A Comprehensive Assessment Framework for Evaluating Adaptive Security and Privacy Solutions for IoT e-Health Applications

Waqas Aman, Fatima Najla Mohammed
Department of Information Systems, College of Economics and Political Science
Sultan Qaboos University, Muscat, Sultanate of Oman

***Abstract*—There exist numerous adaptive security and privacy (S&P) solutions to manage potential threats at runtime. However, there is a lack of a comprehensive assessment framework that can holistically validate their effectiveness. Existing Adaptive S&P assessment efforts either focus on privacy or security in general, or are focused on specific adaptive S&P attributes, e.g. authentication, and, at certain times, disregards the architecture in which they should be comprehended. In this paper, we propose a holistic assessment framework for evaluating adaptive S&P solutions for IoT e-health. The framework utilizes a proposed classification of essential attributes necessary to be recognized, evaluated, and incorporated for the effectiveness of adaptive S&P solutions for the most common IoT architectures, fog-based and cloud/server-based architectures. As opposed to the existing related work, the classification comprehensively covers all the major classes of essential attributes, such as S&P objectives, contextual factors, adaptation action aptitude, and the system's self-* properties. Using this classification, the framework assists to evaluate the existence of a given attribute with respect to the adaptation process and in the context of the architectural layers. Therefore, it stresses the importance of where an essential attribute should be realized in the adaptation phases and in the architecture for an adaptive S&P solution to be effective. We have also presented a comparison of the proposed assessment framework with existing related frameworks and have shown that it exhibits substantial completeness over the existing works to assess the feasibility of a given adaptive S&P solution.**

Keywords*—*Internet of Things; Adaptive Security; IoT Architecture; e-Health; Effectiveness; Privacy

I. Introduction

IoT has become an integral part in the automation and extension of various IT-based services. In healthcare, IoT has shown huge potential. Spending on e-health solutions in IoT is expected to stretch 1.1 Trillion dollars by 2025 [1]. IoT in e-health is a developing research area as the world moves towards remote monitoring, real-time and rapid diagnosis and management of illnesses [2]. It is aiding in real-time identification of ailments, attaining more precise health readings, better reach-out to patients in emergencies, and medical care for patients while they are roaming or having mobility difficulties [2]. The range of functionalities provided by IoT in e-health applications has been significantly beneficial and high in demand, especially in the current COVID- 19 pandemic situation where hospitals are running at total capacity, requiring more efficient remote healthcare solutions.

Despite the multiple benefits offered by IoT-enabled e-health applications, there is an increasing concern about the potential security and privacy (S&P) threats as it primarily utilizes personal and sensitive information, which can be of considerable value for the attacker, for instance in blackmailing and identity frauds [3],[4]. By nature, IoT devices are dynamic because of the frequent environmental changes, mobility, and their heterogeneous and constantly evolving technology. Such properties can result in a more evolved threat spectrum requiring real-time threats handling. To adapt to such circumstances, many studies have proposed adaptive S&P mechanisms. Adaptive S&P is a system's capability to maintain S&P in the presence of contextual changes [5]. It continuously maintains an optimal S&P level of a managed system through an automated monitor, analyze, and adapt feedback loop, unlike traditional S&P controls such as IDS, anti-malware, firewalls, etc., which have limited protection scope and enforce manual and inflexible threat mitigation strategies [5].

IoT e-health is a critical infrastructure consisting of devices, applications, and individuals that handle sensitive patients' data. Adaptive S&P mechanisms are highly essential, mainly to protect and manage actions, such as access, sharing, and disclosing of the information assets and provide effective S&P within the IoT e-health architecture [6, 7]. Hence, the system needs to be flexible, adaptable, and robust to make real-time S&P decisions based on the requirements of the entities associated with the system [6]. When designing and developing adaptive S&P solutions for IoT e-health, it is vital to consider a set of significant attributes; such as privacy and security objectives, contextual factors, self- properties, adaptation action aptitude and analysis, and adaptation mechanisms to develop a solution that is capable of providing holistic S&P in such dynamic contexts. Moreover, these attributes needs to be realized at particular levels with respect to the different phases in the process and to the underlying architectural needs. If a certain attribute or requirement is improperly enforced in the architectural layers, it may adversely affect the competency of the corresponding adaptation phase. Such misconfiguration may lead to, for instance, scope creep or scope crush of the managed devices, resulting in the adaptive system disorganization and ineptitude.

Regardless of the availability of multiple studies and solutions on adaptive S&P, for instance, [8, 9, 10] emphasize on the need to assess their effectiveness. To validate the efficacy, it is vital to recognize and evaluate the essential factors

necessary for an adaptive S&P solutions and the extent to which they are employed as per adaptation and architectural needs. The existing assessment frameworks focus on a particular set of factors irrespective of the underlying architecture [9,13,14,15] and have a limited scope that only address a part of the problem, [9,13,14,15]. Hence, there is a need of an evaluation framework that can holistically assess the feasibility of a given adaptive S&P mechanism for IoT e-health applications.

In this paper, we present the design of an assessment framework that can guide us to comprehensively assess the feasibility of a potential adaptive S&P solution. It, therefore, also provides a reference model to understand and consider the underlying vital aspects of S&P adaptation. The framework is based on a proposed classification of factors that we have compiled from the existing works. These factors were scattered across the literature under different concerns and with limited scope. We have unified them in a classification of five distinct classes: security objectives, contextual factors, adaptation aptitude, and self-* properties and privacy objectives required for effective S&P adaptation. The proposed framework mainly assesses which factors should be covered, where they should be realized in the adaptation process, i.e., monitoring, analysis, or adaptation, and at which layer of the common IoT e-health architectures, fog or cloud/server, should they be employed. Furthermore, we present a detailed comparison of the proposed framework with the potential equivalent works. We have concluded that our framework provides a more comprehensive platform for assessing a given adaptive S&P solution. The fundamental contribution that our framework dispenses is a set of diverse and inclusive factors required for S&P adaptation and evaluates them in the architecture context is particularly vivid.

II. The Assessment Framework

In this section, we provide a comprehensive description and illustration of the proposed classification and assessment framework. The classification mainly identifies and groups the key attributes (factors) necessary for a given adaptive S&P system. The assessment framework utilizes this classification by determining their need and purpose based on two key aspects: the overall adaptation process (Monitor, Analyze, and Adapt phases) and the IoT e-health architecture. These two aspects are necessary to be considered because certain attributes necessary for the S&P adaptation needs to be addressed uniquely in various architectures. For instance, for fog-based architectures it is vital to conduct S&P analysis at the gateway than at a centralized server to fulfil the rapid and personalized threat assessment objectives for which fog-based architectures are devised [11], [12]. Moreover, the scope managed by a given gateway in fog-architecture is limited as compared to one managed by a centralized server. This structured approach of the framework design assists in assessing the feasibility of an adaptive S&P solution in its respective architecture.

