Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 6, July 2021: 6569-6586

Research Article

A Mutual lightweight Authentication Scheme for Fog-Cloud-Based E-Health Services

Bakhe Nleya

Abstract

The new version Internet network, now referred to as the Internet of Things (IoT) facilitates interconnectivity among various objects and devices. The introduction of both Cloud and Fog computing paradigms, device device-to-device (D2D) communication standards, as well as enabling privacy and security approaches, have all contributed to the practical realization of E-health services in IoT-enabled networks. Gen-erally, Fog layer nodes are often located in public places, where they are easily accessible and thus vulnerable to various securi-ty threats. Should this occur, the current and previously gener-ated security keys, as well as device identities, must be kept secret thus ensuring anonymity, unlinkability, forward secrecy, e.t.c. Thus in this paper, we introduce an E-Health authenti-cation and security architecture for the D2D-Aided fog compu-ting model, that facilitates verification of key components such as patients and peripheral devices without involving a central-ized cloud server. This is followed by a proposal for a light-weight anonymous authentication protocol (LAAP) to carry out authentication of the various parties in an E-health system. The proposed protocol is evaluated for various scenarios in D2D-Aided fog computing. Lightweight crypto- graphic primi-tives such as exclusive-or operations and one-way hash func-tion are relied upon to facilitate the inclusion of resource-constrained end-user devices mostly incorporated in body area networks (BANs). Ultimately we carry out an evaluation of the proposed proposal in terms of its efficacy, and security. The proposed protocol is generally found to be practically feasible for implementation in E-health service infrastructures.

Keywords: *E-health, mutual authentication, D2D communication, privacy, security*

[1] Department of Electronics Engineering, Durban, South Africa
bmnleya@gmail.com

Introduction

The IoT network blends several technologies to facilitate connectivity among billions of objects and devices. [1]. The health sector globally is taking advantage of the emergency of the IoT network to roll out Tele-care services that would effectively expand the s existing structures. Such a service will incorporate medical-related informational and multimedia coordination, as well as records processing. The resulting voluminous data exchanges in a Tele-care service, including associated monitoring systems, means that its privacy, as well as security, must be maintained, i.e hackers must be prevented from infiltrating the service. The IoT network is relied upon by this service to enable remote consultations as well as monitoring of patients. Typically monitoring devices (including sensors) will cluster around the body to form a body area network (BAN). Common to both such devices and sensors is that they are constrained in both computational capabilities as well as battery lifetimes. However, in emergencies, medical specialists can monitor the patients without having to be in proximity.

Typical health ailments that may require real-time monitoring, as well as detection, include cardiovascular-related ailments which often lead to heart seizures and consequently failures.

Needless to emphasize that this new development in the health sector is of tremendous benefit to those residing in the countryside. Such a development is now affording them advanced healthcare services despite the unavailability of both enabling technological facilities and specialists in such areas. To try to remedy the situation, in such instances, it might be important to improvise by facilitating constant monitoring of the patient’s health. This could also include monitoring his/her location as well as ensuring that the prescribed medication is administered as per the prescription stipulations. If such a monitoring system is not adequately secured, there is a risk of attacks that could easily compromise the patient’s identity, as well his/her medical records, this leading to the improper taking of the prescribed medications in terms of time intervals and dosages. Worst case scenario is that the patient may ultimately die A typical example would be that of a diabetic patient who has to take a remedial drug at a particular dosage. If an attacker alters both the medication intervals. and dosage, then this could lead to the patient deteriorating in health and consequently dying. In the advent of the current Covid-19 pandemic, it is of vital importance to monitor such patients in case their lungs completely clog, thus leading to respiratory failure and untimely death. By remotely monitoring such patients (i.e while in isolation), we are also preventing the further spread of the virus. In practice, an E-health service health monitoring system can be in the form of several body sensors constituting a wireless body area network (WBAN) that would monitor key environmental changes within the patient’s vicinity as well as body temperature, pulse rate, and heartbeat intervals. Thus, such systems should be implemented in rural areas to provide instant aid in case of an emergency. Besides, the IoT arena has also facilitated a relatively easy rollout of general health care in which any individual’s general condition can be monitored in real-time by putting on wearable devices. Nevertheless, the data that is generated must be handled with confidentiality, integrity, and authenticity in both the network and storage facilities. As such availability, confidentiality, as well as integrity, are necessary primary requirements of data security in Telecare Health. The confidentiality component of data security ensures that only authorized personnel can access an associated telecare health entity such as a database. The integrity aspect guarantees that only an authorized user can carry out necessary modifications of the already stored data with prior permission from the patient. Necessitated access can be granted as per need without interruptions or limitations, hence the need for the availability of the data.

