Computers, Materials & Continua
DOI: 10.32604/cmc.2023.027992
Article

A Secure Multi-factor Authentication Protocol for Healthcare Services Using Cloud-based SDN

Sugandhi Midha[1], Sahil Verma[1,*], Kavita[1], Mohit Mittal[2], Nz Jhanjhi[3,4], Mehedi Masud[5] and Mohammed A. AlZain[6]

[1]Department of Computer Science and Engineering, Chandigarh University, Mohali, 140413, India
[2]Chandigarh Engineering College Jhanjeri, Mohali, 140307, India
[3]School of Computer Science and Engineering, SCE, Taylor's University, Subang Jaya, 47500, Malaysia
[4]Center for Smart Society 5.0 [CSS5.0], FIT, Taylor's University, Subang Jaya, 47500, Malaysia
[5]Department of Computer Science, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[6]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
*Corresponding Author: Sahil Verma. Email: sahilverma@ieee.org
Received: 30 January 2022; Accepted: 15 April 2022

Abstract: Cloud-based SDN (Software Defined Network) integration offers new kinds of agility, flexibility, automation, and speed in the network. Enterprises and Cloud providers both leverage the benefits as networks can be configured and optimized based on the application requirement. The integration of cloud and SDN paradigms has played an indispensable role in improving ubiquitous health care services. It has improved the real-time monitoring of patients by medical practitioners. Patients' data get stored at the central server on the cloud from where it is available to medical practitioners in no time. The centralisation of data on the server makes it more vulnerable to malicious attacks and causes a major threat to patients' privacy. In recent days, several schemes have been proposed to ensure the safety of patients' data. But most of the techniques still lack the practical implementation and safety of data. In this paper, a secure multi-factor authentication protocol using a hash function has been proposed. BAN (Body Area Network) logic has been used to formally analyse the proposed scheme and ensure that no unauthenticated user can steal sensitivepatient information. Security Protocol Animator (SPAN)–Automated Validation of Internet Security Protocols and Applications (AVISPA) tool has been used for simulation. The results prove that the proposed scheme ensures secure access to the database in terms of spoofing and identification. Performance comparisons of the proposed scheme with other related historical schemes regarding time complexity, computation cost which accounts to only 423 ms in proposed, and security parameters such as identification and spoofing prove its efficiency.

Keywords: Multi-factor; authentication; hash function; BAN logic; SPAN-AVISPA

1 Introduction

Competitive advantages of Software Defined Network (SDN) [1] over a traditional network have made it extensively used by any organization to set up their network. SDN has become more valuable with its cloud-based integration. With the rise in the number of chronic diseases and conditions, demand for health care systems is also growing. The increase in consumption diseases and the old age population also need due care and health monitoring from time to time. An increase in consumption of convenience food is also steadily causing health problems. A sedentary lifestyle and desk-bound jobs have raised obesity and diabetes level. Another addition to this has been made by the global pandemics like COVID-19, SARS, HIV-AIDS, F3N2, Spanish Flu, and Cholera to name a few.

The unavailability of expert medical practitioners (MPs) or costly treatment has given birth to remote patient monitoring (RPM). Patients at home feel more comfortable and prefer to be monitored from home [2] than going to THE hospital. RPM enables patient monitoring outside the conventional hospital and clinical settings. It helps reduce the treatment cost, but patients also get free from the hassle of traveling. It helps in improving and providing quality of life to patients all over the world.

The flexibility and ease of using various pervasive technologies like Wireless Medical Sensor Network (WMSN), Cyber-Physical System (CPS), Cloud, IoT, SDN, and Wireless Body Area Network (WBAN) has given use to usage of Remote Tele-Patient Monitoring (RTPM). RPM collect health and medical data of patients with the help of digital technology. Patients wear different sensors or patches through which data is electronically transferred and stored onto a cloud-based SDN [3]. Tele-health solutions are provided to patients in no time. Fig. 1 demonstrates the typical architecture for RPM which is followed by the schemes [4,5].

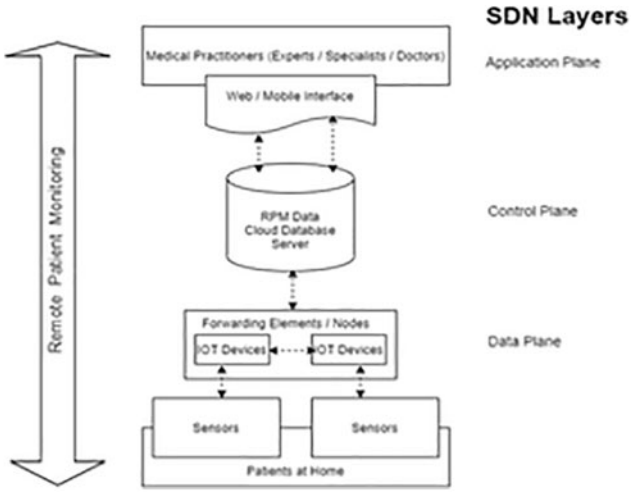

Figure 1: RPM architecture with cloud-based SDN

A WBSN for observing various Patients' Physiological Parameters (PPPs) such as blood glucose levels, BP, ECG, pulse rate, etc. indicates the patient's current health [6,7]. Monitoring is required in real-time due to the criticality of the situation. Moreover, reducing the economic burden, preserving the privacy of patients' data is equally important. MP can access the data from the cloud-based SDN servers from anywhere at any time. But the major concern is where Cloud Service Providers provide IoT services over an insecure public channel to customers [8]. Patients' data is vulnerable to attacks and should be securely accessible to authenticated practitioners. The whole concept is to put the patient's

sensitive data in the public cloud and trust it is a major concern. The main hindrance in the adoption of cloud-based SDN by healthcare providers is security, confidentiality, and trust issues [9].