A. The Proposed Classification

The classification aims to identify and group the fundamental factors necessary for a given adaptive S&P solution. It employs conceptual modeling and provides a basis for comprehending the factors that need to be monitored or managed, essential to effectively achieve security and privacy objectives, and the ones that may trigger the need of adaptation or may be affected by the adaption processes. Hence, it provides a more comprehensive list of essential factors. The proposed classification, as illustrated in Fig. 1, is developed using the steps followed as:

- Key factors were identified in the current literature on adaptive S&P for IoT e-health.
- Factors that have similar semantic and objective(s) were unified into a common factor. For instance, events per second (eps), productivity, and throughput factors are transformed into a more common and distinct label, throughput.
- To be more comprehensive, certain generic factors are broken down into more detailed and vital factors. For example, QoS is further categorized into response time, latency, and throughput.
- The final list of factors was then grouped into distinct classes. Factors were mapped to the relevant classes based on their overall objectives. Table I provides a brief summary describing each class, listed in Fig. 1, in the context of adaptive S&P solution for IoT e-health

B. The Proposed Assessment Framework

The primary objective of the proposed assessment framework is to holistically assess the feasibility of an adaptive S&P solution for IoT e-health. It considers four essential concepts: The proposed classification, detailed earlier, the adaptation processes, the IoT e-health architecture in which an adaptive S&P is employed, and a Mapping Criteria. A brief description to the later three concepts in the framework are detailed as follows.

1) The adaptation process: The adaption process in an adaptive S&P system can be typically divided into three main functionalities or phases [8, 13, 16, 17]: Monitoring, Analysis, and Adaptation. They enable a system to adapt the S&P configurations based on the dynamic changes in the IoT e-health infrastructure in an automated manner. These phases are briefly described as follows:

a) Monitoring: The main goal is to observe, gather and transform contextual information. This includes information about the adaptive system itself (internal factors), such as information related to the software and hardware components responsible for the adaptation process. Monitoring also observe external factors such as those related to the monitored devices, users, network and applications. Therefore, it attempts to collect data essential for a context-aware analysis and adaptation [8, 16, 17].

b) Analysis: Analysis aims to determine potential threats, assess potential vulnerabilities, and analyze the protection level of security and privacy from the related contextual information gathered during the monitoring phase. Hence, the analysis process involves the intelligence by applying a range of methods needed to investigate, correlate, and analyze the context of the potential threats [8, 16, 17].

TABLE I. A SUMMARY OF THE CLASSIFICATION CLASSES

Factors	Summary
Security Objectives	Include the attributes responsible for ensuring the basic security of the IoT e-health resources covered by the adaptive system, from security threats, e.g., authenticating users based on their biometric information, authorizing users based on their role, e.g., medical staff accessing the staff portal, patients accessing the patient's portal.
Privacy Objectives	Refers to the factors that ensure essential privacy, including access, usage, and collection of the information assets in an IoT e-health environment, e.g., collecting, accessing, and using patient's health records such as x-rays and CT scans.
Contextual Factors	Contextual factors can potentially trigger the need for adaptive S&P. This can include internal factors such as architectural factors and external factors such as user preferences. Hence, in the context of adaptive S&P solution, assessing these attributes is essential mainly to ensure that the adaptive solution can consider contextual aspects to respond to the changing context and respond to S&P threats, thus providing holistic S&P.
*Self-*Properties*	Self- * Properties are the basis for the adaptive S&P system itself, as they are capabilities responsible for the adaptive nature of such solutions. These properties enable the adaptive solution to adjust its S&P settings in response to a context and adapt and manage the adaptive solution itself in response to S&P threats. For instance, introducing additional encryption mechanisms in response to a low battery event from one sensing device
Adaptation Action Aptitude	A set of factors that may have a negative impact due to the potential adaptation action. For instance, if a low battery occurrence is detected in a monitoring device, the adaptive solution should adjust the encryption mechanisms to ensure trade-offs amongst confidentiality and the availability of the services.

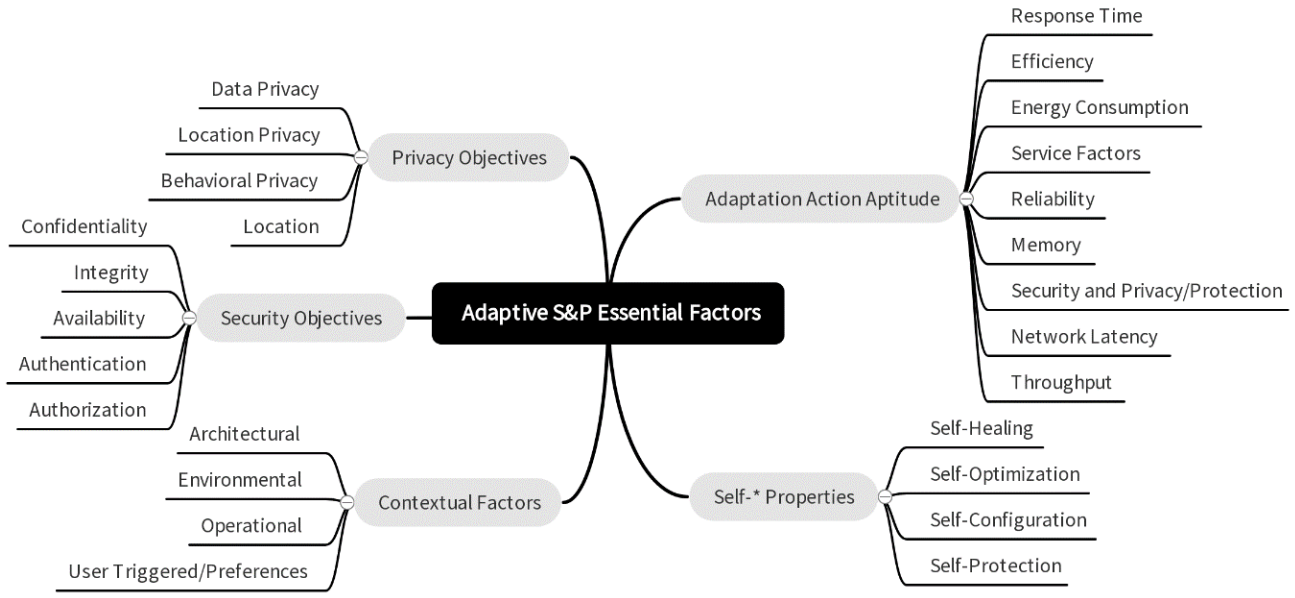

Fig. 1. The Proposed Classification.

c) Adaptation: In the adaptation phase, decisions are made to adapt to any given threat situation. The corresponding functionalities identifies a recommended adaptation configuration based on the threat faced and instructs the monitored asset(s) for its adoption. It is recommended that the system is capable of identifying several adaptation actions and select the optimal one [13]. The adaptation process is responsible for the adaptation decision making whereas the actual adaption action is implemented at the monitored object level [8].