Fog-Cloud Based Telecare Health Framework

To satisfy, necessary privacy, as well as security in the form of availability, confidentiality as well as integrity in Telecare Health services and an enabling network, such as IoT, is required [3]. The network infrastructure will facilitate secure authentication and key exchange by key entities constituting the infrastructure of an E-health service. In this paper, it is assumed that the network supports D2D communication. Note that D2D communication is designed to support direct communication among proximity devices and objects. Typically the envisaged all standard 5G IoT /GSM cellular networks are expected to incorporate this feature. By design ensures fail-safe communications by way of facilitating interoperability between critical public safety networks, public network infrastructures, and LTE (ubiquitous) networks. Its support for g proximity-based communications leads to an improvement in spectrum efficiency as well as utilization, end-to-end throughput, and energy efficiency.

Concurrently new and innovative services and applications can be rolled out. Notably, D2D-communication compatible telecare health devices and objects are potentially a fail-safe backup infrastructure for critical mission networks should the public cellular networks become inaccessible. [4]. Thus in a typical E-health infrastructural service, usage of D2D communication compliant devices is necessary.

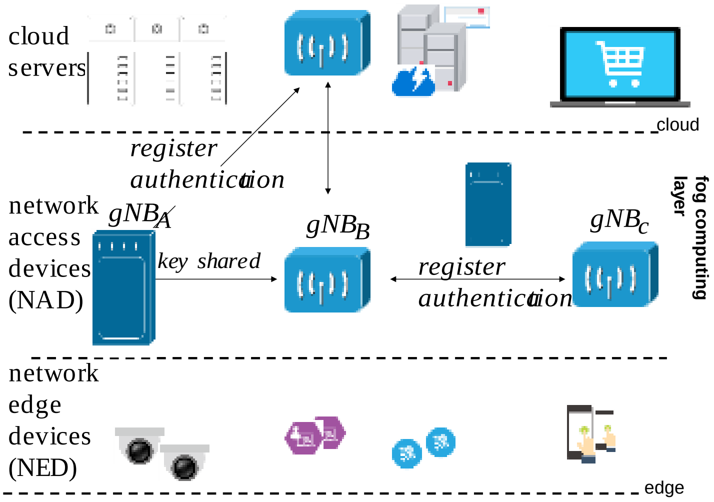

Fig. 1. ***Fog -Computing paradigm.***

At a local level, a 3rd Generation partnership project (3G-PP) IoT-enabled network architecture as well coverage is necessary [5]. Such a network incorporates key blocks such as a D2D communication server, a home subscriber server (HSS), and a mobility management entity (MME). The D2D communication server handles communications among proximity devices. The HSS retains attributes information of the devices as well as granting a set of necessary authenticating tokens.

However, the base infrastructure just discussed cannot guarantee a high level of QoS and this is because of the limited computing (processing) capabilities of the devices themselves. The cloud computing paradigm is also being explored as an alternative [6]. This is because it can render a better QoS to users with elastic resources despite its limitations. The key limitation is that of long round trip times. Besides, it cannot cope up with the low latency requirements of most health directly related services and applications. Hence of recent the Fog Computing paradigm was introduced to directly respond to the latency minimization issue.

It exploits the fog layer, which is the interfacing layer between the core and peripheral network sections to drastically reduce latencies as well as boost the limited computing powers in resource-constrained devices. It can also provide network context information which ultimately is used by fog applications and services to optimize context awareness. Its support for location-awareness; means it can fully support device mobility which is a direct booster for location-based services and applications. Fog computing easily provides a local overview whereas a global overview will still be provided by cloud computing. Primarily a fog computing model comprises key elements such as (i) network edge device (NED), (ii) network access device (NAD), i.e., fog node, in the proximity of a NAD, and (iii) cloud server (CS). This is illustrated in Fig. 1.

The NEDs will mostly be populated by various deice-constrained devices such as micro-powered smart devices and sensors acquiring data from a specified locality. The NAD has relatively enhanced with more computation capabilities, and given that it has a more reliable power supply, it can thus be bestowed with authentication functionalities as it will always be available.

As is known though Fog- Cloud computing paradigms affords various features such as improved computing efficiency as well as better bandwidth provisioning, However, it also has various privacy as well as security concerns. Concerning privacy, authentication requests increase as there is always a likelihood of handover chances among fog nodes increasing at NEDs. Whereas most of the authentication has been relegated to fog nodes, however, the performance bottleneck attributed to authentication cannot be avoided due to the number of requests incrementing. It is therefore imperative that new security infrastructural architectures be explored to address these issues. Furthermore, since fog nodes acquire and process lots of sensitive data, it is necessary to always preserve the privacy and security of the processed data. The mobility of NEDs , implies interaction with several different fog nodes, thus contributing to more privacy and security issues as well. Thus whereas the Fog layer significantly reduces the centralized cloud server processing loads, it is however necessary to maintain the footprint of data privacy from them. In that way, privacy protection will be ensured.