Together, all these factors have worked as a driving force for us to propose "A secure multi-factor authentication protocol for healthcare services using Cloud-based SDN". The Cloud-based SDN [10,11] combines the advantage of both SDN and Cloud offering a new revolution to the technological world in terms of efficiency and practicality. To ensure the confidentiality and privacy of patients' data, the proposed novel heterogeneous communication architecture provides a multifactor authentication policy. The proposed scheme exploits customized SDN and a framework [12–14] of body sensors coupled with IoT nodes, Cloud Analytics support for smart summarisation.

1.1 Motivation & Contribution

Various economic and availability issues that given gear to health services. Cloud-based SDN [15] has widespread deployment in this field. Patients' data may get compromised on cloud servers and is prone to various attacks such as Denial of Service (DoS), Man in the Middle (MITM) attack, replay, phishing, etc. The unauthorized access can manipulate SDN control and application plane southbound and northbound interfaces. Once the health data has been compromised that is compromised forever: Patient's health can suffer and life is at stake. Security remains a major concern in any domain. But It has a major role to play in terms of patients' privacy. The proposed scheme is capable enough to deal with illegitimate user access to cloud-based SDN database servers. The primary aim of this work is to present a guaranteed authentication scheme for real time health system. A protocol which overcomes the drawbacks of high communication cost and high computation overhead over existing protocols.

This research contributes as below:

- Users' role is an important measure for defining security privileges. Different levels of privileges provide secure access to users. New flow entries are generated by ensuring the implementation of real-time policies.
- The authorization & authentication principle helps the SDN Controller to lay the network policies.
- IAM policy implementation ensures the role-based policy for security privileges.
- Various network metrics and measures work as a performance indicator for the network and ensure the quality of service in the transmission flow & resources across.
- AVISPA tool has been used to prove the strength of various security parameters.
- The superiority of the scheme in comparison with the existing one has been proved over computational cost and various securities attack parameters.

1.2 Paper Organization

The remaining paper is structured in the following manner. Section 2 critically reviews the existing authentication schemes in the health sector regarding the three technological dimensions of cloud, SDN, and IoT. In Section 3, various security threats and attacks on the cloud-based SDN architecture have been presented. Section 4 explains the proposed scheme architecture in detail. In Section 5, a detailed analysis of the proposed scheme has been performed using AVISPA. Section 6 includes the performance analysis of the proposed scheme with the existing ones. Finally, Section 7 presents the conclusion.

2 Related Work

This section gives existing methods used in the literature review for this research. In this different research work and conducted study has been discussed. The proposed method's significance to solve the given threats has been introduced. A critical review of the existing authentication schemes and security in the health sector regarding the three technological dimensions of cloud, SDN, and IoT has been conducted as depicted in Fig. 2.

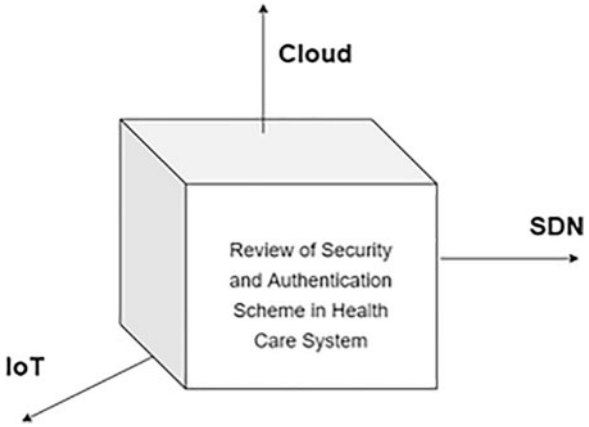

Figure 2: 3D analysis of security and authentication scheme in health care systems

2.1 Review of Security in the Healthcare Sector about Cloud Computing

A virtual machine (VM) has been created as a cloud server that fetches the data from IoT nodes as depicted in Fig. 1. Data is routed to the cloud data centers and cloud servers process the data smartly and provide the information to the MPs through web or mobile query interface. SDN centralized controller manages the distributed cloud architecture and acts as a one-stop honey pot for the attackers. Cloud-based SDN offers flexibility, agility, programmability, scalability, and economic infrastructure. Cloud-Based SDN centralised control causes several threats such as unauthorised access, data tampering, phishing, DoS attacks, etc. as mentioned by Heidelberg in [16]. Sinanc et al. [17] mentioned how the availability and reliability of information will largely be affected due to internal loopholes in the usage of internet connection. Another obstacle may be of interoperability of devices due to the lack of common communication standard which is required for collaboration with healthcare services as presented by Midha et al. in [9,18]. An open and shared environment of cloud-based SDN hampers the security and privacy of patient's data found by Abukhousa et al. in [18], C. Networks [19] have claimed that the cloud is prone to various security attacks. Abbas et al. [5] and Ahuja et al. [20] have mentioned that healthcare providers lack trust in Cloud-based SDN servers due to security and privacy breaches which hinder its adoption.

