Towards a Gateway-based Context-Aware and Self-Adaptive Security Management Model for IoT-Based eHealth Systems

Waqas Aman[1], Firdous Kausar [2]
Information Systems Department, College of Economics and Political Science[1]
Electrical and Computer Engineering Department, College of Engineering[2]
Sultan Qaboos University
Muscat Oman

***Abstract*—IoT-based systems have considerable dynamic behavior and heterogeneous technology participants. The corresponding threats and security operations are also complex to handle. Traditional security solutions may not be appropriate and effective in such ecosystems as they recognize and assess a limited context, they work well only with high-end and specific computing** platforms**, and implement manual response mechanisms. We have identified the security objectives of a potential IoT-eHealth system and have proposed a security model that can efficiently achieve them. The proposed model is a context-aware and self-adaptive security management model for IoT, in eHealth perspective that will monitor, analyze, and respond to a multitude of security contexts autonomously. As these operations are planned at the gateway level, the model exploits the advantages of computing in the Fog Layer. Moreover, the proposed model offers flexibility and open connectivity to allow any smart device or *thing* to be managed irrespective of their native design. We have also explained how our model can establish and serve the essential security objectives of an IoT-based environment.**

Keywords*—*Internet of things; security; self-adaptation; context awareness; ehealth

I. Introduction

This Internet of Things (IoT) has huge prospects in the healthcare sector. Both the service providers and patients demanding continuous monitoring, such as those having chronic conditions or living remotely can greatly benefit from its realization. IoT-enabled health systems can considerably cut off the cost, time, and efforts required in traditional healthcare services. Corresponding solutions can offer more personalized services and can greatly extend traditional services. The concept has also brought a substantial convenience for individuals who want to keep a continuous track of their health related activities. Recently, a high demand for the related health sensors and wearables has been observed globally. IBM estimates that IoT-based health solutions will achieve a $1 trillion market share by 2025 [1].

The IoT-eHealth environment is considerably dynamic and heterogeneous. The mobility aspects and environmental changes introduce high dynamicity, which make it challenging to recognize and manage an operational context manually. Moreover, because of the *things*, services and users' diversity, substantial heterogeneity exists in approaches to the *things'* design, communication, processing, and data representation. These two concerns can introduce significant obstacles for the IoT-eHealth system beneficiaries to consider and adopt any related solution.

Since personal and other sensitive data are processed and communicated in such ecosystems, particularly in IoT-eHealth, providing suitable security and privacy (S&P) features is of utmost importance. The current IoT-eHealth solutions in the market, e.g., smart apps, experimental and ready-to-use solutions and platforms, such as [2-4], provide security as a single and fixed and single solution. For example, protecting data communication using SSL implementation only. All other critical operations and components of the ecosystem, irrespective of their individual S&P requirements, have to agree with these fixed and single solutions. Thus, a compromise is made that may lead to fatal security breaches at some point of time.

Traditional S&P solutions like anti-malwares, firewall, IDS, etc. are not feasible to be incorporated in individual *things* for a variety of reasons. These *things* may be smart sensors but may not have the satisfactory computing resources necessary to accommodate them. Moreover, these solutions are designed for limited and specific computing platforms, and may not address the IoT heterogeneity. Above all, these solutions analyze a particular security concern, e.g. malwares, specific network traffic, or some integrity issue or behavior, but do not assess the overall context.

Moreover, Critical process in IoT-eHealth including security, data analysis, mobility, and adaptation, if performed at the gateway, i.e., the Fog layer, rather than the Cloud can significantly improve overall system performance [5]. Current literature, such as [6-8] seems to either have ignored the realization of security capabilities at this layer or have provided stringent solutions, or have focused on a particular threat type or security objective.

A. Solution Objectives

The above-mentioned shortcomings and problems motivate us to design a security model for IoT-enable systems with the following desired security objectives.

1) Holistic security: Unlike traditional S&P solutions, the model needs to be holistic and should not focus on a particular (or few) threat(s) or objective(s).

2) Self-Adaptation and context awareness: Context refers to information that is used to describe a situation whereas context-awareness is the property of an entity to use context to provide relevant information and service [9]. Context can be primary, secondary, or conceptual [10]. Primary is the raw data generated by objects. Secondary context is refined from primary context to identify target variables. Conceptual context reflects the relationship among different contexts. IoT-based systems being dynamic environments, operational and environmental contexts may change frequently. Therefore, an anticipated security system should be able to monitor, refine, analyze, the above-mentioned context types.