Thus in this paper, we introduce an E-Health authentication and security architecture for the D2D-Aided fog computing model, that facilitates verification of key components such as patients and peripheral devices without involving a centralized cloud server. This is followed by a proposal for a lightweight anonymous authentication protocol (LAAP) to carry out authentication of the various parties in an E-health system. The proposed protocol is evaluated for various scenarios in D2D-Aided fog computing. Lightweight crypto- graphic primitives such as exclusive-or operations and one-way hash function are relied upon to facilitate the inclusion of resource-constrained end-user devices mostly incorporated in body area networks (BANs). Ultimately we carry out an evaluation of the proposed proposal in terms of its efficacy, and security. The proposed protocol is generally found to be practically feasible for implementation in E-health service infrastructures.

E-Health Generalized Security Framework

We commence this section by describing the proposed Fog-Cloud security architecture which assumes D2D aided computing paradigm. The generalized architecture is illustrated in Fig. 2. We later discuss the general security requirements for an E-Health service system.

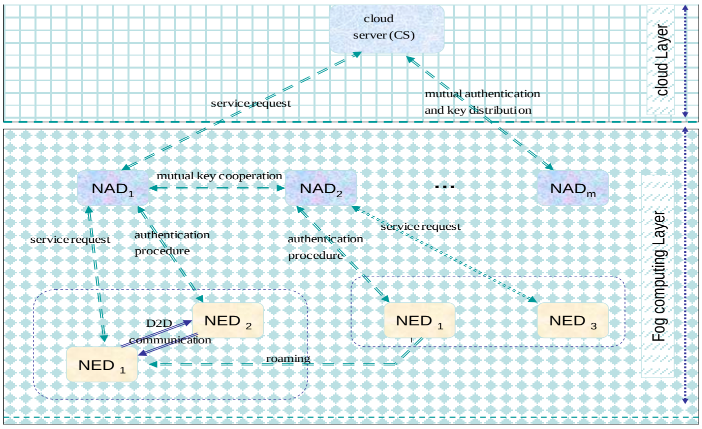

Fig. 2. .E-health system infrastructural framework

As earlier cited, traditional, Fog computing-based systems a NAD and NED can only authenticate each other via the cloud server (CS) and in the process, the performance is significantly impaired in terms of end to end latencies experienced, required extra bandwidth, as well as more security vulnerabilities(as an extra entity is involved). However, it is generally noted that many service/ application scenarios such as handover in LTE/5G wireless networks require the support of low latency, and for that D2D communication, the paradigm would be appropriate. Note that D2D communication facilitates as well as supports direct communication between devices in proximity. It is a feature incorporated in 5G/LTE IoT and GSM cellular networks. It ensures interoperability between public network infrastructures, critical public safety networks, and other ubiquitous networks such as the current LTE. Its goal in supporting proximity-based communications is to improve spectrum utilization, spectrum efficiency, end-to-end throughput, and energy efficiency, and at the same time facilitating novel applications and services. D2D-communication compatible devices and objects are potentially a fail-safe backup infrastructure for critical mission networks should the public cellular networks are suddenly malfunction or shut down totally.

The ever-growing population of NEDs, risks the NADS being overwhelmed with computational loads. Thus it may be necessary for peer NADs to cooperate and share such loads when necessary. Similarly for roaming NEDs, peer NADs can still cooperate in authenticating the roaming NED without the involvement of the CS. Thus a Fog computing model with cooperative D2D communications will be ideal in facilitating NEDs to interact as well as to authenticate without involving the distant CS. In that way, heavy computing loads at both the NADs and CS are avoided.

As illustrated in Fig 2. it is possible to support various authentication scenarios: For example, by default, a given NED within the domain of a given NAD will normally authenticate via a CS. Once authenticated, it can subsequently authenticate any other NED within that domain. If the already authenticated NED is mobile and is now entering a new NAD domain, then the last visited NAD will cooperate with the new NAD to authenticate the roaming NED.

With regards, to E-health key entities include a patient (with one or more senor NEDs embedded around the body), medical specialist (with his/her mobile GSM handset), hospital, medical database. The communicating devices are likely to be resources constrained in terms of processing power, memory as well as battery life. As such the IoT network is expected to provide connectivity with support for mobility, sparse location of entities location awareness, and low delays (latencies) latency. We thus in this paper advocated for the Fog-cloud computing paradigm which will also ensure support for privacy and security.