2.2 Review of Security in the Healthcare Sector Concerning SDN Interfaces

Referring to Fig. 1, communication between the application layer and the control layer is performed with the help of RESTful or native Java APIs, which are termed as North Bound Interfaces (NBIs) in SDN. The non-standardized and diverse nature of NBIs in SDN makes it more challenging to handle in front of security. The various OpenFlow switches available in the market possess limited Content Addressable Memory [19]. In case, NBIs fail to put integrity constraints on the operations of various network applications; malicious applications come and replace existing high priority flow

entries rules with low priority rules on the data plane [21]. Malicious applications inject rules in the absence of constraints but also edit and delete the existing flow rules resulting in network performance degradation and overall data leakage [22] through poor NBI management. As depicted in Fig. 1, South Bound Interfaces (SBIs) are responsible for communication between the data plane and control plane. A packet_in message is generated for the SDN controller in response to each captured packet on the network. Any malicious attacker can forge IPs and MACs and can initiate data transfer in the network. Whenever the packet comes into the network, the OpenFlow switch will treat it as a new flow and generate a packet_in message for SDN Controller. Too many packet_in messages to SDN Controller [23] make the SDN Controller unavailable for legitimate users. So DoS and DDoS [2,8,24] is considered to be the major threat to the controller.

2.3 Review of Security in the Healthcare Sector Concerning IoT

Zhihan et al. [25] have listed that usage of IoT devices triggers trust, privacy, and security issues in the exchange of healthcare data. Hosseini Khayat [26] have presented potential hazards related to IoT devices' security, integrity, availability, and privacy implications. Yan et al. [27] have mentioned that security attacks such as hampering safety and utility are pervasive in IoT devices and patients' security is endangered. Various studies [20,28] have shared the vulnerability of IoT devices to security attacks.

2.4 Review of Authentication Schemes in Health Care Systems

Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) as mentioned in [29] controls illegitimate access on the database servers. This mainly implies access rights and privileges and is one of the most widely used techniques in the healthcare system. A lot of work has been done regarding security and privacy in health systems.

Midha et al. [15] in his work proposed a protocol based on generating a session key for accessing health care data with fog computing. Reference [30] in their work have shown that computational cost has been compromised to ensure strong security. C. Networks [19] have presented a novel approach to Shamir's Secret Share Scheme (SSS) to access cloud data to ensure protection from data loss, protect data loss and illegitimate access, and privacy disclosure. Health data confidentiality is ensured using the SSS technique for encrypting data. C. Networks [19] have discovered that the technique does not present the trade-off between efficiency and security.

Tseng et al., [21] have introduced a model by proposing a group-based access structure and Cipher text-Policy Attribute-Based Encryption (CP-ABE) to cater to the issue of data confidentiality and access privacy over health data. Ghosh et al., [13] have demonstrated that neither the technique is efficient nor practically implacable.

Narayana et al., [22] have proposed a 3 factor model for ensuring authenticity–(i) Cryptographic role-based technique. (ii) Location and Biometric based Authentication. (iii) A wavelet steganography to ensure the trust of patients on cloud data. Method ensures the resilience from MITM and replay attacks. But as mentioned in Shin et al., [24], the method does not ensure the integrity and availability of ehealth data and computational overhead is high.

Yan et al. [27] have deployed cloud-based privacy-aware role-based access control (CPRBAC) model which guarantees low computational complexity and communication cost. But the method does not ensure the protection of data in terms of privacy attacks as mentioned in [26]. Narayana et al. [22] have proposed a framework based on public key infrastructure (PKI) claiming that methodology ensures confidentiality, integrity, authenticity, availability, and suitability.

Ahuja et al., [20] have proposed an architecture for ensuring privacy in ehealth infrastructure by using Trusting Virtual Domains (TVDs). In [29], it has been presented that architecture still does not address various issues related to authenticity, anonymity, and non-repudiation.

2.5 Limitations of the Previous Studies

- Most of the existing techniques failed to provide mutually strong authentication.
- TLS/SSL security is optional in most of the techniques due to the OpenFlow nature of SDN.
- Authentication schemes are mostly implemented on IoT nodes and gateway but MPs get direct access to data servers without authenticity.
- Most of the techniques lack sharing of updation status with other devices.
- Most of the techniques lack security in terms of non-repudiation, key freshness, and anonymity.

3 Security Issues and Requirements on the Cloud-based SDN Architecture

This section of the paper presents the various security threats prevailing on the electronic health records (EHR) on the Cloud-based SDN and the security requirements that are expected of the proposed approach.

3.1 Security Issues

Open flow communication has been supported by making Transport Layer Security and Secure Socket Layer (TLS/SSL) an optional part but it has brought a serious threat to communication interfaces. Traffic can be easily intercepted on the communication interface lines which will lead, leading to several attacks like an exploit, malware, data leakage, etc. No end-to-end encryption scheme has been adopted in this, which increases the chances of an attack on data and messages. Tab. 1 shows the various risk categories in Cloud-based SDN and their description.