2) IoT eHealth Architecture: The IoT e-Health architecture specifies the nature of data processing within the overall system [18], [19]. This study considers the two major IoT e-health system architectures, cloud/ server and fog-based system architecture, which are commonly used in the IoT e-Health settings.

a) Cloud/Server Architecture: In Cloud/Server architectures, illustrated in Fig. 2, data processing is performed in a centralized manner, typically using cloud computing or centralized servers controlled by the healthcare service provider [6], [20]. To enforce S&P adaptation in a cloud/server architecture, the monitoring is carried out within the gateway and health systems layer. This includes data collection, filtration, transformation, and further communication, etc., to the upper layers. Device Layer merely act as events generators. However, in certain instances, monitoring is performed at the device layer. For instance, GPS sensors and authentication interfaces can monitor and send out events to the gateway layer, which are further processed by the gateway. In contrast, the analysis and adaptation decision-making is performed at the health systems layer, comprising the cloud/centralized servers [13, 21].

b) Fog architecture: Fog architectures, shown in Fig. 3, use the computing resources at the gateway level to carry out the processing of the data gathered from the sensors [22]. The fog nodes, the gateways, perform data normalization, which

consist of storage, computing, and network connectivity, thus enabling them to analyze and make time-sensitive decisions on the time-sensitive data collected [23]. In the context of S&P adaptation, in fog architectures, threat monitoring, analysis, and adaptive decision-making are typically performed at the gateway layer [8, 24]. However, as established earlier, in certain instances, monitoring can also be performed in the device layer. In fog architectures, health-related data collected from the device layer is sent to the cloud. It is part of the primary storage and commuting resource, performing data analytics and visualization [23].

3) The mapping criteria: The mapping criteria, detailed in Table II, describes information on what and where different attributes should be realized within the different IoT system architectural layers and whether and what adaptation process should be applied on them to enforce effective S&P adaptation. Therefore, it maps a given attribute to the respective architectural layer and adaptation phase based on its requirement in an adaptive S&P solution. Table III – VII illustrate the proposed assessment framework, and shows how the different attributes in the proposed classification have been mapped based on the adaptation process and the IoT e-health architectural layers. For convenience, below we describe how the table structure should be interpreted to comprehend the architectural and process level requirements of a given attribute:

- The Class and Attributes columns corresponds to the classes and respective factors, as detailed in the proposed classification, which are essential for S&P adaptation.
- The Process column indicate whether or not a given attribute is required be monitored (M), Analyzed (A), or Adapted (Ad). Moreover, it also reflects whether the respective mechanism(s) of the attribute is Utilized (U). An absence of a label indicate that it is not required.
- The System Architecture column, further categorized into Fog and Cloud/Server architecture, indicates where, specifically, in the respective architectures should an attribute is required to be utilized, monitored, analyzed, adapted. For instance, GM depicts that a given attribute needs to be monitored at the Gateway Layer, HU indicates that the mechanism(s) related to the factor should be utilized at the Health System Layer, and GAd shows that the corresponding factor needs to be adapted at the Gateway Layer.

The assessment framework for individual class is illustrated and detailed underneath.

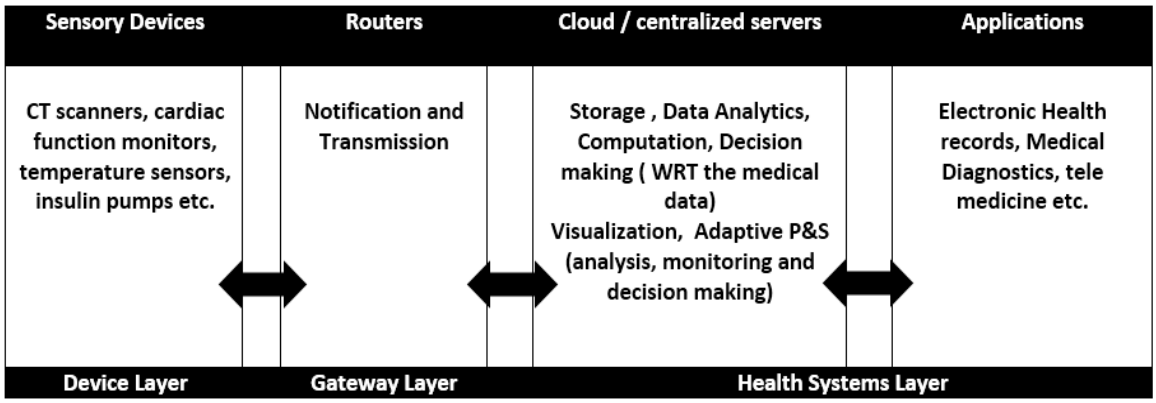

Fig. 2. Figure 2. IoT e-Health Cloud/Server Architecture.

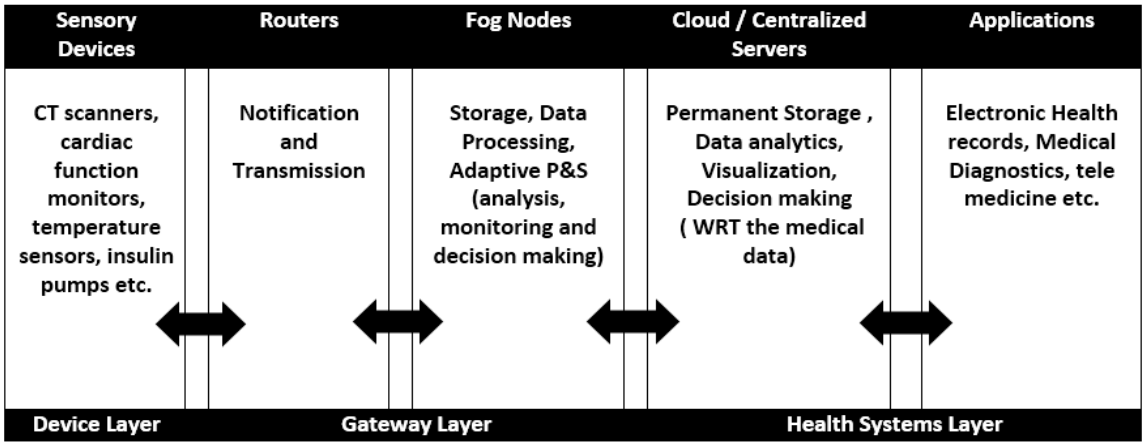

Fig. 3. IoT e-Health Fog Architecture.