Moreover, to adapt optimally and flexibly against a given context, that requires reconfigurations, the system should identify and suggest multiple feasible security options to choose from, instead of relying on a stringent, fixed and single security solution. Such reconfigurations should be performed autonomously to enable the self-adaptation, which is a desired property in IoT-based ecosystems [5]. We refer to self-adaptation as the ability of the system to take decisions and actions to respond to a security situation, either a threat or a legitimate security request or operation.

3) Open connectivity: To address the IoT heterogeneity, the anticipated system should be open to accept any (authorized) device. Having such a feature will allow things to be managed by the system irrespective of their computing and communication stack diversity. We consider the thing to be a smart device that has apt processing and memory capacities, besides having any sensing and actuating abilities.

4) Minimize decision delays: To ensure that real-time security services, deemed as critical, are accomplished near to the edge devices (things). Such realization will minimize any delays in analysis, decision making, and response, and will reduce the potential corruption that may be caused during data transfer between edge and remote servers, including those in the Cloud.

In this paper, we attempt to conceptualize a system model to comprehend and capture the listed objectives. We present the system Ontology to highlight the major concepts and their relationships. The proposed Ontology, with the help of Semantic Web Technologies, will be exploited further to be utilized at system runtime. Moreover, to conceptualize the system model, a layered architecture is specified.

Rest of the article is organized as follows: Related work is presented in Section 2 followed by a detailed description of the proposed system in Section 3. In Section 4, we provide a discussion to extend the system functionality and to elaborate how the anticipated objectives can be managed by the proposed system. Finally, a conclusion and future plans are discussed in Section 5.

II. Related Work

S. Dey et al. [11] presented a context-adaptive security framework deployment at cloud server for different mobile cloud computing applications in order to provide secure communication among mobile client and cloud server. Security framework comprises of the cognitive, adaptive, and authentication module. They use the notion of object-oriented cloud federation where there is one master cloud and varied number of inner clouds. Each incoming connection request from a mobile client is received by master cloud that performs its verification by utilizing cognitive module. The adaptive module selects an appropriate inner cloud where mutual authentication is performed by authentication module through Message Digest and Location-based Authentication (MDLA) [12] technique in order to establish secure communication session between mobile client and cloud sever. It also lacks the parameter escalation inside MDLA.

M. Hamdi et al. [13] proposed a game-based adaptive security mechanism for the IoT- eHealth, Body Area Network (BAN) application. An adaptive security policy based on Markov game-theoretic model is proposed with respect to energy, memory, channel, intruder and hybrid adjustment. Adaptation of security policy parameters is only performed at sensor nodes or devices without considering the preferences of users. It basically concentrating on self-optimization for authentication and self-healing for communication purpose. Some other adaptive security techniques based on game theory are proposed in [14, 15].

Abie [16] proposed models for adaptive security and trust management for autonomic message-oriented middleware system. It works on the basic principle of collecting and analyzing the contextual information from environment and system and modifying the security parameters to varying environment dynamically. This is a theoretical model and has not been tested for real IoT application to validate its performance.

A learning-based adaptive security management mechanism for IoT eHealth applications is proposed in [17, 18]. It performs the adaptive security management by regularly monitoring and gathering the information of changes in the environment. It applied analytical function on gathered information to find the changes in the environment and predictive function is applied to calculate the potential actions based on evaluation. The decision making device takes a decision of adapting to the changes or not. The final step is to perform the validation and evaluation of the capability to adapt to the difficulties in dynamic environment with increasing level of threats.

Gebrie et al. [19] presented a risk-based adaptive authentication method for device and user which regularly observes the changes in the channel characteristics such as RSSI, channel gain, temporal link signature and Doppler's measurement. It then performs the analysis on the observations by using naïve byes machine algorithm and adapt to different authentication level by anticipating the security risk in the changing environment.

An architecture of a testbed for adaptive security for the IoT in eHealth is presented in [20] by utilizing the open source software and commercial ready-made products. A patient health related information is collected by low power sensing modules which forward this information through a gateway device to eHealth application in the cloud. They provide lightweight solution in term of energy consumption but not focused on security concerns.