Table 1: Simple risk categories

Risk	Risk description
Insider	Accidently an Authenticated and authorised user may tamper EHR when the user is trying to perform some legitimate action.
External attack	An unauthenticated or unauthorised user may temper the data and resources through illegitimate access.
Data access	An attacker may be so strong that it can breach the access policies or can enter into the network by faking its identity. Attackers can either tamper with or steal the EHR.
Data leakage	Data is personal and confidential, and it may leak to the illegitimate user.
Exploit	There may be loopholes in the network system; which an attacker can exploit to access data and resources.
Malware	Using the loopholes of the network system, malicious code can be injected inside the Cloud-based SDN flow which may lead to serious damage to patients' data and information.
Denial of service	Any illegitimate user/users may overburden the server to bring it down. In this case, the server even won't respond to legitimate users.

(Continued)

Table 1: Continued

Risk	Risk description
Traffic hijacking	An attacker may intercept the flow entries of OpenFlow tables which leads to the hijack of network information and data.
MITM attack	An adversary may listen to the conversation between the user and the application and may temper the patient information or later may use it to affect the network.
Replay attack	It is also known as a playback attack where an attacker may repeat the data transmission maliciously or delay it.
Impersonation attack	An adversary may present itself as a trusted party and steal sensitive patients' information.

3.2 Security Requirements

Following are the requirements that the proposed scheme should possess:

i) Confidentiality: The patient's data is confidential and personal. The patient may not want to share it with any other person. So measures should be used to ensure that no outsider or external can get access to a patient's data.
ii) Integrity: Checks and conditions should be enforced to ensure data consistency and accuracy.
iii) Availability: EHR should be available to the right users at the right time. Backup should be maintained so that in case of any failure, data can be recovered.
iv) Mutual Authentication: Cloud-based SDN servers and MPs should be independently capable of generating shared sessions before the information exchange.
v) User Anonymity: Protocol must ensure that the user identity remains hidden from the attacker so that it can represent itself as a legitimate user.
vi) Forward Secrecy: Freshness of the message should be preserved by using timestamp nonces etc. to avoid replay attacks.
vii) Scalability: The scheme must ensure scalability due to clouds and IoT which shows tremendous growth over time.

4 Proposed Scheme

The proposed scheme follows a 3-way handshake–connection establishment, data transfer, and connection termination to ensure the secure transmission of data and no loose open connection. Tab. 2 mentions the notations used in paper.

Table 2: Symbol/variable notations

Symbol/variable notation	Description
MP	Medical practitioner
Ser	Server
uid	User identity

(Continued)

Table 2: Continued

Symbol/variable notation	Description
pwd	Password
bio	Biometric imprint
NMP	Random number nonce
TS	Time stamp
S	Secret message
$\oplus$	XOR operation

The connection Establishment phase is further divided into 3 sub-phases to ensure user authenticity. This phase ensures that the identified user is valid and has access to the cloud server's patients' database. The proposed Scheme has been depicted in Fig. 3.

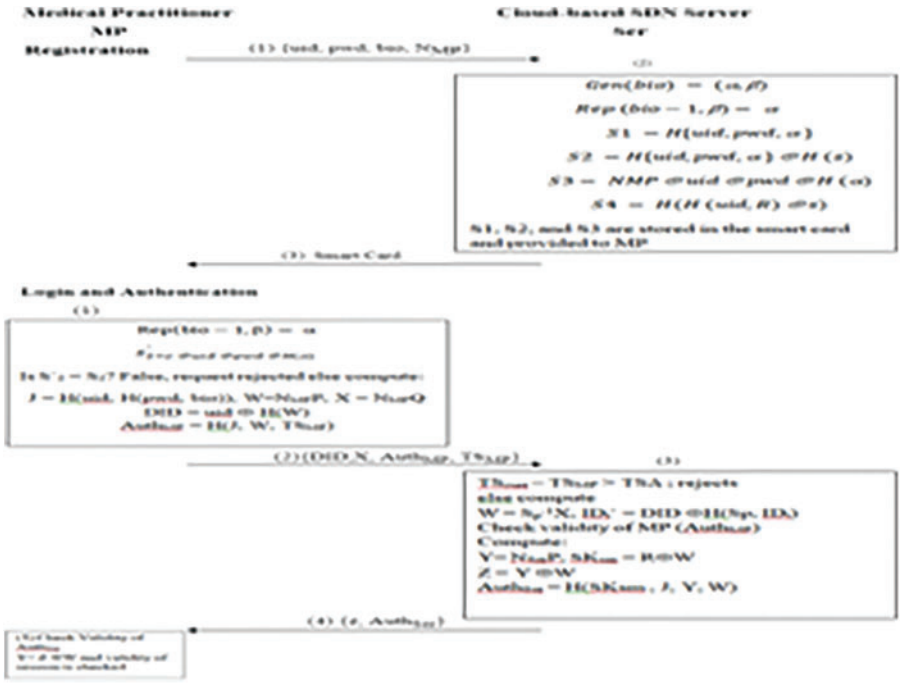

Figure 3: Proposed authentication phases

a) Registration phase: MPs choose user id (uid), password (pwd), and biometric imprint (bio) and send it as a challenge to the SDN-based Cloud sever (Ser). Bioimprint is generated using alpha and beta as in Eq. (2). MP also generates a fresh random number a nonce (N_{MP}) or timestamp to ensure the freshness of the message. All this information is sent by the MP to Ser as depicted in Eq. (1) over a secured hash channel using the hash function of Eq. (4).

$$S = MP \rightarrow Ser\colon \{uid, pwd, bio, \text{NMP}\} \tag{1}$$

$$Gen(bio) = (\alpha, \beta) \tag{2}$$

α, β are two arbitrary strings generated such as mentioned in Eq. (3).

$$Rep(bio - 1, \beta) = \alpha \tag{3}$$

$$H(S) \oplus NMP \tag{4}$$

On receiving user id (uid), password (pwd), and biometric imprint (bio), the Server (Ser) performs the validity check to ensure the correctness of the user and answers to the challenge sent by the MP.

