authentication system in wireless networks using verifier local revocation group signature scheme. Lombok, Indonesia: IEEE; 2016. p. 49-54.
[13] Zhu J, Ma J. A new authentication scheme with anonymity for wireless environments. *Consumer Electron*. 2004; 50(1): 231-235.
[14] Horn G, Preneel B. Authentication and payment in future mobile systems. *Comput Security ESORICS.* 1998; 98: 277-293.
[15] Yang C, Ma W, Wang X. Novel remote user authentication scheme using bilinear pairings. *Lecture Notes in Computer Science.* 2007; 4610: 306-312.
[16] Abi-Char PE, Mhamed A, Bachar E-H. A fast and secure elliptic curve based authenticated key agreement protocol for low power mobile communications. *The 2007 International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST 2007)*. IEEE ; 2007. p. 235-240.
[17] Zhang L, Tang S, Luo H. Elliptic curve cryptography-based authentication with identity protection for smart grids. *PLoS ONE*. 2016; 11(3): e0151253. Available from: https://doi.org/10.1371/journal.pone.0151253.
[18] Gebreyohanes MG, Asse AM. Adaptation mechanisms of camels (camelus dromedarius) for desert environment: A review. *Journal of Veterinary Science & Technology*. 2017; 8(6): 486. Available from: https://doi.org/10.4172/2157-7579.1000486.
[19] Sudarsono A, Al Rasyid MUH. *2016 International Seminar on Intelligent Technology and Its Applications*. An anonymous authentication system in wireless networks using verifier-local revocation group signature scheme. Lombok, Indonesia: IEEE; 2016. p. 49-54.
[20] Joshi A, Mohapatra AK. Authentication protocols for wireless body area network with key management approach. *Discrete Mathematical Sciences and Cryptography.* 2019; 22(2): 219-240.
[21] Tang J, Liu A, Zhao M, Wang T. An aggregate signature-based trust routing for data gathering in sensor networks. *Security and Communication Networks.* 2018; 2018: 1-30. Available from: https://doi.org/10.1155/2018/6328504.
[22] Mehmood A, Natgunanathan I, Xiang Y, Poston H, Zhang Y. *2014 IEEE International Advance Computing Conference (IACC)*. Anonymous authentication scheme for smart cloud based healthcare applications. IEEE Access; 2018. p. 33552-33567.
[23] Sun W, Cai Z, Liu F. *2017 International conference on e-health networking application and services*. A survey of data mining technology on electronic medical records. IEEE; 2017. p. 1-6. Available from: https://doi.org/10.1109/Healthcom40869.2017.
[24] Takyar A. *How does cloud computing impact healthcare industry*? LeewayHertz. Available from: https://www.leewayhertz.com/cloud-computing-in-healthcare/ [Accessed 20th March 2022].
[25] Red Hat Fuse. *Apache Camel Security*. Red Hat Customer Portal. Available from: https://access.redhat.com/documentation/enus/red_hat_jboss_fuse/6.2/html/security_guide/arch-architecture-camel
[26] Hossain MS, Muhammad G, Guizani N. Explainable ai and mass surveillance system-based healthcare framework

to combat covid-i9 like pandemics. *IEEE Network*. 2020; 34(4): 126-132.
[27] Yang G, Jan MA, Menon VG, Shynu PG, Aimal MM, Alshehri MD. A centralized cluster-based hierarchical approach for green communication in a smart healthcare system. *IEEE Access*. 2020; 8: 101464-101475.
[28] Raj J, Shobana S, Pustokhina I, Pustokhin D, Gupta D, Shankar K. Optimal feature selection-based medical image classification using deep learning model in internet of medical things. *IEEE Access*. 2020; 3: 58006-58017. Available from: https://doi.org/10.1109/ACCESS.2020.2981337.