An adapted security model based on Ontology for smart environment is proposed in [21]. Data is collected about the changes in environment by using different security parameters and stored in Ontology. A security risk is measured by different security parameters knowledge stored in Ontology to do the prediction of future events. It does not provide with the details or examples of risk-based security parameters.

A survey on different adaptive security mechanisms in the ubiquitous computing environment is given in [22]. It provides the analysis of different security methods by using different security measures based on trust and context in the continuously changing environment.

Harb et al. [23] proposed a context aware group key management protocol for securing the multicast communication in IoT applications. It deploys a context aware security server for the purpose of establishing secure multicast session by gathering context data from nodes and key distribution servers, analyze the gathered data and assign nodes to appropriate key distribution servers to acquire the group key. Context- awareness is evaluated based only on load balancing among different key distribution centers without taking into account the threats or risk levels associated with dynamic environment.

Abie et al. [24] described a risk management architecture for IoT healthcare applications. It exploits the game theory concepts for risk analysis in dynamic environment and takes the decision of adjusting the level of security parameters and altering the configuration of security system based on changes in the surroundings.

Philip et al. [25] developed a context aware policy-based access control system for computing devices. Policy is devised based on data gathered from different resources within the control system and from environment and analyze this date by with respect to context in order to take decision of granting access to resources or execution of queries.

A context and quality of service aware Ontology-based trust model is proposed in [26], which take the feedback from services users to adapt the trust model as per users' requirements. It develops the two distributed trust propagation and service discovery models to enhance the security and trust of discovery structure.

III. The Proposed System

We elaborate the system model from two perspectives, the system Ontology and its conceptual architecture. The Ontology, shown in Fig. 1, highlights the system's major concepts. An Ontology provides an ease to conceptualized and describe the complex concepts and their relationships during a system design phase, and when developed with semantic technologies, it can also be utilized at runtime. Hence, we chose to capture the IoT-eHealth multi-variant and complex concepts and the concerning vocabulary in the proposed Ontology. It will be refined further and will be adopted during system execution. The architectural view, depicted in Fig. 2, highlights how the major components and communication among them can be perceived.

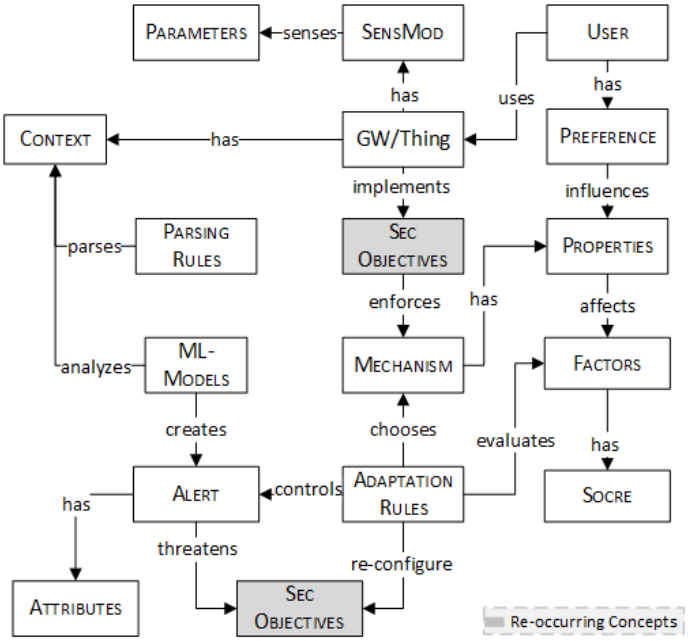

Fig. 1. The Proposed System Ontology.

A. The Proposed System Ontology

This section describes the major concepts in the proposed system Ontology. It comprises the vocabulary necessary to comprehend the diverse concepts related to security, devices, application, capabilities, configurations, and users. The Ontology will serve as a key knowledgebase during analysis and adaptation. A high-level illustration is presented in Fig. 1.