$N^{-1}{}_{MP} \oplus N_{MP}$ to ensure the freshness of the message and generates the smart card with the uid, pwd and bio for the user and sends to MP and stores the information in the DB server for authentication later as depicted in Eqs. (5) and (6).

$$S0 = Ser \rightarrow MP\colon \{smart\ card, NSer\} \tag{5}$$

$$H(S0) \oplus NSer \tag{6}$$

To send the smart card information to the MP and store required information onto its memory, Ser performs Eqs. (7) to (10).

$$S1 = H\{uid, pwd, \alpha\} \tag{7}$$

$$S2 = H\{uid, pwd, \alpha\} \oplus H(s) \tag{8}$$

$$S3 = NMP \oplus uid \oplus pwd \oplus H(\alpha) \tag{9}$$

$$S4 = H(H(uid, R) \oplus s) \tag{10}$$

S1, S2, and S3 are stored in the smart card and provided to MP to use as validation medium to access the patients' data. The Ser stores S4 in its memory for the future verification process.

b) Login and Authentication phase: Once the MP has registered him/her onto the cloud Server; Later S/He can access the patient's data with the smart card which works as user authenticity. In this process, both the MP and Ser mutually authenticate each other. Various properties ensured in this phase are

- Message 'S' is secret means encrypted over a secure hash channel.
- N_{MP} is fresh so is message 'S'
- Ser authenticates 'S' built by MP
- MP authenticates the Ser during the session with the session key

On received uid, pwd, and bio from MP; α information is extracted from the smart card using Eqs. (11) and (12).

$$\text{Rep}(\text{bio} - 1, \beta) = \alpha \tag{11}$$

$$S'_{2=c\oplus uid\oplus pwd\oplus H(\alpha)} \tag{12}$$

Is $S'_2 = S_2$? If the user is authenticated the login request is sent to Ser with timestamp (TS) as specified in Eq. (13).

$$Smart\ card \rightarrow Ser\colon \{MPid, TS\} \tag{13}$$

On receive MP will check TS of a message with T_{curr}; If it is less than equals allowed threshold time $T\Delta$; access to patient's data is granted else server will reject login. And similarly, the message flows from the Ser to MP and the entire verification validation process is repeated at the MP to guarantee mutual trust.

5 Security Analysis

An analysis of the proposed protocol has been performed using the AVISPA tool on the VM.

5.1 Formal Verification Using Span-AVISPA

AVISPA is a modular automated tool which validates internet security protocols and applications. It specifies security protocols and their properties in formal language. It offers robustness and scope with a large library set.

AVISPA tool has been used for the formal analysis of the proposed technique. High-Level Protocol Specification Language (HLPSL) has been used for documenting the scripts based on the roles of Medical Practitioners and Cloud-based SDN servers. Scripts written in the HLPSL are translated to the Intermediate Format (IF) by the translator. IF is inputted to the four different backends named as On-the-fly Model-Checker (OFMC), Constraint-Logic based Attacker Searcher (CL-AtSe), SAT-based Model-Checker (SATMC), and Tree Automata-based Protocol Analyser (TA4SP) to analyse the fulfillment or violation of security goals. Fig. 4 depicts the structure of the AVISPA tool [13].

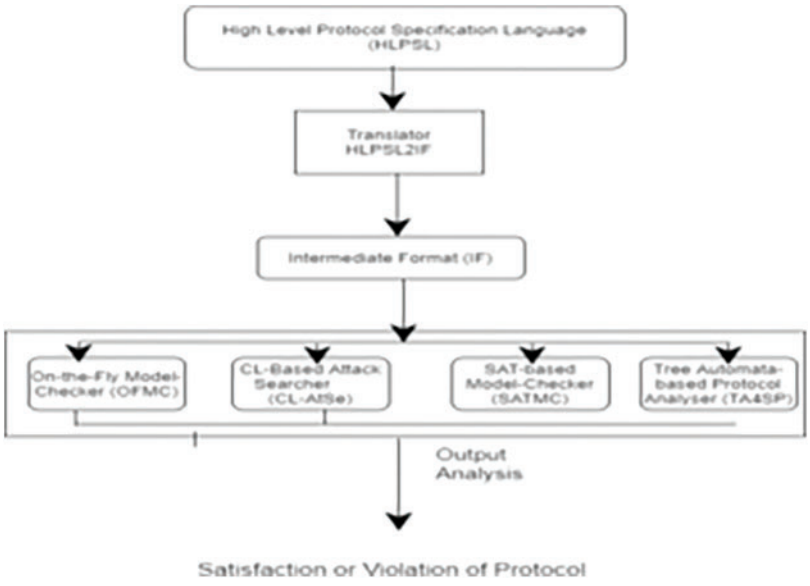

Figure 4: AVISPA tool architecture

Proposed secure protocol method has been tested under worst assumptions also. Message has been tampered, server attacks has been conducted by exploiting loop holes in the system. Replay attack has been conducted which mostly go unnoticed. AVISPA tool has been used to develop a secure protocol. AVISPA integrated with different backends to exhibit the secure protocol. Proposed Protocol follows the process as exhibited in Fig. 5.