TABLE II. THE ASSESSMENT FRAMEWORK'S MAPPING CRITERIA

Criteria #	Criteria for mapping an attribute with the adaptation process
1	**Utilized (U):** Reflects that the corresponding mechanism or attribute is utilized either as a mechanism to ensure S&P or as a factor/attribute to be evaluated for optimal adaptation decision in the adaptation phase.
2	**Monitoring (M):** Attributes are mapped to monitoring process when they are required to be *observed or monitored* for security and privacy threat/risk analysis or when they are utilized in the monitoring process.
3	**Analysis (A):** Attributes are mapped to the analysis process when they are *assessed* for the security and privacy threat/risk analysis or when are they utilized in the analysis process.
4	**Adaptation (Ad):** Attributes are mapped to the adaptation process when they are required to be adapted, evaluated during the adaptation decision, or utilized in the process.
	Criteria for mapping an attribute with the adaptation process IoT e-health architecture
	Attributes are mapped within the fog and cloud/server architecture, with regards to where in the architecture, **Device layer (D)**, **Gateway layer (G**) and **healthcare service provider controlled layer (H),** Cloud/Central servers, these attributes are required to be **(M), (A), (Ad)** and **(U)**.

TABLE III. CLASS – SECURITY OBJECTIVES

Class	Attributes	Process	System Architecture				
			Fog Architecture		Cloud/server Architecture		
			Layers				
			D	G	D	G	H
Security Objectives	Confidentiality	M,A,Ad,U	DU	GM,GU GA,GAd	DU	GM,GU	HM,HU, HA,HAd
	Integrity	M,A,Ad,U	DU	GM,GU, GA,GAd	DU	GM,GU	HM,HU, HA,HAd
	Availability	M,A,Ad,U	DM,DU, DA	GM, GU, GA,GAd	DM, DA, DU	GM,GU	HM,HU, HA,HAd
	Authentication	M,A,Ad,U	DM,DU, DA	GM,GU, GA,GAd	DM, DA, DU	GM,GU	HM,HU, HA,HAd
	Authorization	M,A,Ad,U	DU	GM,GU, GA,GAd	DU	GM,GU	HM,HU, HA,HAd

C. Assessing Security Objectives

As highlighted in Table III, mechanisms related to security attributes, e.g. encryption, integrity checks, etc., should be utilized within all the layers to ensure the respective objectives. Authentication, which may consist of a user, API, or service identity confirmation, monitoring and analysis is typically performed at the device level. Similarly, availability, which involves the accessibility and constancy of data, services and devices, are monitored and analyzed at the device layer, particularly when using smart devices. For all other attributes, the gateway layer, within fog architecture, handles all the adaption phases. Availability and Authentication related may be further normalized and correlated for analysis at this layer. In a cloud/server based architecture, the gateway layer mainly serves as an agent to monitor (M) the devices and services under its authorization or scope. Whereas, the health systems layer performs the analysis and adaptation phases for all devices and services. It also handles complex or high level monitoring and analysis of events arriving from potential multiple gateways as well this generated by its native applications or services.

D. Assessing Privacy Objectives

As illustrated in Table IV, similar to the security objectives class, methods or mechanisms related to each highlighted privacy attribute should be utilized within all the layers in both architectures. In a fog-based architecture, the gateway layer is responsible for performing all the adaptation phases for its underlying devices and services. Location is typically monitored at the device layer, as there can be devices that would require monitor to send out alerts, hence it needs to be monitored at the device layer and further normalized at the gateway. In a cloud/server- based architecture, a particular gateway monitors its respective devices and services. The health systems layer carries out all the adaptation phases for the entire scope including its own hosting services.

E. Assessing Contextual Factors

The Contextual factors focuses on the importance of any internal or external changes that may be experienced at any layer of the architectures. Such changes may trigger the need of S&P adaptation. Therefore, all related factors should be monitored at every layer within both architectures, as reflected in Table V. However, environmental factors, which mainly refer to changes that may occur outside a monitored device, should be monitored at the gateway layer [11, 13, 14, 25, 26, 27, 28]. Users (patient, practitioners, and system admins) should be permitted to change their preferences, and therefore, the corresponding mechanism should be enforced for utilization at all layers. typically monitored at the device layer, as there can be devices that would require monitor to send out alerts, hence it needs to be monitored at the device layer and further normalized at the gateway. In a cloud/server- based architecture, a particular gateway monitors its respective devices and services. The health systems layer carries out all

the adaptation phases for the entire scope including its own hosting services.

F. Assessing Factors Affecting Adaptation Action Aptitude

Adapting any attribute, for example adapting to new confidentiality settings, may have a negative impact on the system's performance, usability, or S&P objectives. Therefore, it is essential to evaluate the aptitude of a potential solution to a faced threat in the adaptation phase. Attributes corresponding to this notion are captured in the Adaption Actions Aptitude class. Table VI illustrates the most common and vital attributes that are necessary to be evaluated in the adaptation phase (Ad).

TABLE IV. CLASS – PRIVACY OBJECTIVES

Class	Attributes	Process	System Architecture				
			Fog Architecture		Cloud/server Architecture		
			Layers				
			D	G	D	G	H
Privacy Objectives	Data Privacy	M,A,Ad, U	DU	GM,GU,GA,GAd	DU	GM,GU	HM,HU,HA,HAd
	Communication Privacy	M,A,Ad, U	DU	GM,GU,GA,GAd	DU	GM,GU	HM,HU,HA,HAd
	Behavioral privacy	M,A,Ad, U	DU	GM,GU,GA,GAd	DU	GM,GU	HM,HU,HA,HAd
	Location Privacy	M,A,Ad, U	DM,DU	GM,GU,GA,GAd	DM,DU	GM,GU	HM,HU,HA,HAd

TABLE V. CLASS – CONTEXTUAL FACTORS

Class	Attributes	Process	System Architecture				
			Fog Architecture		Cloud/server Architecture		
			Layers				
			D	G	D	G	H
Contextual Factors	Architectural Factors	M,A,Ad	DM	GM,GA,GAd	DM	GM	HM,HA,HAd
	Environmental Factors	M,A,Ad	-	GM,GA,GAd	-	GM	HM,HA,HAd
	Operational Factors	M,A,Ad	DM	GM,GA,GAd	DM	GM	HM,HA,HAd
	User preferences	M,A,Ad, U	DM, DU	GM,GA,GAd, GU	DM, DU	GM,GU	HM,HU,HA,HAd

TABLE VI. CLASS – ADAPTION ACTION APTITUDE

Class	Attributes	Process	System Architecture				
			Fog Architecture		Cloud/server Architecture		
			Layers				
			D	G	D	G	H
Adaption Actions aptitude	Response Time	Ad	-	GAd	-	-	Had
	Efficiency	Ad	-	GAd	-	-	Had
	Energy Consumption	Ad	-	GAd	-	-	Had
	Service factors	Ad	-	GAd	-	-	Had
	Reliability	Ad	-	GAd	-	-	Had
	Memory	Ad	-	GAd	-	-	Had
	Security & Privacy	Ad	-	GAd	-	-	Had
	Network Latency	Ad	-	GAd	-	-	Had
	Throughput	Ad	-	GAd	-	-	Had

TABLE VII. CLASS – SELF-* PROPERTIES

Class	Attributes	Process	System Architecture				
			Fog Architecture		Cloud/server Architecture		
			Layers				
			D	G	D	G	H
Self-* Properties	Self-Healing	M,A,Ad, U	DM	GM, GU, GA, GAd	DM	GM	HM, HU, HA, HAd
	Self- Configuration	M,A,Ad, U	DM	GM, GU, GA, GAd	DM	GM	HM, HU, HA, HAd
	Self-Optimizing	M,A,Ad, U	DM	GM, GU, GA, GAd	DM	GM	HM, HU, HA, HAd
	Self-Protecting	M,A,Ad, U	DM	GM, GU, GA, GAd	DM	GM	HM, HU, HA, HAd

Since, the adaptation phase is conducted at the gateway in the fog architecture, and at the health system layer in the Cloud/Server architecture, the highlighted attributes should be evaluated at the respective layers. Assessing these attributes enables to determine if the adaptive S&P solution can ensure trade-offs amongst these attributes during adaptation, especially in a critical environment such as e-health, where time-sensitive decisions are made.

