Context-Aware Authentication for the Internet of Things

Kashif Habib, Wolfgang Leister
Norwegian Computing Center
Oslo, Norway
e-mail: Kashif.Sheikh@nr.no, Wolfgang.Leister@nr.no

Abstract— **Many traditional authentication and access control mechanisms do not use context-aware approach, i.e., those mechanisms do not incorporate context parameters while making authentication and authorisation decisions. The context unaware mechanisms can be inadequate for the Internet of Things due to its dynamic and heterogeneous environment. The context information can be used to reconfigure security mechanisms and adjust security parameters. The contextual information can be integrated into various security mechanisms such as authentication, access control, encryption, etc. The context-aware security is the dynamic adjustment of security policy based on the context. In this paper, we discuss the context-awareness techniques for authentication and access control mechanisms. We present the concepts of context, context- awareness, and context based security and highlight contextual attributes that can be used to support and enhance authentication and access control mechanisms for the Internet of Things.**

Keywords-Context; context-awareness; Internet of Things; authentication; access control; security.

I. INTRODUCTION

The Internet of Things (IoT) has gained much popularity in recent past due to integration of smartphones, tablets, and sensor networks into the Internet. The IoT envisions an environment in which sensors, recording devices, smartphones, tablets, and laptops are networked together and are actively monitoring changes in their surroundings. The contextual information can be monitored through various sources, such as sensors deployment, device status, and user's behaviour. The devices collaborate with each other to further facilitate human computer interactions or to provide the environmental information. The data provided by sensors or other recording devices are referred to as contextual data, since they contain information about the context in which each entity or user is located. Mobile devices are one of the common platforms to access resources in the IoT where contextual information can be considered dynamic. The contextual information can be about user's location and behaviour, current time, state of system resources, and state of network and security configurations.

The IoT faces some challenges such as security, privacy, trust, and context-awareness about the surrounding environment and about system state itself. The challenges are important because the IoT is dynamic in nature and does not have very well defined network boundaries. The IoT envisages dynamic and heterogeneous environment in which a context-aware based security can deal with the security problems. The ubiquitous applications can utilise the environmental information for decision making [1]. This means that the security mechanisms developed for the IoT can incorporate the contextual information while making a security decision. A security mechanism can be considered context-aware, if it can spot the event happening in surrounding environment. Context-awareness is an essential element for an authentication system while evaluating associated risks with a system [2].

A. Motivation and Contribution

Previously, we have developed an authentication framework based on biometric modalities and wireless device radio fingerprinting [3]. Our framework ensures that the received data at remote medical center belongs to correct patient and identifies the fabricated data. Incorporating context awareness and adaptive security in our framework are challenges because a non-match between stored and given templates always can not be treated as a threat to the system, rather there can be situations where environmental or system's context can assist us in decision making. Adaptive security can make template matching more flexible and we can adjust security level instead of blocking transmission during no-match due to the changed context. In this paper, we discuss and elaborate context, context-awareness, context-aware security, and context-aware authentication concepts for the IoT. While discussing the above mentioned concepts, our main focus is towards context-aware approaches for authentication and access control mechanisms and we classify the mechanisms according to context modelling approaches.

The paper is organized as follow: in Section II, we introduce context and context-awareness concepts. In Section III, we review context-aware security paradigm. The context-aware security models, frameworks, protocols, and prototypes for authentication and access control mechanisms are highlighted in Section IV. Section V contains some discussions and Section VI concludes the paper followed by future work.