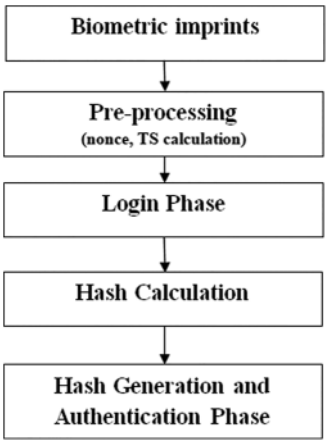

Figure 5: Proposed protocol method

AVISPA architecture is role-based. The various roles played in the ehealth care architecture are MPs, Cloud-based SDN Server, Session, Environment, and goal are defined in the HLSPL. Fig. 6 represents the session key execution for the protocol and proves the validity of the protocol in terms of its safety during the attack.

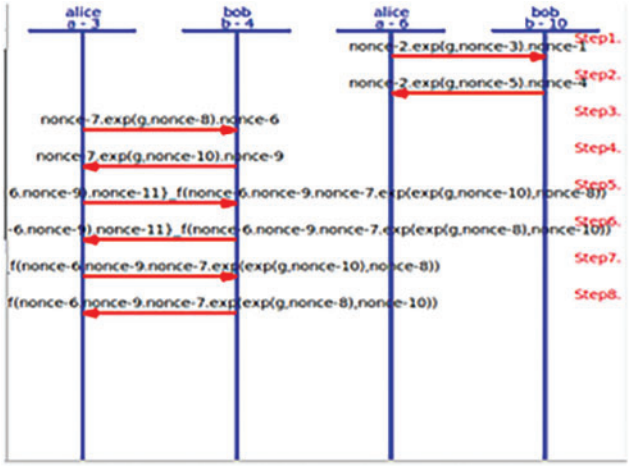

Figure 6: User authentication with nonce

5.2 Informal Verification and Theoretical Analysis

This section defines the important theoretical analysis of the proposed scheme against the attacks and various security issues prevailing on patients' data as discussed in Section 3.1. Tab. 3 defines the verification of the proposed tool which shows the validity of the tool over several security requirements.

Table 3: Informal protocol verification

Security requirement	Protocol verification
Data Confidentiality (DC)	Messages are protected using Hash Function and a layer of cryptography is performed using XOR operation. Random number W and M has been chosen through the polynomial function and is comparably infeasible to detect. Independent generated session keys add an extra layer of confidentiality to maintain the privacy of patients' data.
Mutual Authentication (MA)	Both MP and Cloud Server need to auth themselves before the data transmission.
User Anonymity (UA)	User identity is masked using a hash function and is labeled as DID which ensures the anonymity of the user.
Key Freshness (KF)	Time Stamps are generated to ensure the validation of messages at both the ends of Cloud Server and MP.
Data Integrity (DI)	As depicted in the results of Figs. 5 and 6, the protocol is safe from attackers and intruders.
Availability	Legitimate MP always gets access to the Patients' data based on its role.
Scalability (SC)	Cloud-based SDN server provides the flexibility and scalability to add new patients.
DoS, Message replay Attack (MRA)	Key freshness and time stamps help in protecting the message from being resent.
Impersonation attack (IA)	MP and user are authenticated with fresh session keys and smart card which avoids stealing of identities by illegitimate users.
MITM	A smart card verification scheme makes it impossible for the attacker to crack the authentication process.
Practicality (P)	The proposed technique has been simulated on the AVISPA tool.

6 Performance Comparison

This section presents the comparison of various security features of the proposed protocol and related protocol as shown in Tab. 4. It has been observed that all the existing protocols suffer from one of the other security weaknesses. The proposed scheme ensures the fulfillment of all the security requirements and is safe from intruders and attackers.

Table 4: Performance comparison of proposed scheme and existing protocols

Property	Hamid et al.	Marwan et al.	Smithamol et al.	Ibrahim et al.	Shah and Prasad	Lohr et al.	Proposed
DC	√	√	√	√	X	X	√
MA	√	√	√	√	X	X	√
UA	√	√	√	√	√	X	√
KF	√	√	√	√	√	√	√

(Continued)

Table 4: Continued

Property	Hamid et al.	Marwan et al.	Smithamol et al.	Ibrahim et al.	Shah and Prasad	Lohr et al.	Proposed
DI	√	√	X	X	√	√	√
SC	√	√	√	√	√	√	√
DoS	√	√	√	√	√	√	√
MRA	X	X	√	√	X	√	√
IA	√	X	X	√	√	√	√
MITM	√	X	√	√	√	√	√

Session key generated by Yan et al., [27] in his work lacks message replay attack support and does not maintain key freshness which leads to MRA and in turn responsible for DoS attacks. Hosseini-Khayat [26] in his secret share scheme is not able to ensure the integrity of the message and is suffered from a MITM attack. Ghosh et al. [13] intheir work on CP-ABE could not protect data from impersonating attack loop-hole in the system. 3-factor model [29] ensure the safety from DoS [3], MITM and MRA attacks but does not ensure data integrity.