Overall, facilitators of IoT Fog -cloud-based E-Health service systems ought to be fully cognizant of the inherent threats as well as vulnerabilities. Security and privacy must be addressed proactively and all vulnerabilities and threat vectors must be considered. Summary security requirements include:

- Confidentiality: ensures that communications between, key entities such as patients, medical specialists, hospitals, and medical database(s) are secured against any unauthorized or malicious misuse. Confidentiality must also be ensured for the entire system, i.e, communications between various IoT devices, NEDs , NADs, and CSs.
- Data security (integrity): The E-health service-related data exchanged among various entities (parties) must be protected against any intentional manipulation. It might be necessary to invoke an integrity check at various points in the network.
- Availability: Full accessibility, as well as the availability of key data, must be ensured. In other words, systems must be put in place to prevent malicious acts intended to deliberately disrupt or harmfully affect communication or the quality of service provided by the IoT-cloud-based system’s communication network

- Access Control: Enforcing restrictive access to protected data by way of possibly evaluating, deciding, and enforcing access.
- Anonymization: use of anonymous authentication protocols to preserve privacy and security.
- Authentication: verifying and validating user credentials.
- Resistance Attraction: avoiding or preventing attacks from unauthorized users.

Proposed Lightweight Authentication Scheme

In this section, we assume a D2D Fog computing-based paradigm-based model as discussed in the previous section s. In proposing the scheme, our ultimate design goals is in both its resilience, robustness, communication efficiency, computational simplicity, as well as energy efficiencies. In short, the ultimate goal is that any authorized (authenticated) entity/party within the scheme's domain of operation ought to be able to resist any attacks.

It should be noted that lightweight encryption is opted for in this scheme as most e-health associated do not incorporate enough processing resources hence generally regarded as resource-constrained. The Fog computing infrastructure as outlined in the previous sections will also assist in reducing the end-to-end latencies i.e between the patient and medical specialist, or the latter and the medical database usually located in the CS [6].

Imperatively, identity anonymity and security should be guaranteed by way of robust mutual authentication as well as secured session key exchanges. Because we have incorporated the Fog computing layer, the mutual authentication 's resilience is enhanced by the existence of two pathways for its execution, the existing 3GPP authentication and the fog layer assisted infrastructure.

Pseudonym identities will be used by most of the key service entities and participants.

A: Initial Service Registration

In this section, we summarily provide the proposed scheme's basics. An individual, who suddenly feels unwell, will normally be attended to at the nearest hospital or clinic where initial registration formalities are carried out and thereafter he/she becomes a patient. Each patient/ or patient's device (NED) or both can now use the temporary credentials provided at the health center to register with the cloud server (CS) via a secured link. The following procedural steps are adhered to, e.g. a patient's devices (regarded as forming a group or a BAN) will register as follows:

Each device in the group/ BAN), NED_i formalizes a request to be registered with the CS.

CS initiates an n bit counter $gcount$ which will be automatically incremented for each formal request received.

Once again, the CS increments $gcount$, i.e. $[gcount]+1$, computing a transaction sequence number:

$$T_{seq} = \{gcount\}+1 \tag{1}$$

a secret key K_{ec}, and a pseudo ID :

$$PID = \{pid_1 , pid_{2,....pid_n}\} \tag{2}$$

that are assumed unlinkable.

The CS dispatches the parameters generated in the previous steps together with a group key GK to the NED_i.

B: Authentication with Fog layer

This takes place when for the first time a patient's device (BAN member), NED_i wishes to exchange data (mages captured) to the CS. . The procedural steps can be summarised as follows:

The NED_i contacts the nearest NAD and furnishes it with:

$$NED_i \rightarrow NAD : M_{A_1} : \{AID, N_x, T_{seq}\} \tag{3}$$

The information is generated as follows:

$N_x = N_e \oplus K_{ec}$ is computed by NED_i, where, where N_e is a randomly generated number. Similarly, the NED_i generates :

$$AID = h(ID_{NED_i} \| K_{ec} \| T_{seq}) \tag{4}$$

where, and ID_{NED_i} is the patient device's ID. K_{ec} is computed from any one of the unused pid s i.e $K_{ec} = AID = pid_j, k_{em_j}$ (5)

Because at this stage the two parties are unknown to each other, this information (request message) will be rerouted to the CS.

$$NAD \rightarrow CS : M_{A_2} : \{Fwd, M_{A_1}\} \tag{6}$$

Upon receiving the message M_{A_2} from the NAD, it verifies it. As follows:

Firstly it locates the T_{seq} from the local database (DB) and at the same time retrieves ID_{NED_i} as well as K_{ec} from the same local DB to for use in the verification process. If verification succeeds, the CS generates a communication key CK and a new transaction sequence number $T_{seq_{new}}$. Consequently, the NED_i further computes:

$$e1 = h(K_{ec} \| T_{seq}) \oplus T_{seq_{new}} \tag{7}$$

$$e2 = h(K_{ec} \| ID_{ED_i}) \oplus CK \quad \mathrm{Re}\,s_{CS} = h(e1 \| e2 \| K_{ec}) \tag{8}$$

and consequently updates;

$$T_{seq} = T_{seq_{new}} \tag{9}$$

The CS then confirms the NAD verification in the form of a response message M_{A_3}.