II. CONTEXT AND CONTEXT-AWARENESS

The term context-aware can be defined for different application areas and for different purposes. There are several definitions of context-awareness in the literature [4]. According to Schilit and Theimer [5], "a system is context-aware if it can provide context relevant information and services to users and applications from the set of context types, such as location, identification of nearby people, objects and changes to those objects." Soon after them, Schilit et al. [6] also de-

 ISBN: 978-1-61208-405-3

fined a context-aware system. According to them, "a system is context-aware if it can adapt itself to the context." Afterwards, many people defined context-aware systems in a similar way. For example, according to Dey [7], "a system can be context-aware if it uses context to provide relevant information and, or services to the user, where relevancy depends on users' task." According to Ryan et al. [8], "a system is context-aware if it has the ability to detect and sense, interpret and respond to aspects of a user's local environment and to the computing devices themselves." Dey and Abowd [9] define context as "any information that can be used to characterise the situation of an entity that is considered relevant to the interaction between a user and an application". According to Krish [10] "context is a highly structured amalgam of information, physical and conceptual resources that go beyond the simple facts of who or what is where and when to include the state of digital resources, people concepts and mental state, task state, social relations, and the local work culture, to name a few ingredients".

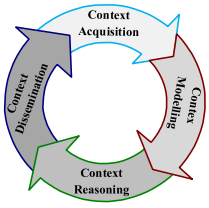

Figure 1. Context life cycle

As depicted in Figure 1, a context-aware system follows the life cycle process to deliver contextual information. Gomez and Wrona [11] identified context information discovery, context information acquisition, and context information reasoning as main steps in a life cycle of context-aware system. Bernardos et al. [12] identified context acquisition, information processing, and reasoning and decision as main phases in a typical context management system. After reviewing the life cycles of context-aware system, Perera et al. [13] derived context acquisition, context modelling, context reasoning, and context dissemination as four phases in a typical context management system.

1) Context information acquisition:

A context-aware system collects contextual information from the discovered context information providers and stores it in a context information repository for further reasoning. The context acquisition can also follow pull and push modes. The pull mode allows context-aware system to request contextual information, whereas in case of push mode, context information providers push context information to the context-aware system.

2) Context information modelling:

The contextual information is processed in terms of attributes, characteristics, relationships, quality-of context attributes and the queries for synchronous context requests. Afterwards, the new context information is organised and added to the existing contextual information repository for use.

3) Context information reasoning:

A reasoning mechanisms facilitate applications to utilise the available context information. In order to establish a reasoning mechanism, a single piece of context information or a collection of such information can be used.

4) Context information dissemination:

The applications requiring contextual information use context dissemination to acquire context. The context is disseminated using query and subscription methods. In a query method, the context management system can use that query to produce results. In a subscription method, the applications subscribe the requirements with a context management system that provides the results upon detecting an event.

TABLE I. SUMMARY OF CONTEXT TYPES

Context type	Captured contextual information	Available sensors and technologies
Physical context	Light, temperature, noise, humidity level, traffic conditions.	Photodiodes; biosensors; thermometer; ultraviolet sensors.
Computing context	Network capacity; connectivity; bandwidth; costs of computing and communication; resources such as printers, and workstations; available processors and devices accessible for user input and display.	Touch sensors implemented in mobile devices; microphones; system log; user behaviour monitoring; device log, various environmental sensors.
User context	User location, collection of nearby people, user profiles, social situation.	Active badge system; GPS; camera; mercury switches; GSM; motion detectors; accelerometers.

The three important aspects of context are: where you are, whom you are with, and what resources are nearby [14]. Based on these aspects, context can be divided into three parts: user context, computing context, and physical context. Table I provides a summary of available sensors and technologies to capture contextual information for each context type.

TABLE II. SUMMARY OF CONTEXT ATTRIBUTES

Attributes	Description
Context categories	Conceptual; measurable; static; dynamic; continuous; discrete; internal; external; material; social; physical; virtual; real-time; unreal-time; natural; technology; social; location; identity; time; activity
Context-awareness approaches	*Active context-awareness:* Contextual changes are discovered by detecting changes in the application's behaviour. *Passive context-awareness:* Applications present the updated context to a user.
Context learning approaches	*Sensed context:* Environment information; user's physical information; user's interaction habits and interactive historical records. *Derived context:* Computed on the go; explicit context; user preferences.
Context modelling	Key-value; mark up scheme; graphical; object oriented; logical; ontology.