CPRBAC model [28] does not ensure privacy and confidentiality which should be an integral part of the patients' database system. Zhihan et al., [25] architecture is weak in terms of data confidentiality, mutual authentication, and user anonymity. The proposed architecture ensures the validation of each qualitative metric and computation cost.

Tab. 5 represents the computation cost (ms) for the proposed and existing protocol schemes. Fig. 7 shows that the proposed scheme is best in the case of security requirements and ensures efficiency in terms of computation cost. Results have been derived using simulation on AVISP.

Table 5: Computation cost

Efficiency	Hamid et al.	Marwan et al.	Smithamol et al.	Ibrahim et al.	Shah and Prasad	Lohr et al.	Proposed
Computation cost (ms)	729	748	534	578	632	654	423

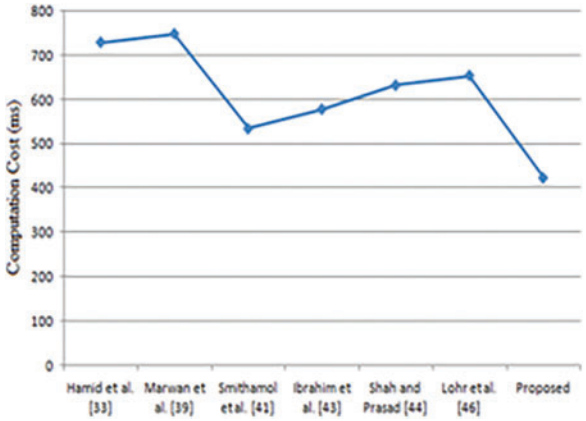

Figure 7: Performance comparison–computation cost (ms)

7 Conclusion and Future Work

Remote Health Monitoring System (RHMS) provides ease for treating patients anytime and anywhere. Patients' data on the Cloud-based SDN server has greater scope in terms of flexibility and scalability. Still, security is a major issue where it is difficult to keep patients' sensitive data secure. Patients' information may compromise which may lead to poor health management. Our Proposed Protocol maintains key freshness and data integrity through biometric imprints, nonce and timestamp calculation for each transaction. Our proposed protocol focused on all the authentication issues and updated all the security patches to ensure the secure access of patients' records. The proposed protocol is proactive to all the security threats and provides guaranteed access to legitimate users. Our proposed protocol does not only provide security but is also efficient in terms of computation cost over existing protocols. Verification has been done by the widely used and accepted tool AVISPA. However, the proposed method deals with all the proactive measures related to security threats; a lot more work can be done in terms of tampering and repudiation in terms of patient data. The future work includes the implementation of the protocol on the real-time testbed and major improvements in terms of tampering and repudiation threats.

Funding Statement: Taif University Researchers Supporting Project number (TURSP-2020/98), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Midha, G. Kaur and K. Tripathi, "Cloud deep down—SWOT analysis," in *IEEE 2nd Int. Conf. on Telecommunication and Networks (TEL-NET)*, pp. 1–5, 2017.

[2] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," *Elsevier Computer Networks*, vol. 54, no. 15, pp. 2688–2710, 2010.

[3] S. Midha and K. Tripathi, "Assessing the quality of service of POX controller in SDN," *International Journal of Computational Engineering Research (IJCER)*, vol. 8, pp. 21–25, 2018.

[4] Y. Al-Issa, M. A. Ottom and A. Tamrawi, "EHealth cloud security challenges: A survey," *Journal of Healthcare and Engineering*, vol. 2019, no. 1, pp. 1–15, Article id-7516035, 2019, https://doi.org/10.1155/2019/7516035.

[5] A. Abbas and S. U. Khan, "A review on the state-of-the-art privacy-preserving approaches in the e-Health clouds," *IEEE Journal of Biomedicine Health Informatics*, vol. 18, no. 4, pp. 1431–1441, 2014.

[6] X. R. Zhang, W. F. Zhang, W. Sun, X. M. Sun and S. K. Jha, "A robust 3-D medical watermarkingbased on wavelet transform for data protection," *Computer Systems Science & Engineering*, vol. 41, no. 3, pp. 1043–1056, 2022.

[7] X. R. Zhang, X. Sun, X. M. Sun, W. Sun and S. K. Jha, "Robustreversible audio watermarking scheme for telemedicine and privacy protection," *Computers, Materials & Continua*, vol. 71, no. 2, pp. 3035–3050, 2022.

[8] B. Wang and M. Ma, "A smart card-based efficient and secured multi-server authentication scheme," *Wireless Personal Communication*, vol. 68, no. 2, pp. 361–378, 2013.

[9] S. Midha, K. Tripathi and M. K. Sharma, "Practical implication of using dockers on virtualised SDN," *Webology*, vol. 18, pp. 312–330, 2021.