Upon receiving the confirmation message M_{A_3}, the NAD inturn generates a tracking number, $Track\ \mathrm{No.}$ as well as a random number R_n for computing;

$$TN = h(CK \| R_n) \oplus Track\ No. \tag{10}$$

and

$$\mathrm{Re}\,s_{NAD} = h(Track\ No. \| CK \| R_n) \tag{11}$$

It then sends a confirmation message M_{A_4} to the patient's device NED_i. Once NED_i, receives the message M_{A_4}, it verifies its validity by inspecting the response parameters $\mathrm{Re}\,s_{CS}$ (from CS) and $\mathrm{Re}\,s_{NAD}$ (from the NAD) before decoding $T_{seq_{new}}$, and CK. Finally it updates. T_{seq} to $T_{seq_{new}}$.

Because in D2D fog-assisted computing, neighboring devices (i.e. in a group) can assist one another by secluding any outsider (hackers). In this case, they will share a channel (link) key K_{ij}. In that way, the authentication process can be summarised as follows:

When it becomes necessary for another BAN device NED_j to liaise with a NAD, then the NAD can authenticate it with the help of the most recently authenticated device in this case NED_i. For that, NED_j furnishes its identity in the form of an alias:

$$AID = h(ID_{NED_j}, \| \ GK \| \ T_{seq}) \tag{12}$$

as well as generating a common group authentication request;

$$G_{auth} = h(ID_{NED_j} \| \ R_n \| \ GK \| K_{ij}) \tag{13}$$

Once NED_i receives such a request message M_{B_1} from it will carry out the necessary verifications before sending a confirmation message M_{B_2} to the NAD.

Upon receiving the confirmation message M_{B_2} from NED_i the NAD validates all key parameters including the Track number($TrackNo.$), and also decode tk. After successful validation of all key parameters, it will send a response message M_{B_4} to NED_i.

Upon receiving M_{B_4} from the NAD, it checks the validity of $\mathrm{Re}\,s_{NAD}$ as well as encoding the tk key. The latter is done using both the link key (K_{ij}) and the group key (KC)

$$tk^{\#} = h(GK \| \ ID_{ED_j} \| \ K_{ij}) \oplus tk \tag{14}$$

Ultimately it sends a confirmation message M_{B_4} to NED_j.

After receiving M_{B_4}, ED_j validates it before broadcasting a random number Rn to all group members.

When a surveillance camera is moved to a new NAD, then the last visited NAD will assist the new one in verifying it.

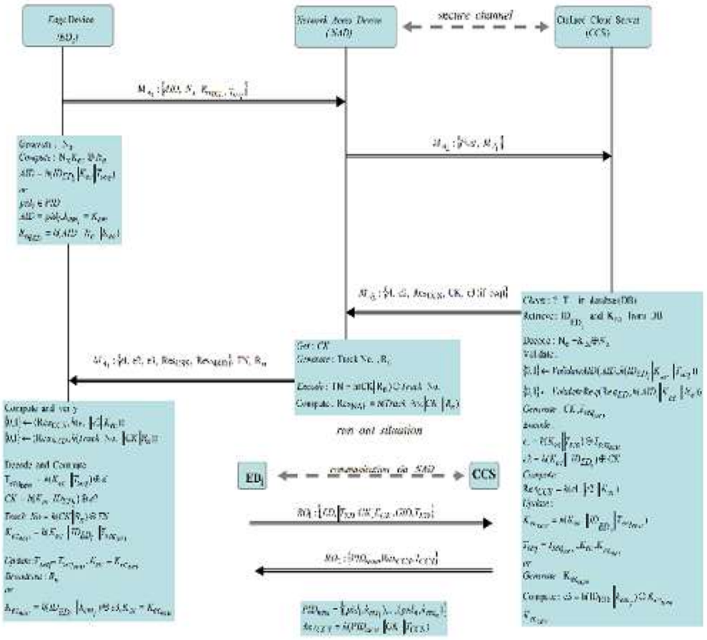

Fig. 3. Summary: Authentication for D2D-Aided Fog Computing

Figure 3 above summarises the overall authentication steps of the proposed scheme.

analysis

In this section, we carry out both the performance as well as security analysis of the proposed scheme.