- *GW/Thing:* It is the device, the gateway (GW) or a *thing*, to be monitored. GWs need to monitored continuously too as they are critical assets in IoT-eHealth scenarios and in the proposed systems settings
- *Context:* Information that describes a security phenomenon, event, or situation including both potential threats and security related requests or operations. It can be sensing, communication, storage, processing, and security adaptation information of the monitored devices. Both stored and current contexts
- *SensMod:* The sensing (or actuating) component of a *thing.* A *thing* may have more than one such components
- *Parameters:* Refers to both environmental and health related characteristics, e.g. heat, temp, camera orientation, ECG, etc.
- *User:* the system user, e.g., the patient
- *Preference:* the user preferences about the system usage, e.g. connectivity, security and privacy, usability, etc.
- *Sec-Objective:* Refers to the security related objectives, e.g., authentication, key management, availability, confidentiality, device authentication and registration, etc.
- *Parsing Rules:* Rules used by the systems to parse, transform, and refine the primary context collected from the source (*thing*) or from the *thing-gateway* region
- *Mechanism:* The security algorithms or techniques need to implement and ensure the *SecObjectives*, e.g., AES, ECDHE, Challenge/Response schemes, CAPTCHA, etc.
- *Properties:* The necessary properties of the Mechanisms, e.g., Key length, random numbers, Password Length, digital certificate, image or audio CAPTCHA, etc.
- *Factors:* System features including those derived from user preferences and *thing* competences, e.g. usability, reliability, QoS, battery life, etc., that may be negatively or positively influenced by a given Mechanism's *Property*.
- *Score:* Each Factor has a utility value (score) associated in accordance to the *Property*. For instance, a high AES's key length has an increased *reliability* value but could have a lower value for QoS for a low-end temperature sensor. Thus, for each *Property*, there will be an aggregated score that will represent the overall utility of the *Property.*
- *Adaptation Rules:* Rules that will direct the selection and evaluation of the particular *Mechanisms*, their *Properties* and score aggregation against a particular *Alert* (final derived context) generated.
- *ML Models:* Machine Learning (ML) models that will analyze a given *Context*. These will be supported by ML algorithms and current/stored context.
- *Alert:* A security token that highlight a particular security threat or request that needs immediate attention, e.g. DoS, Code Injection, device registration and authentication, etc. It can also be considered as the final, analyzed or derived context required for adaptation decision.
- *Attributes:* Data items to distinctly describe a given Alert, e.g., Level, device information, risk or request info, etc. In other words, they accumulate an Alert context.

B. System Architecture

It can be perceived, as in Fig. 2 that the architecture implements a control feedback loop. It collects context from its infrastructure components, and then controls them with an adapted configuration(s) as a feedback. The architecture is comprehended in three logical layers.

The Monitored **Device Layer** is composed of all the managed devices, including the *things* at the edge and gateways at the Fog layer. The **Local Context Manager** collects the device native context by listening to the output terminal, e.g. the device serial port, of the *thing.* Such context could be the notifications or events generated and written to the terminal. This manager also provides an interface between the monitored device and the **Context Manager**'s *Parsing Agents* to communicate the context collected. The **Local Controller** receives and parses the new security configurations (vocabulary) or instructions from the **Context Adapter** *(Messenger)* and passes them to the respective referenced security library in the *Security Modules* component, which adapts them upon receipt. **Security Modules** is a framework of security libraries that will implement corresponding mechanisms. **Sensing Module** is responsible for environmental and health related parameters.