Table II provides a summary of context attributes. Context is classified according to context categories, context-awareness approaches, context learning approaches, and context modelling approaches.

 ISBN: 978-1-61208-405-3

III. CONTEXT-AWARE SECURITY

Many existing computer networks comply with allow and deny based access control policies. Allow means granting access when the user or device credential matches with pre-stored credentials and deny means blocking access when the user or device credential do not match with pre-stored credentials. This type of system can be considered static in nature because it does not take into consideration other factors such as, contextual information from the user or device environment while making allow and deny decisions. But the IoT has a dynamic environment, where flexible security policies using contextual information can potentially increase the effectiveness of security decisions.

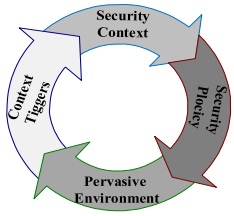

Figure 2. Context-aware security

The security context is defined by Kouadri and Brézillon [15] as: "a set of information collected from the user's environment and the application environment and that is relevant to the security infrastructure of both the user and the application." Brézillon and Mostéfaoui [16] define the security context as a situation where a security solution considers a set of information while making a specific security decision. For example, while detecting an intrusion during communication, security mechanism may adapt to strong authentication method. As depicted in Figure 2, initially the pervasive computing environment is controlled by some security policy depending upon the initial context at that time [16] [17].

Context triggers refer the dynamic changes in the environment with the passage of time. Security context refers this new context that is to be considered while deploying new security actions as a result of the change. A security policy indicates the rules and regulations that govern who has the access and who doesn't in each type of situation. Thus, the security policy should be flexible enough to accommodate changing contexts.

Strang and Linnhoff-popien [18] surveyed the relevant approaches to modelling context. The authors reviewed various approaches, classified relative to their core elements, and evaluated with respect to their appropriateness for ubiquitous computing. Many context-aware applications based on various context models have been developed in past for a variety of application domains. The existing approaches to context information modelling are sorted into six categories [18] [19] [20], which are based on the data structures used for lying out and exchanging context data in the respective system. Table III summarises the available security context modelling approaches.

Halunen and Evesti [21] presented some possibilities of utilising context-aware systems in adaptive user authentication settings. They suggested to first use the context information to control an adaptive security system and then linked to the authentication scheme via tags.

TABLE III. SUMMARY OF SECURITY CONTEXT MODELING

Key-value modelling: *Description:* simple key-value pairs to define the list of attributes and their values describing context; information used by context-aware applications. *Strength:* easy to manage; simple data structure to depict the contextual information. *Weakness:* limited capabilities in: (i) capturing a variety of context types; (ii) capturing contextual relationships; (iii) dependencies, timeliness, and quality of context information; (iv) sophisticated structuring for enabling efficient context retrieval algorithms.
Mark-up scheme modelling: *Description:* it uses a variety of mark-up languages; hierarchical data structure consisting of mark-up tags with attributes and content; the content of the mark up tags is usually defined by other mark-up tags. *Strength:* can sort the context information by category, priority, and runtime process. *Weakness:* Limited capabilities in: (i) allowing consistency checking; (ii) supporting reasoning on context, on context uncertainty and on higher context abstractions.
Graphical modelling: *Description:* obtained through transformation algorithms; graph data structures and richer data types, e.g., unified modelling language and object role modelling. *Strength:* generic; hierarchically structured allowing the association of a context with an appropriate action. *Weakness:* lack of support for distributed context model; handling incompleteness; lack of formalism for on line automated access.
Object oriented modelling: *Description:* uses object oriented languages to design the dynamic property of the context; the context information is used as a method applied to an object; context processing details are encapsulated on an object level; access to contextual information is provided through specified interfaces only. *Strength:* favours the trust inside the network; partial validation but often not very formal; reuse can be supported through inheritance and composition. *Weakness:* does not provide the support for interoperability; handling incompleteness; has a flat information model.
Logical modelling: *Description:* the context is defined with facts, predictions or roles; a goal is to form new expressions or facts from previous ones; a logic defines the conditions in which a concluding expression or fact may be derived. *Strength:* formalism; structuring. *Weakness:* uncertainties; time variations; validation issues.
Ontology modelling: *Description:* represents a concept group in a given domain, and the relationship between the different concepts; depicts a domain with a graph of concepts; contextual relationships may be hierarchical or semantic. *Strength:* strong regarding the distributed composition requirement; partial validation is possible; comprehensive set of validation tools available. *Weakness:* uncertainties in handling, scalability issues in searching large data volumes.