G. Assessing the System's Self-* Properties

To ensure self-management, the adaptive system has to enforce the monitor, analyze, and adaptation loop feedback in its own processes. This implies that the system has to manage the respective adaptation phases and corresponding functions on the corresponding devices and layers. As reflected in Table VII, the self-* properties for all components responsible for monitoring, analysis and adaptation should be monitored at their respective layer where they are implemented. However, further monitoring (high level), analysis, and adaptation should be handled by gateway in the fog architecture whereas the hospital system layer in the Cloud/Server architecture will manage the same.

III. Results and Discussion

This section critically evaluates the proposed classification and existing assessment frameworks that are proposed for the purpose of assessing adaptive S&P solutions for IoT and/or IoT e-health. The main objective of this effort is to compare our proposed framework with the existing frameworks to evaluate their aptitude in addressing the essential attributes for S&P adaptation with respect to the adaptation process and system architecture. The frameworks that are compared here are: MST [9], AFAS [13], SAS [14] and SMAS [15]. Although there are less numbers of models to be considered for comparison, they are the most related and current efforts with our work and the concept at hand. Furthermore, we intend to reflect on the current practices rather to assess a comprehensive list of existing efforts.

A. The Comparison Approach

The comparison of the frameworks has been made using two dimensions; the evaluation criteria and the comparison score. The criteria intend to determine the comprehensiveness and applicability the reviewed models in the context of Adaptive S&P and aims to conclude:

- Whether or not and to what extent do the reviewed frameworks or models cover the phases in the adaptation process?
- Whether an evaluation framework is suitable to assess Adaptive S&P in a particular IoT-eHealth architecture or both fog-based and server/Cloud-based?
- Which required/identified attributes and to which extent are they addressed by a given evaluation framework or model?

The Comparison score illustrated in Table VIII is an analytical indicator of the level of conformance of an evaluation framework with the comparison criteria, after it is validated. The higher the score is, the better is the evaluation framework. Hence, it enables us to comprehend the comprehensiveness, applicability, and, therefore, the feasibility of the proposed and existing assessment frameworks in assessing adaptive S&P solutions for IoT e-health. The following table describes the criteria on how each aspect of the comparison approach is scored, in order to evaluate each of the candidate frameworks.

B. Analysis of Security Objectives

The major processes; monitoring, analysis and adaptation has been addressed by all the frameworks, however, AFAS, MST and the proposed framework addresses the utilized (U) process as well as illustrated in Fig. 4. AFAS, SAS and SMAS claim to assess all the attributes under security objectives. However, they provide abstract or insufficient information on the architecture and the architectural layers that the framework assesses. Hence it is unclear on how the adaptation requirements are evaluated within the different architectural layers. Whereas MST considers all the adaptation processes, as well as majority of the security objectives, however the framework is only designed to assess cloud/server based architecture's. Hence having a better comprehension of security objectives for Cloud/Server based architectures as opposed to AFAS, SAS and SMAS. Amongst the assessed frameworks, the proposed framework has a better comprehension of the security objectives, as it evaluates these attributes in the context of both, cloud/ server based and fog architectures. Moreover, the assessed frameworks have addressed the majority of the security attributes. However, the authorization attribute is somehow underestimated, which is concerning.

C. Analysis of Privacy Objectives

As illustrated in Fig. 5, SAS and the proposed framework have addressed all the major processes. Additionally, the proposed framework addresses the utilized (U) process as well. None of the frameworks, except from the proposed framework, addresses all the privacy attributes in the context of architecture. SAS highlights the data privacy attribute however, its realization in the context of the architectural aspects is unclear to draw further conclusions. Furthermore, amongst the privacy attributes, data privacy has been mostly addressed in the evaluated frameworks. However, those discussing it only state its importance and consequences and fail to provide details of it, to be addressed at the corresponding architectural layers to ensure effective S&P adaptation.

D. Analysis of Self-* Properties

Similar to the privacy objectives class, the self-*properties classes as shown in Fig. 6 have been widely ignored by majority of the frameworks. The frameworks AFAS and the proposed framework that do consider this class have addressed all the major adaptation processes. Although it claims to assess all the self-*properties attributes, it provides abstract information on the architectural aspects within its assessment.

Hence it is unclear on how the framework assesses the given attributes within the different architectural layers.

Whereas the proposed framework evaluates the self-*properties attributes amongst different architectural layers for both fog and cloud/server based architectures.

TABLE VIII. COMPARISON SCORE DESCRIPTION

Attribute Context	Criteria Description	Score
Adaptation Process (P)	1 point for each process when an attribute is clearly addressed by an identified adaptation process. **Note:** maximum points for a process conformance of an attribute vary from attribute to attribute. Refer to *The Mapping Criteria* for the required processes for each attribute under various classes.	1-4
Architectural (A)	All or the majority of the requirements related to a given attribute are addressed at the corresponding layers for **both** architectures (fog and Cloud/server)	5
	Few of the requirements related to a given attribute are addressed at the corresponding layers for **both** architectures (Fog and Cloud/ Server)	4
	All or the majority of the requirements related to a given attribute are addressed at the corresponding layers for a **single** architectures (fog or Cloud/server)	3
	Few of the requirements related to a given attribute are addressed at the corresponding layers for a **single** architectures (fog or Cloud/Server)	2

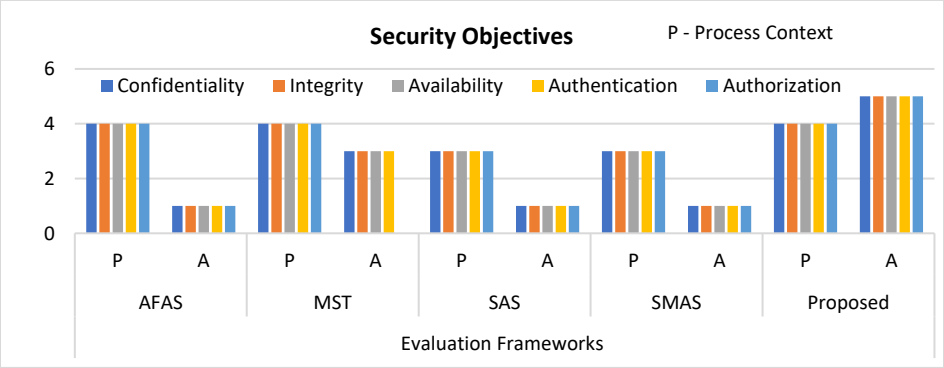

Fig. 4. Comparative Scores of Security Objectives.