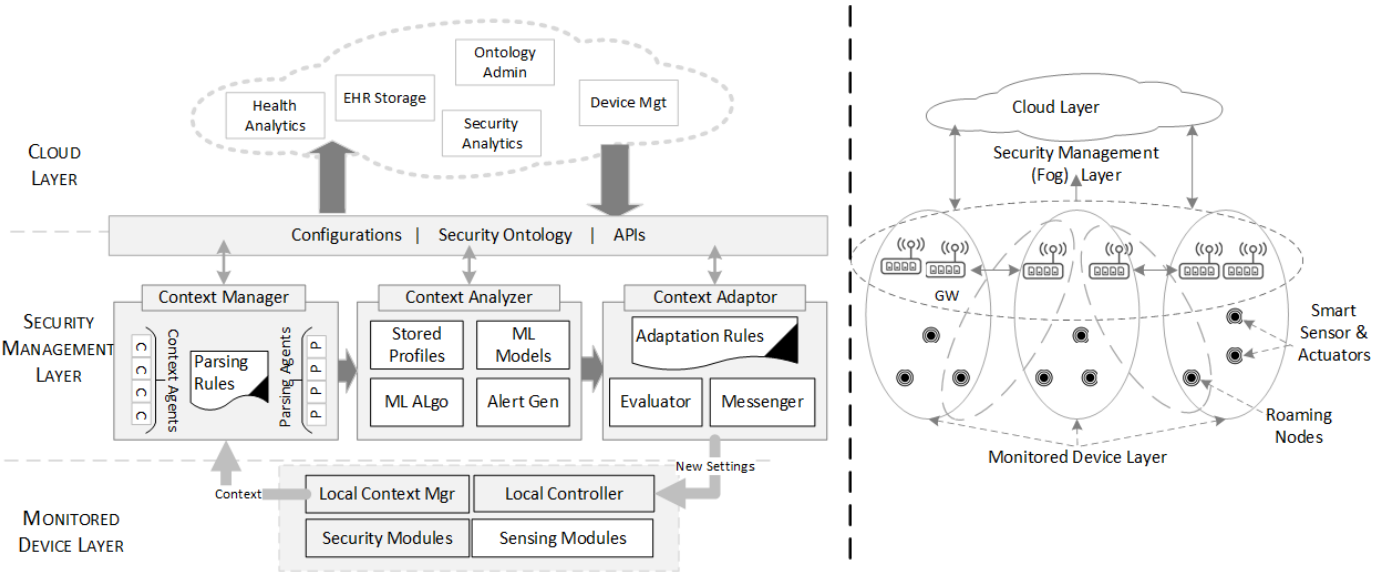

Fig. 2. System Architectural Concept–Layered View.

The Security Management Layer (SML) is implemented in the Fog Layer, i.e., at the Gateway, to avoid the concerns highlighted in the Section 1 (point *d*). As the gateway manages most of the critical operations, it must be considered as a vital asset and should be monitored as well. Therefore, as stated earlier, its processing context, communication, and adaptation behaviors must also be assessed. SML contains three major components that monitors and analyzes a context, and decides whether and what to choose (adapt) as new configurations. Using device-specific **parsing agents and rules**, the **Context Manager** parses, refines, and transforms the monitored context. Device-specific agents' existence is necessary to recognize and transform the context from vendor-specific implementation to the anticipated system-specific format. **Context Agents** can be considered as utilities that capture the *thing-gateway* region specific context, e.g. device in/out-bound communication pattern. **Context Analyzer** integrates the intelligence require to analyze and correlate contexts for possible risks or any other security request or operation. Analysis will be supported by **Machine Learning (ML) models**, current context, and stored data (context or profile). **Alert Generator** is a component that will transform any security context, analyzed by the ML Model(s), to an actionable token (alert) that will contain the necessary information to distinctly characterize the analyzed (concluded) context. The **Context Adaptor** ensures the autonomous and optimal security response to the alert notified. The **Adaptation Rules** provides the necessary guidelines to choose the concerning particular *Mechanisms*, their *Properties*, and scores stored in the Ontology. Using a score aggregation mechanism, the **Evaluator** will assess all the selected mechanisms their respective properties, as well as the current security settings to decide new optimal security configurations or instructions. This decision is collected, organized, and communicated by the **Messenger** with the monitored device Local Controller.

The Cloud Layer, although not in the scope of this study, may be used for a variety of services including, health diagnostics, record storage, and may provide interfaces to applications that may access such information.

IV. Discussion

In this section, we provide arguments and explanation to detail how the objectives, identified in Section 1, could be managed by the proposed model. We also extend the discussion to include implementation perspectives and computation complexity.

A. Holistic Security

Instead of focusing on a particular set of threats, the proposed system is able to capture and analyze a multitude of contexts, including in/out-bound communication behavior, device processing integrity, etc. Moreover, the security adaptation behavior will also be assessed to protect the system from any rouge or compromised gateways. Furthermore, the monitored contexts are correlated among each other to offer more comprehensive analysis and build a reliable context for adaptation. Moreover, beside threat analysis, the system also manages other security operations, such as device authentication while roaming and new device registration, and sharing of analysis intelligence. Therefore, the system covers a broader spectrum of security.

B. Self-Adaptation and Context Awareness

To understand how the proposed model enforces context awareness, consider the following *availability vs. confidentiality* scenario. If it is analyzed that the battery of a critical actuator has exhausted to a particular lower threshold, multiple encryption *mechanisms* and their *properties* for that device will be assessed. Assuming that availability has a preference here, the *property* among the available *properties* (and their corresponding *mechanisms*) having a higher utility

for QoS (availability) will be adapted, instead of choosing a one that has a higher security reliability. Later on, when the actuator is charged to reach a higher level, the system will adapt to higher security state, with maximum utility for security reliability. It can be concluded that that system is continuously observing, analyzing, and self-adapting to multiple contexts, including current status of a device component, its resources, user preferences, security requirements, and again any change in the operational environment (battery status). Therefore, the system adapts autonomously and efficiently while being context-aware.