The setup in Figure 4, is used in the performance evaluation of the scheme.

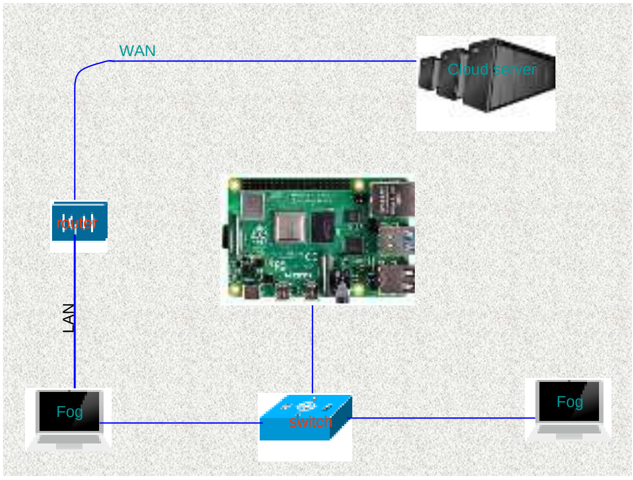

Fig. 4. Experimental setup

The setup comprises a quad-core processor (Raspberry Pi 4, 8GB RAM, Gigabit Ethernet, USB3.0, wireless LAN, Bluetooth 5.0, and USB-C power and platform. The overall network environment as shown in Fig 3 is controlled. For Fog computing, we have two units, both located close to the switch and the quad processor. The three are located on the same LAN segment. The cloud server has the same specifications as our processor and is located at a collaborating university (National University of Science and Technology, Bulawayo) which is approximately 2 000 km away.

Table 1. Computational Overheads for various Operations

operation	*turnover time (ms)*
pairing operation	7.01
hash operation	0.01
symetric key encryption	0.025
assymetric key encryption	1.4
mod. exp. operation	0.8
chinese reminder theorem	6.88

A: Security Analysis

We hereby in this section summarily carry out the proposed scheme's security capabilities based on the requirements that we have already outlined in previous sections. These include security requirements such as privacy, confidentiality as well as immunity against eavesdropping.

- To ensure reliable mutual authentication by the various entities and parties constituting the E-health service system relies on parameters such as T_{seq} and AID . Should any of the parameters be deemed invalid, the authentication process is aborted. From the CS 's side. Note that the NED will always rely on parameters such as MA_4 and $\mathrm{Re}\,s_{CS}$ to mutually authenticate with the NAD and CS . From equations (8), (9), and (10) it is clear that the value parameter AID is a long-term secret exclusively known to the CS and NED_i . Because T_{seq} is also known to both CS and NED_i at the same time, refreshed for every session. Effectively this prevents any possible eavesdropping and replay attacks. then replay attacks.
- To ensure secured key exchanges among the various key entities (parties), the communication key is centrally generated, i. e in this case by the CS before being distributed in encoded form to NED_i and NAD . Equation (8) is an expression of the encoded format. Both NED_i and NAD will then utilize this same key to enhance as well as ensure complete privacy and integrity.
- By using a one-time- alias feature (using AID), we seclude the possibility Eavesdropping related attacks as there is no direct relationship between the aliases. To further enhance security in this regard, it is also noted that often the security parameters exchanged between parties are one-time.
- For a group of devices constituting BAN it is only necessary for the first device NED_i to be fully mutually authenticated by a NAD . Then afterward the rest of the member devices in BAN authenticate by being assisted by the most recently communicated NED_i member.

B. Performance Evaluation

We briefly explore this scheme's relative performance and efficiency. Notably, for efficiency, we focus on relative implementation costs of lightweight AEAD ciphers, as well as energy consumption. The scheme is expected to provide adequate security and privacy and hence this necessitates consideration of its efficacy in terms of prime security primitives that we discussed previously, i.e. they include but are not limited to authentication, data confidentiality/integrity, anonymity e.tc. In detail, the applied cryptographic algorithms are the digital signature, the Diffie–Hellman key exchange algorithm, and the AEAD cipher. A few additional key parameters that we define to assist in the analysis include:

- t_{DS} - time required to process digital signature.
- t_{DS} -verification time for a single digital signature.
- t_{DH} - time lapse is required to process a key exchange.
- t_{AEAD} - the processing time for the AEAD cipher.
- l_{tr} - average transmission latency in D2D communication.