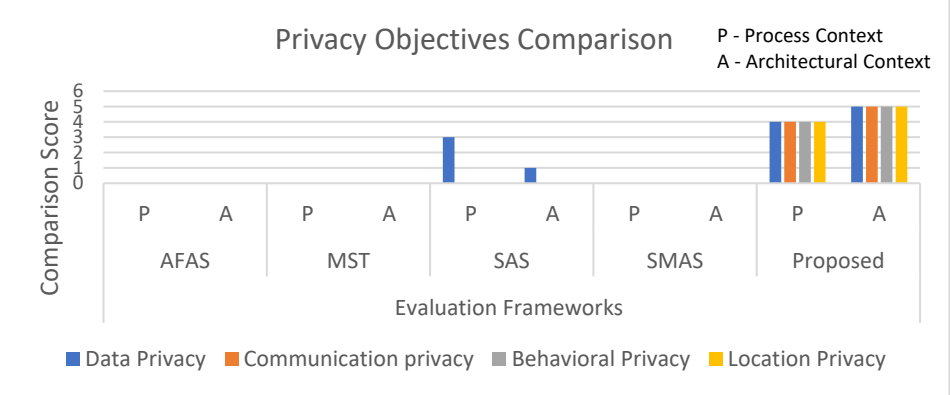

Fig. 5. Privacy Objectives Comparison.

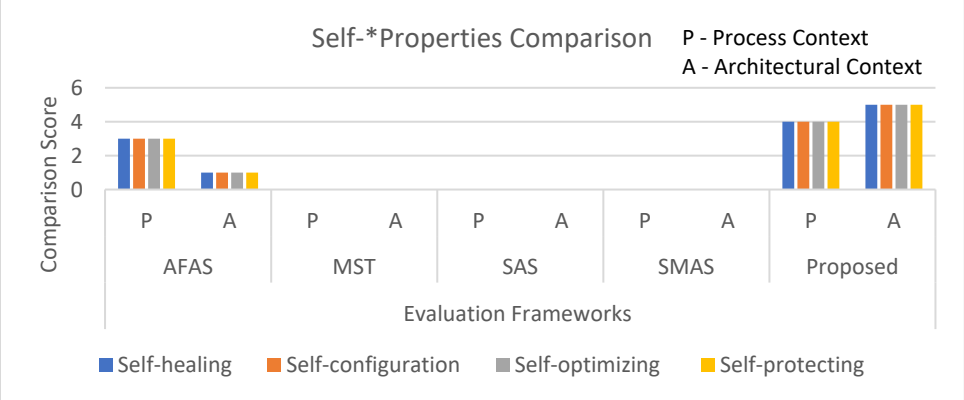

Fig. 6. Self-*Properties Comparison.

E. Analysis of Contextual Factors

The major processes; monitoring, analysis and adaptation have been addressed by all the frameworks as illustrated in Fig. 7. However, the proposed framework addresses the utilized (U) process essential for the user preferences attribute. AFAS and SMAS addresses' majority of the contextual attributes, however the details on the architectural aspects are abstract thus. Hence assessment of these attributes on the architectural layers is indistinct. MST and SAS only consider environmental and operational factors, where MST provides sufficient information on the assessment of these attributes within the layers of cloud/server based architecture. However, SAS provides unclear information on the assessment of these attributes within architectural layers. While the proposed framework considers all the contextual factors within the layers of both architectures.

Amongst the attributes within this class, architectural factors have been ignored by MST and SAS. It is essential to consider architectural factors when assessing adaptive S&P solutions, especially since IoT e-health is a diverse, dynamic, and mobile architecture where new devices can be added or existing devices can be updated or removed more frequently. Hence, the system should be able to handle such changes [13], [25].

F. Analysis of Adaptation Action Aptitude

As shown in Fig. 8, all the frameworks that consider the adaptation action aptitude attributes consider the main process which is adaptation AD, where these attributes are evaluated. SAS does not consider this class in its evaluation, whereas SMAS only considers Energy consumption, Reliability and S&P attributes but lacks architectural details.

However, AFAS, MST and the proposed framework considers all the attributes under this class. However, in terms of the architectural aspects, the proposed framework assesses these attributes within both architectures, while MST only assess these attributes within cloud/server based architecture, and, AFAS provides abstract information on the assessment of these attributes from an architectural perspective.

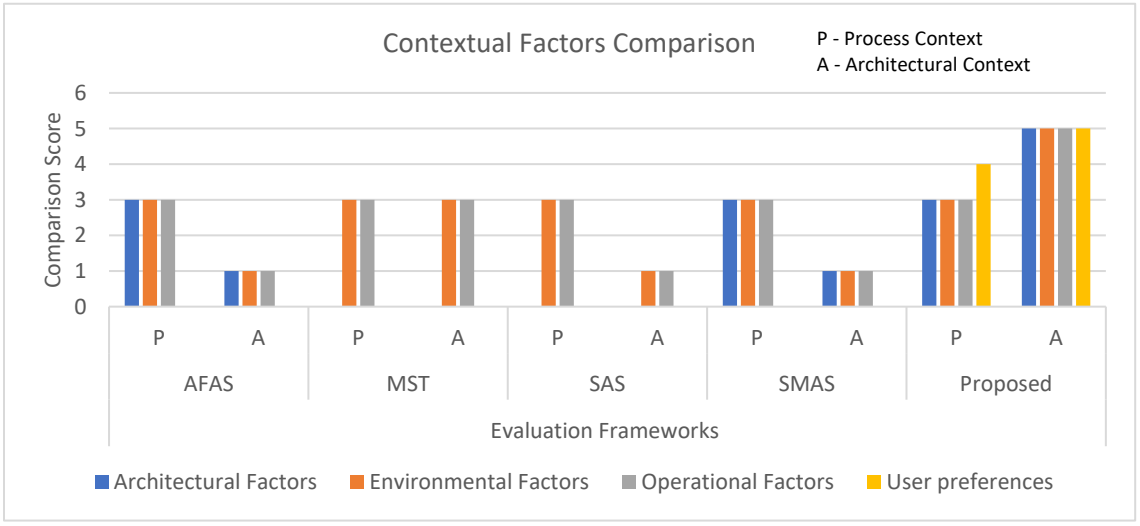

Fig. 7. Contextual Factors Comparison (Note: the Maximum Points for a Process Conformance for Architectural, Environmental and Operational Factors Attributes is 3, Whereas the Process Conformance for user Preferences Attribute is 4).