Primary context or raw data about communication, processing, etc. are intercepted and gathered via the *Context Agents* and *Local Context* publishers, and are further refined by *the Parsing Agents* to build *Secondary context*. The later will be then further assessed by the ML models to develop a c*onceptual context* to correlate different secondary contexts for potential risks and further decisions.

C. Open Connectivity

Smart *things*, including gateways, vendors focus on sensing and actuating modules and, usually, do not embed capacities, such as the proposed *Security Modules*. New heterogeneous devices may be introduced, existing may be modified, or they may hover from one gateway to another, which will make connectivity and therefore security management a challenge. To ensure that any smart object can be connected to and managed by the proposed systems, we intend to introduce a Secure Registration protocol. The objective of this protocol will be to register new heterogeneous objects and install the operational components, tinted in the *Monitored Device Layer* of Fig. 2, necessary for the proposed system to work efficiently. Further explanation is provided in the implementation perspective sub-section.

D. Avoiding Decision Delays

The entire monitoring-analysis-adaptation process is realized at the *thing-gateway* layer. Such a design can increase the overall process performance and throughput deemed suitable and required at the *thing*-level to operate efficiently, as anticipated at the Fog layer [5, 6].

E. Extension to the Cloud

Currently, our aim is to detail and strengthen the proposed system at the *thing-gateway* level. However, we would like to extend the proposed concept to include the Cloud layer as it is a key aspect in Cloud-assisted eHealth solutions. The underlying concepts can be reviewed for security contexts related to a spectrum of activities performed at in the Cloud and in the *Gateway-Cloud* region. However, initially, this region and the corresponding context is used to access and confirm information required for device authentication and registration, and any related security analysis that is necessary to achieve the secure open connectivity objective.

F. Lightweight Approach

The proposed concepts require that the monitored devices, including sensors, should have the *Security Modules***,** a container having a collection of security libraries, available for security adaptation at runtime. Although, we have highlighted previously about our viewpoint of a smart *thing*, one may perceive that a *thing* should now necessitate more extended computational resources for the proposal to work efficiently.

However, security computations (changes) may be required occasionally, only when system needs adaptation, and is not continuous task. However, such a *thing* will only need some extra memory than the usual to accommodate the *Security Modules* and miniatures scripts to send and receive messages. Heavy tasks, such as context refinement, analysis and adaptation decision making are still executed outside these anticipated *things*, and are performed in the gateway at the Fog layer.

G. Implementation-Initial Plan

The security registration protocol, highlighted previously, will securely install the necessary components required by the system. The installation will be guided by two modes, *gateway* and *thing*, whereas the installed object will be a middleware. In case of *gateway* mode, both the components of the Security Management and Monitored Device Layers will be installed. In the *thing* mode, only the components of the Monitored Device Layer will be installed.

We intend to implement a secure messaging protocol, such as Message Queuing Telemetry Transport (MQTT) [27], to realize the communication of contexts for analysis and adaptation. As shown in Fig. 3, the *thing-gateway* region primary contexts will be organized into topics and published via publishers (Pub) to a Broker that will forward them to the device-specific (parsers) subscribers (Sub) for further refining and transformation. Similarly, a *thing* local context will be sent to the broker however, such context will be sent as captured whereas it organization into topics will be performed at the Broker to avoid any additional computations at the *thing* level. Moreover, the new adapted settings, when confirmed by the *Context Adapter*, will be communicated using this messaging system with the respective device(s) subscribers.

A number of techniques, tools, and technologies are available to describe and develop the proposed Ontology. We intend to adapt Resource Description Framework (RDF) and Web Ontology Language (OWL) to develop the ontology and will use SPARQL [28] to access and update it.