Thus the processing time of a D2D communication processing time is [53];

$$t_{D2D} = \sum l_{tr} + \sum t_{DS_{sign}} + \sum t_{DS_{ver}} + \sum t_{DH} + \sum t_{AEAD} \qquad (15)$$

We will make a comparison of the proposed scheme's performance with equivalent schemes that are based on the following encryption algorithms:

1. AES Galois/Counter Mode (AES—GCM) algorithm [7]. This is based on a block encryption mode of operation that affords high speed of authenticated encryption and data integrity. It achieves both encryption and decryption using either a 128-bit, 192-bit, or 256- bit cipher key. CM mode provides both privacy (encryption) and integrity
2. ASCON:[8] This is an AEAD version cipher algorithm based on duplex sponge modes. It uses a 128-bit key, a 128-bit IV, and produces a 128-bit authentication tag. The internal state is 320-bit long and is represented by five 64-bit registers, noted x_0 to x_4. Finally, the secret key is XORed to the 128 last bits of the state.
3. SpoC (Sponge with masked Capacity). [9] This is a permutation-based mode of operation for authenticated encryption with associated data (henceforth "AHEAD") functionality. The high-level design is inspired by the Beetle mode of operation. It offers a higher security guarantee with smaller states as compared to some of the previous AEAD designs based on the Sponge paradigm.
4. Spook (Sponge-Based Leakage-Resistant Authenticated Encryption): [10] This is an algorithm for authenticated encryption It is primarily designed to support low energy

implementation, especially when protection against side-channel attacks is required. Spook is generally regarded as an efficient single-pass algorithm.

5. GIFT-COFB [6], [10] This primarily a block cipher-based AEAD design that uses GIFT-128 as the underlying block cipher.. Both encryption and decryption algorithms do not require any decryption call to the underlying block cipher. This significantly reduces the overall hardware footprint in combined encryption-decryption implementations.

The computational cost performance of the proposed scheme is carried out using the setup of Figure 4. It is weighed of the various computational cost entities as expressed by equation (15). In so doing we make a comparison with similar schemes. The results are graphed in Figure 5.

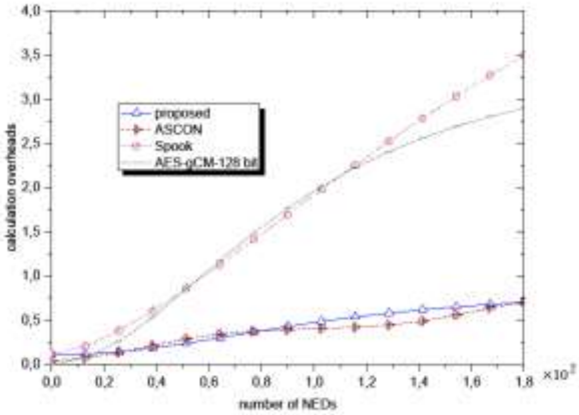

Figure 5. Computational costs of the 4 schemes

In the comparison, we vary the number of devices (NEDs) to a maximum of 180. The data is aggregated per single or several BANs

As can be observed in the same figure, the overhead generated by the proposed scheme is relatively low throughout.

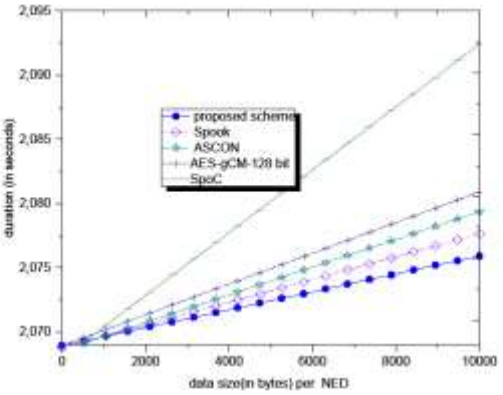

Figure 6. Communication overheads generated per session

This also compares with that of the ASCON algorithm-based security scheme. Partly, this is because both schemes rely on lightweight key agreement identity authentication, whereas the Spook and AES rely on bilinear pairing authentication, which is characterized by relatively intensive calculations.

Figure 6 plots the duration of the D2D communication complete session when transmitting data messages per group (BAN). Relatively the proposed scheme achieves all required communications within a relatively short time in comparison with the rest of the schemes.

Figure7 plots the energy consumption comparisons from where we can deduce energy efficiencies. In the plot, the proposed and ASCON-based security schemes expend relatively lower energy in comparison with the rest of the schemes. Taking into consideration that the proposed scheme displays relatively superior performance when compared to the rest, it is, therefore, better suited for implementation in E-health systems since most of the associated devices are power constrained.