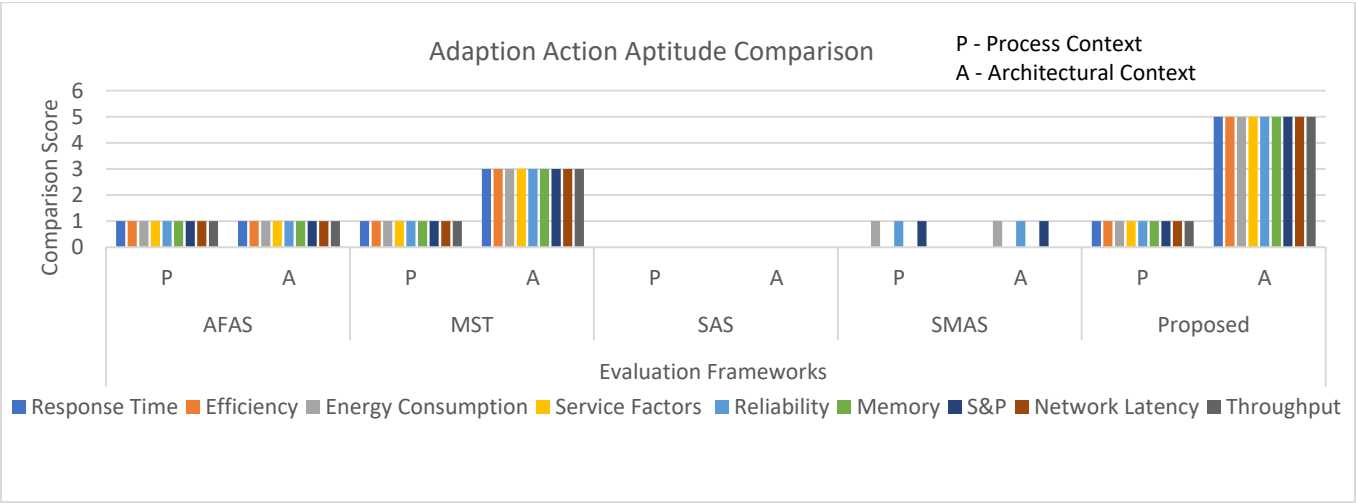

Fig. 8. Adaption Action Aptitude Comparison (Note: The Maximum Points for a Process Conformance for Attributes in this Class is 1).

IV. Discussion on the Overall Comparison

This section highlights the overall outlook of the compared frameworks at the class level. The underneath discussion is based on the observations reflected in Fig. 9, which depicts the maximum points achieved by each compared framework by aggregating their attributes' points in each class, as a result of the above comparison.

It can be observed that although the proposed framework offers a more in-depth view of the security objectives, overall, there seems to be an above average comprehension and consensus on achieving the related attributes. Moreover, except for the proposed framework, all other frameworks have considerably overlooked the privacy aspects. Apparently, privacy objectives are assumed to be enforced with security mechanisms, which should not be exercised as they have different purposes, scopes, and mechanisms. Alongside security objectives, it is vital to address the privacy objectives from different perspectives. The lack of privacy objectives can potentially lead to misuse of patient's sensitive information, such as unauthorized disclosure or usage and even potential identity frauds [3], [4].

Similar to the privacy objectives, the adaptive system's self-* properties are also underestimated. Doing so may lead to the compromise of the system itself. It can be seen that the proposed framework exceptionally stressed on the need of considering the self-* properties. Whereas, AFAS provides fair details of the related properties at the adaptation process level, it lacks to provide enough information on the architectural aspects within its assessment.

MST assesses majority of the attributes for cloud/ server based architectures only. Although AFAS, SMAS, and SAS consider majority of the contextual attributes, these frameworks provide very abstract information on the architectural aspects. It is apparent that the proposed framework fully suffices the adaption action aptitude requirements for both fog and cloud/Server architectures. While, MST assesses all of the attributes for cloud/ server based architecture only. Although AFAS and SMAS consider all the attributes under this class, the frameworks provide unclear information on the architectural requirements.

V. Conclusion and Future Plans

The proposed framework assists us to recognize, realize, and assess the essential factors for adaptive S&P solutions in the context of the IoT e-health architecture and the adaptation process. It lets us evaluate related solution in a broader spectrum, the overall needs, therefore providing a comprehensive understanding of the overall problem. The comparison made with the existing assessment frameworks reflects that our work introduces considerable improvements by how essentials attributes should be managed in the context of architecture and the adaptation process, which is the key contribution. Most of the frameworks discounted the architectural aspects and their importance, which may negative affect the whole purpose of an adaptive system. Moreover, current assessment frameworks are more focused on a particular set of essential factors or generally highlight them. In contrast, the presented framework provides a holistic set of attributes or requirements that address all the major aspects of an adaptive S&P system and assess them in the context of underlying architecture and the adaptation process. Thus, offers a comprehensive mechanism to assess the feasibility of a given adaptive S&P solution.

Although this study primarily studies e-health as an IoT application, it can be generalized to similar IoT-based architectures. Nevertheless, it needs further investigation to consummate this hypothesis. Furthermore, assessing specific performance and QoS factors of adaptive S&P solutions for IoT e-health from a quantitative perspective could result in a more considerable attempt. In addition, the proposed framework could have added more value if common practices or mechanisms for each attribute were highlighted. This would have offered a sense of trending mechanisms and made the criteria more mature and comprehensive.

In future, we plan to extend this research by addressing the limitation discussed. We plan to study other IoT architectures to investigate if the proposed assessment framework can be utilized or requires further refinements. Moreover, we intend to further improve the proposed assessment framework by investigating the commonly utilized mechanisms for each attribute and analyzing the trends in the mechanisms utilized to make the framework more beneficial and inclusive. Lastly, we intend to work on a more rigor assessment to present a more acceptable capability maturity model.