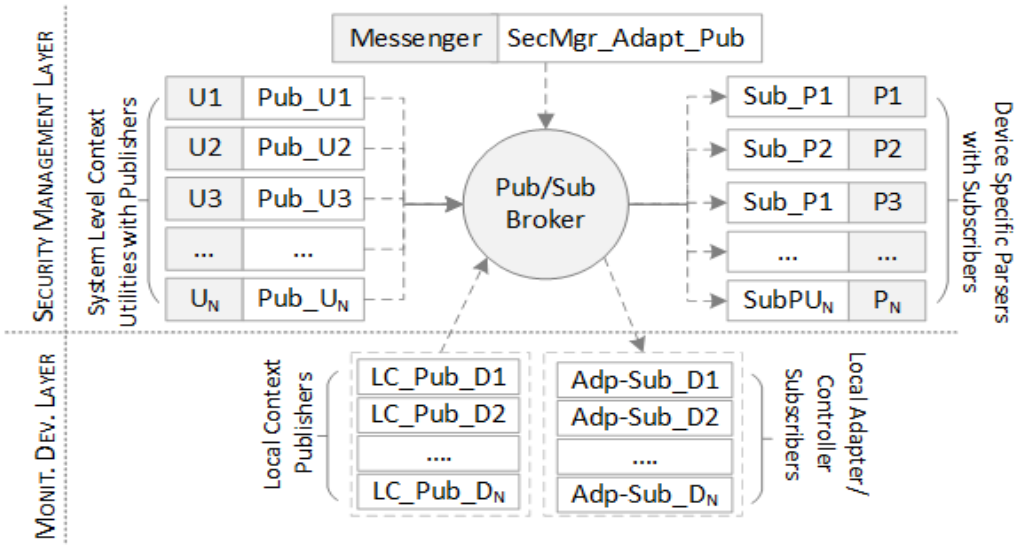

Fig. 3. Gathering and Communicating context via a Pub/Sub System.

V. Conclusion and Future Work

IoT-based systems are dynamic and heterogeneous environments. Traditional security measures are infeasible to provide protection in such an environment as they are fixed solutions designed for specific computing platforms and cover limited context. We presented the Ontology and the conceptual design of a context-aware and self-adaptive security model that would be helpful to overcome the shortcomings in the traditional solutions, such as the limited context scope and optimal autonomous response. Moreover, the proposed model is able to handle the dynamic and heterogeneous traits in an IoT-based system.

Our next step is to detail the technical architecture and framework, investigate, suggest or adapt techniques for the major processes, i.e., context monitoring, analysis, correlation, and adaption. Furthermore, we intend to develop a prototype supported with an IoT-based eHealth case study to realize and validate the functionality and feasibility of the proposed system.

Acknowledgment

The work in this paper is supported by the Sultan Qaboos University under the internal grant approved for the research project, titled Cloud assisted eHealth. Moreover, we are grateful to the anonymous reviewers for their valued feedback.

References

[1] How Internet of Things (IoT) is changing the face of Healthcare. Online: https://www.ibm.com/blogs/insights-on-business/healthcare/internet-things-iot-changing-face-healthcare/. Last Accessed: 25 December 2018.

[2] e-Health Sensor Platform V2.0 for Arduino and Raspberry Pi. Online: https://www.cooking-hacks.com/documentation/tutorials/ehealth-biometric-sensor-platform-arduino-raspberry-pi-medical. Last accessed: 19 December 2018.

[3] Samsung Health. Samsung Electronics Co. Smart application for Health tracking. Available at: https://goo.gl/e11p7g Last accessed: 19 December 2018

[4] Kaa Platform for Medical Internet of Things (IoT). Online: https://www.kaaproject.org/healthcare/. Last accessed: 19 December 2018.

[5] Rahmani, Amir M., Tuan Nguyen Gia, Behailu Negash, Arman Anzanpour, Iman Azimi, Mingzhe Jiang, and Pasi Liljeberg. "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach." Future Generation Computer Systems 78 (2018): 641-658.

[6] Moosavi, Sanaz Rahimi, Tuan Nguyen Gia, Ethiopia Nigussie, Amir M. Rahmani, Seppo Virtanen, Hannu Tenhunen, and Jouni Isoaho. "End-to-end security scheme for mobility enabled healthcare Internet of Things." Future Generation Computer Systems 64 (2016): 108-124.

[7] Aman, Muhammad Naveed, Kee Chaing Chua, and Biplab Sikdar. "Mutual authentication in IoT systems using physical unclonable functions." IEEE Internet of Things Journal 4, no. 5 (2017): 1327-1340.

[8] Chen, Ray, Jia Guo, and Fenye Bao. "Trust management for SOA-based IoT and its application to service composition." IEEE Transactions on Services Computing 9, no. 3 (2016): 482-495.