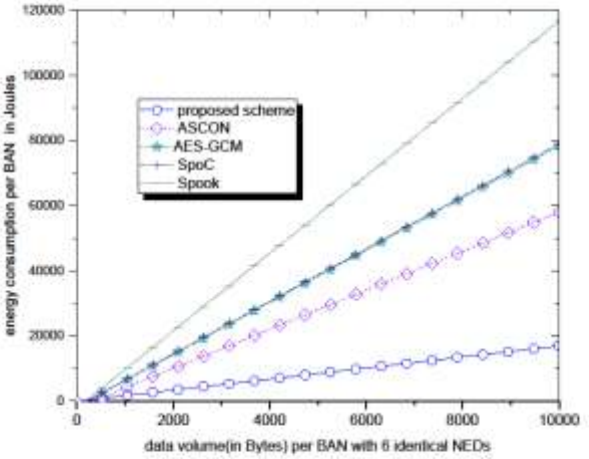

Figure 7. Energy consumption

Conclusion

This paper proposes a D2D communication-based Lightweight authentication and key agreement scheme that ensures both privacy and security for patients who have enrolled for such a service. The fact that the authentication can be done via an insecure link means that even in the absence of 3GPP network coverage, patients would still be able to link with the nearest health care center and medical specialists, thus making the scheme both resilient and robust. This is because D2D communication supports direct device linking of proximity devices and thus an affected device would still reach the nearest peer that is within sufficient coverage range.

The paper uses lightweight message authentication that is meant to reduce computational and communication loads, as well as operating in an energy-efficient manner. Its efficacy in terms of ensuring both security and privacy was explored. Overall, we conclude that the scheme would be quite viable in the practical implementation of E-health services as most of the devices are resource-constrained in terms of computational as well as operating power requirements.

In the foreseeable future, the same work will be extended to further optimize network and power resources, by way of further minimizing computational overheads [11], [12]. Reducing the latencies experienced by NEDs during authentications/ authorizations will also be explored.

References

M. Pasha and S.Shah, “Framework for e-health systems in IoT-based environments” Wireless Communications and Mobile Computing Volume 2018.

P. Świątek and A. Rucinski, "IoT as a service system for eHealth," 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013), 2013, pp. 81-84, doi: 10.1109/HealthCom.2013.6720643.

K. Monteiro, É. Rocha, É. Silva, G. L. Santos, W. Santos and P. T. Endo, "Developing an e-Health System Based on IoT, Fog and Cloud Computing," 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), 2018, pp. 17-18, doi: 10.1109/UCC-Companion.2018.00024.

J. Lee and J. H. Lee, "Performance Analysis and Resource Allocation for Cooperative D2D Communication in Cellular Networks With Multiple D2D Pairs," in IEEE Communications Letters, vol. 23, no. 5, pp. 909-912, May 2019, doi: 10.1109/LCOMM.2019.2907252.

S. Fang, Y. Gao, C. Zhang and X. Hei, "Achieving 3GPP Fairness for LTE-U and WiFi Coexisting Networks in Unlicensed Spectrum," 2019 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), 2019, pp. 1-2, doi: 10.1109/ICCE-TW46550.2019.8991934.

P Gope “”,LAAP: Lightweight anonymous authentication protocol for D2D-Aided fog computing paradigm”,Computers & Security,Volume 86,2019,Pages 223-237,M, Wang, and Z., Yan, “Privacy-preserving authentication and key agreement protocols for D2D group communications”, IEEE Transactions on Industrial Informatics, vol.14, no.8, pp.3637-3647, 2018.

Gul, M.J., Rehman, A., Paul, A. et al. Blockchain Expansion to secure Assets with Fog Node on special Duty. Soft Comput 24, 15209–15221 (2020). https://doi.org/10.1007/s00500-020-04857-0

A. Alrawais, A. Alhothaily, C. Hu, X. Xing and X. Cheng, "An Attribute-Based Encryption Scheme to Secure Fog Communications," in *IEEE Access*, vol. 5, pp. 9131-9138, 2017, doi: 10.1109/ACCESS.2017.2705076.

J.P. Degabriele, C. J. Patrick, “Sponges Resist Leakage: The Case of Authenticated Encryption, Advances in Cryptology – ASIACRYPT 2019, 2019, Volume 11922

Farjana N., Roy S., Mahi M.J.N., Whaiduzzaman M. (2020) An Identity-Based Encryption Scheme for Data Security in Fog Computing. In: Uddin M., Bansal J. (eds) Proceedings of International Joint Conference on Computational Intelligence. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-13-7564-4_19.

L. P. Bopape, B. Nleya and P. Khumalo, "A Privacy and Security Preservation Framework for D2D Communication Based Smart Grid Ser-vices," 2020 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa, 2020, pp. 1-6, doi: 10.1109/ICTAS47918.2020.233995.

B. Nleya and C. Mulangu, "An Overview of GREEN Networking and Power Savings in Optical Backbone Networks," 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa, 2018, pp. 1-6, doi: 10.1109/ICABCD.2018.8465402.