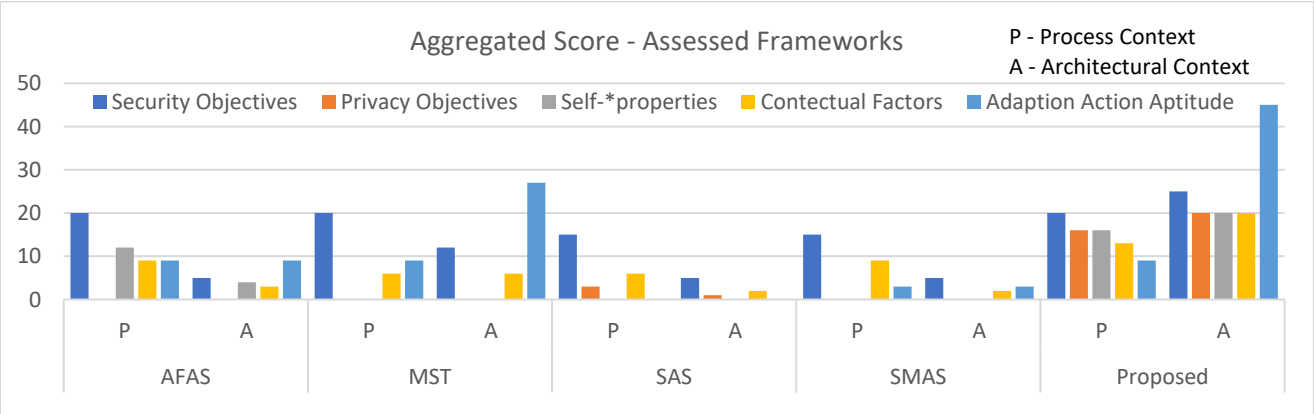

Fig. 9. Aggregated Scored of the Compared Assessment Frameworks.

REFERENCES

[1] Manyika J, Chui M, Bisson P, Woetzel J, Dobbs R, Bughin J et al. The Internet of Things: Mapping The Value Beyond The Hype. 24th Ed. New York, NY, USA: McKinsey Global Institute; 2015.

[2] Malasinghe LP, Ramzan N, Dahal K. Remote patient monitoring: a comprehensive study. Journal of Ambient Intelligence and Humanized Computing. 2019 Jan; 10(1):57-76.

[3] El Emam K. Guide to the De-Identification of Personal Health Information [Internet]. 1st Ed. New York, USA: Auerbach Publications; 2013 [cited 12 January 2022]. Available from: https://bit.ly/3aYSCTy

[4] Malin BA, Emam KE, O'Keefe CM. Biomedical data privacy: problems, perspectives, and recent advances. Journal of the American medical informatics association. 2013 Jan 1; 20(1):2-6.

[5] Schaub F, Könings B, Weber M, Kargl F. Towards context adaptive privacy decisions in ubiquitous computing. In2012 IEEE International Conference on Pervasive Computing and Communications Workshops 2012 Mar 19 (pp. 407-410). IEEE.

[6] Boudko S, Abie H. Adaptive cybersecurity framework for healthcare internet of things. In2019 13th International Symposium on Medical Information and Communication Technology (ISMICT) 2019 May 8 (pp. 1-6). IEEE.

[7] Yang Y, Zheng X, Guo W, Liu X, Chang V. Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. Information Sciences. 2019 Apr 1;479:567-92.

[8] Aman W, Kausar F. Towards a Gatewaybased Context-Aware and Self-Adaptive Security Management Model for IoT-Based eHealth Systems. International Journal of Advanced Computer Science and Applications. 2019 Jan 1;10(1):280-7.

[9] Aman W, Snekkenes E. Managing security trade-offs in the internet of things using adaptive security. In2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) 2015 Dec 14 (pp. 362-368). IEEE.

[10] Gebrie MT, Abie H. Risk-based adaptive authentication for internet of things in smart home eHealth. InProceedings of the 11th European Conference on Software Architecture: Companion Proceedings 2017 Sep 11 (pp. 102-108).

[11] Arfaoui A, Kribeche A, Senouci SM, Hamdi M. Game-based adaptive remote access VPN for IoT: Application to e-Health. In 2018 IEEE Global Communications Conference (GLOBECOM) 2018 Dec 9 (pp. 1-7). IEEE.

[12] Arfaoui A, ben Letaifa A, Kribeche A, Senouci SM, Hamdi M. A stochastic game for adaptive security in constrained wireless body area networks. In2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC) 2018 Jan 12 (pp. 1-7). IEEE.

[13] Aman W. Assessing the feasibility of adaptive security models for the internet of things. InInternational Conference on Human Aspects of Information Security, Privacy, and Trust 2016 Jul 17 (pp. 201-211). Springer, Cham.

[14] Leister W, Hamdi M, Abie H, Poslad S. An evaluation framework for adaptive security for the IoT in eHealth. International Journal on Advances. 2014 Dec 1.

[15] Savola RM, Abie H. Metrics-driven security objective decomposition for an e-health application with adaptive security management. InProceedings of the International Workshop on Adaptive Security 2013 Sep 8 (pp. 1-8).

[16] Abie H, Savola RM, Bigham J, Dattani I, Rotondi D, Da Bormida G. Self-healing and secure adaptive messaging middleware for business-critical systems. International Journal on Advances in Security. 2010;3(1&2).

[17] Abie H, Balasingham I. Risk-based adaptive security for smart IoT in eHealth. InProceedings of the 7th International Conference on Body Area Networks 2012 Feb 24 (pp. 269-275).

[18] Farahani B, Barzegari M, Aliee FS, Shaik KA. Towards collaborative intelligent IoT eHealth: From device to fog, and cloud. Microprocessors and Microsystems. 2020 Feb 1;72:102938.

[19] Salehie M, Pasquale L, Omoronyia I, Nuseibeh B. Adaptive security and privacy in smart grids: A software engineering vision. In2012 First International Workshop on Software Engineering Challenges for the Smart Grid (SE-SmartGrids) 2012 Jun 3 (pp. 46-49). IEEE.

[20] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems. 2013 Sep 1;29(7):1645-60.

[21] Dey S, Sampalli S, Ye Q. A context-adaptive security framework for mobile cloud computing. In2015 11th International Conference on Mobile Ad-hoc and Sensor Networks (MSN) 2015 Dec 16 (pp. 89-95). IEEE.

[22] Sethi P, Sarangi SR. Internet of things: architectures, protocols, and applications. Journal of Electrical and Computer Engineering. 2017 Jan 26;2017.

[23] Farahani B, Firouzi F, Chang V, Badaroglu M, Constant N, Mankodiya K. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Generation Computer Systems. 2018 Jan 1;78:659-76.

[24] Rahmani AM, Gia TN, Negash B, Anzanpour A, Azimi I, Jiang M, Liljeberg P. Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Future Generation Computer Systems. 2018 Jan 1;78:641-58.

[25] Gheisari M, Wang G, Khan WZ, Fernández-Campusano C. A context-aware privacy-preserving method for IoT-based smart city using software defined networking. Computers & Security. 2019 Nov 1;87:101470.

[26] Zemmoudj S, Bermad N, Omar M. CAPM: Context-aware privacy model for IoT-based smart hospitals. In2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) 2019 Jun 24 (pp. 1139-1144). IEEE.

[27] De Matos E, Tiburski RT, Amaral LA, Hessel F. Providing context-aware security for IoT environments through context sharing feature. In2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) 2018 Aug 1 (pp. 1711-1715). IEEE.

[28] Zhu J, Kim KH, Mohapatra P, Congdon P. An adaptive privacy-preserving scheme for location tracking of a mobile user. In2013 IEEE International Conference on Sensing, Communications and Networking (SECON) 2013 Jun 24 (pp. 140-148). IEEE.