[10] T. Sharma, S. Verma and K. Verma, "Intelligentheart disease prediction system using machine learning: A review," *International Journal of Recent Research Aspects (IJRRA)*, vol. 4, no. 2, pp. 94–97, 2017.
[11] G. Ghosh, K. Verma, M. Sood and S. Verma, "Internet of Things based video surveillance systems for security applications," *Journal of Computational and Theoretical Nanoscience*, vol. 17, no. 6, pp. 2582–2588, 2020.
[12] S. Midha and K. Triptahi, "Extended TLS security and defensive algorithm in openflow SDN," in *Proc. 9th Int. Conf. Cloud Comput. Data Sci. Eng. Conflu*, Amity Noida, India, pp. 141–146, 2019.
[13] G. Ghosh, K. Verma, D. Anand, S. Verma, D. B. Rawat *et al.,* "Secure surveillancesystems using partial-regeneration-based non-dominated optimization and 5D-chaotic map," *Symmetry*, vol. 13, no. 8, pp. 1435–1447, 2021.
[14] S. Midha and K. Tripathi, "Remotely triggered blackhole routing in SDN for handling DoS," in *Lecture Notes Networks Systems., International Conference on IoT Inclusive Life (ICIIL)*, NITTTR Chandigarh, India, vol. 116, pp. 3–10, 2020.
[15] S. Midha and K. Tripathi, "Extended security in heterogeneous distributed SDN Architecture," in *Advances in Communication and Computational Technology. Lecture Notes in Electrical Engineering*, G. Hura, A. Singh, L. SiongHoe(eds.), Vol. 668, Springer, scopus indexed, Singapore, pp. 991–1002, 2021, https://doi.org/10.1007/978-981-15-5341-7_75.
[16] P. Brey, Ethical aspects of information security and privacy. *Security, Privacy, and Trust in Modern Data Management*. M. Petković and W. Jonker (Eds.), Springer Berlin Heidelberg, pp. 21–36, 2007.
[17] D. Sinanc and S. Sagiroglu, "A review on cloud security," in *ACM SIN 2013-Proc. 6th Int. Conf. on Secure Information Networks*, pp. 321–325, 2013, https://doi.org/10.1145/2523514.2527013.
[18] E. AbuKhousa, N. Mohamed and J. Al-Jaroodi, "e-Health cloud: Opportunities and challenges," *Future Internet*, vol. 4, no. 3, pp. 621–645, 2012. https://doi.org/10.3390/fi4030621.
[19] C. Networks, "V350-centec open SDN platform," 2013. [Online]. Available: http://www.valleytalk.org/wp-content/uploads/2013/04/Centec-Open-SDN-Platform.pdf.
[20] S. P. Ahuja, S. Mani and J. Zambrano, "A survey of the state of cloud computing in healthcare," *Network Communication Technololgy*, vol. 1, no. 2, pp. 48–54, 2012. https://doi.org/10.5539/nct.v1n2p12.
[21] Y. Tseng, M. Pattaranantakul, R. He, Z. Zhang and F. Nait-Abdesselam, "Controller DAC: Securing SDN controller with dynamic access control," in *IEEE International Conference on Communication*, Paris, France, pp. 203–211, 2017. https://doi.org/10.1109/icc.2017.7997249.
[22] S. Narayana, J. Rexford and D. Walker, "Compiling path queries in SDN," in *Proc. third Work. Hot Top. Softw. Defin. Netw.-HotSDN'14*, Santa Clara, USA, pp. 181–186, 2014, http://dl.acm.org/citation.cfm?doid=2620728.2620736.
[23] P. Rani, Kavita, S. Verma and G. N. Nguyen, "Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network," *IEEE Access*, vol. 8, pp. 121755–121764, 2020. https://doi.org/10.1109/ACCESS.2020.3004692.
[24] S. Shin, V. Yegneswaran, P. A. Porras and G. Gu, "AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks," in *Proc. of the 2013 ACM SIGSAC Conf. on Computer & Communications Security*, Berlin Germany, pp. 173–185, 2013.
[25] L. V. Zhihan, L. Qiao and S. Verma, "AI-enabled IoT-edge data analytics for connected living," *ACM Transactions on Internet Technology*, vol. 4, pp. 1–20, 2021.
[26] S. Hosseini-Khayat, "A lightweight security protocol for ultra-low power ASIC implementation for wireless implantable medical devices," in *5th Int. Symp. Medical Information Communication Technology ISMICT 2011*, pp. 6–9, 2011.
[27] R. Yan, T. Xu and M. Potkonjak, "Semantic attacks on wireless medical devices," *Proceedings IEEE Sensors*, vol. 2014-Decem, no. December, pp. 482–485, 2014.

[28] I. Nikolaevskiy, D. Korzun and A. Gurtov, "Security for medical sensor networks in mobile health systems," in *Proc IEEE Int. Symp. a World Wireless, Mob. Multimed. Networks, WoWMoM*, Sydney, NSW, Australia, vol. 2014, pp. 283–290, 2014.

[29] N. Nagalakshmi, G. L. Anand Babu, K. S. Reddy and T. Ashalatha, "Security challenges associated with big data in health care system," *International Journal of Engineers and Advance Technology*, vol. 9, no. 1, pp. 4057–4060, 2019.

[30] J. Voris, J. Jermyn, A. Keromytis and S. Stolfo, "Bait and snitch: Defending computer systems with decoys, Cite Seer," 1–25, 2013. [Online]. Available: http://academiccommons.columbia.edu/catalog/ac:163019.