[9] Abowd, Gregory D., Anind K. Dey, Peter J. Brown, Nigel Davies, Mark Smith, and Pete Steggles. "Towards a better understanding of context and context-awareness." In International symposium on handheld and ubiquitous computing, pp. 304-307. Springer, Berlin, Heidelberg, 1999.

[10] Perera, Charith, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. "Context aware computing for the internet of things: A survey." IEEE communications surveys & tutorials 16, no. 1 (2014): 414-454.

[11] Dey, S. Sampalli and Q. Ye, "A Context-Adaptive Security Framework for Mobile Cloud Computing," 2015 11th International Conference on Mobile Ad-hoc and Sensor Networks (MSN), Shenzhen, 2015, pp. 89-95.

[12] S. Dey, S. Sampalli and Q. Ye, "A light-weight authentication scheme based on message digest and location for mobile cloud computing," 2014 IEEE 33rd International Performance Computing and Communications Conference (IPCCC), Austin, TX, 2014, pp. 1-2.

[13] M. Hamdi and H. Abie, "Game-based adaptive security in the Internet of Things for eHealth," 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, 2014, pp. 920-925.

[14] T. Bonaci and L. Bushnell, "Node capture games: a game theoretic approach to modeling and mitigating node capture attacks," International Conference on Decision and Game Theory for Security, Springer, 2011, pp. 44–55.

[15] D. Shen, G. Chen, E. Blasch and G. Tadda, "Adaptive Markov Game Theoretic Data Fusion Approach for Cyber Network Defense," MILCOM 2007 - IEEE Military Communications Conference, Orlando, FL, USA, 2007, pp. 1-7.

[16] H. Abie, "Adaptive security and trust management for autonomic message-oriented middleware," 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, Macau, 2009, pp. 810-817.

[17] Reijo, M, Savola., Habtamu, Abie., Markus Sihvonen., "Towards Metrics-Driven Adaptive Security Management in E-Health IoT Applications". Proceedings of the 7th International Conference on Body Area Networks, 2012, pp. 276- 281.

[18] W. Leister, M. Hamdi, H. Abie, S. Poslad, A. Torjusen, "An Evaluation Framework for Adaptive Security for the IoT in eHealth", International Journal on Advances in Security, 7(3&4), 2014, pp. 93-109.

[19] M.T. Gebrie and H. Abie, "Risk-based adaptive authentication for internet of things in smart home eHealth", In Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings (ECSA '17). ACM, New York, NY, USA, 2017, pp. 102-108.

[20] Y. Berhanu, H. Abie, M. Hamdi, "A testbed for adaptive security for IoT in eHealth". In Proceedings of the International Workshop on Adaptive Security (ASPI '13). ACM, New York, NY, USA., 2013.

[21] Evesti, A., and Ovasga, E.,EVESTI, A., AND OVASKA, E. "Ontology-based security adaptation at run-time. In Self-Adaptive and Self-Organizing Systems(SASO)",20104th IEEE International Conference on (2010), IEEE, pp. 204–212.

[22] G. Jagadamba , B. S. Babu, " Adaptive Security Schemes based on Context and Trust for Ubiquitous Computing Environment: A Comprehensive Survey", Indian Journal of Science and Technology, Volume 9, Issue 48, December 2016.

[23] H. Harb, A. William, O. A. El-Mohsen, "Context Aware Group Key Management Model for Internet of Things", In Proceedings of the Seventeenth International Conference on Networks, ICN 2018, Athens, Greece, April 22, 2018.

[24] H. Abie and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth", In Proceedings of the 7th International Conference on Body Area Networks (BodyNets '12). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium, 2012, pp. 269-275.

[25] A. Philip, C. Paul , C. Simon ,N. Julia , R. Mark , "System and Methods for Context-Aware and Situation-Aware Secure, Policy-Based Access Control for Computing Devices", United States Patent Application 20180157858, 2018.

[26] Li, Y. Bai, N. Zaman and V. C. M. Leung, "A Decentralized Trustworthy Context and QoS-Aware Service Discovery Framework for the Internet of Things," in IEEE Access, vol. 5, pp. 19154-19166, 2017.

[27] Message Queuing Telemetry Transport (MQTT). Online: http://mqtt.org/ Last accessed 19 December 2018.

[28] SPARQL Query Language for RDF. Online https://www.w3.org/TR/rdf-sparql-query/ Last accessed 19 December 2018.