The different approaches to model security context possess some weaknesses as mentioned in Table III. For example, key-value modelling based approach possesses weak-

nesses such as, distributed composition of contextual data, partial validation, information quality, incompleteness, and formalism. Graphical modelling approach also lacks in terms of distributed composition of contextual data. Mark-up scheme and logic based modelling approach can be considered weak in terms of handling incompleteness and ambiguity in contextual data. Object oriented model usually require strong distributed composition requirements which are difficult to manage for the devices in the IoT due to limited resources.

IV. RELATED WORK

The context-awareness for authentication and access control mechanisms has been an active research field among researchers. In this section, we classify the context-aware techniques proposed in the existing literature according to context modelling approaches discussed earlier.

1) Key-value modelling:

Hayashi et al. [22] introduced context-aware scalable authentication using multiple passive factors by modulating active factors to authenticate users. The authors proposed a generic probabilistic framework to select appropriate active authentication factors, given a set of passive authentication factors. They developed prototypes, and investigated the feasibility and effectiveness of their proposed framework.

Context-aware mobile biometric authentication based on support vector machines is proposed by Witte et al. [23]. Based on the contextual information measured from the environment, the authors constructed subject-specific context models in order to train support vector machine. The authors demonstrated the feasibility of the proposed architecture by developing a mobile application for data collection purposes.

Said et al. [24] presented a context-aware security controller and proposed to integrate it in the long term evolution/evolved packet system access. The authors motivated the integration of a context-aware security controller to minimize the overall security cost. They showed that the controller activates security mechanisms according to the contextual information such as the application type and the device capabilities.

2) Mark-up scheme modelling:

Goel et al. [25] described an authentication framework for a context-aware environment. In order to support role-based and location-based access control, the authors used a combination of a user's context, authentication policies and light weight tagging. The framework has a provision for extension to support other contextual information from available resources, environment, and the users who interact with that environment.

Hu and Weaver [26] presented a dynamic, context-aware security infrastructure for healthcare applications. The access control model extends the role based access control mechanism by associating access permissions with context-related constraints. They described the capability of their model by showing authorization decisions approach based upon context information in addition to roles.

A mechanism for modelling complex and interwoven sets of context-information by extending ambient calculus with new constructs and capabilities is presented by Kjægaard and Pedersen [27]. According to the authors, the calculus is a step in the direction of making formal methods applicable in the area of pervasive computing. In particular, the authors identified the key area of the expressiveness of formal models of context-awareness which are represented as hierarchical and independent sets of information.

3) Graphical modelling:

Feng et al. [28] incorporated contextual information to improve user authentication by presenting a touch based identity protection service. In order to authenticate a user on continuous basis, they analysed real life touch data as well as underlying contextual information.

Lenzini [29] presented trust-based and context-aware authentication in a software architecture for context and proximity-aware services. The author described context management architecture for context-aware services. The software based architecture collects, arranges, and elaborates high-level contextual information from a sensor network. The author used contextual information to distinguish among different identities, and to evaluate to which extent they are authentic.

Bandinelli et al. [30] presented a context-aware security framework for next generation mobile networks. The authors introduced a context-aware security framework for addressing the problems of end-to-end security on behalf of end-users in a next generation network scenario. Their security framework uses contextual graphs to define security policies encompassing actions at different layers of communication systems while adapting to changing context.

4) Object oriented modelling:

Badram et al. [31] presented context-aware user authentication, supporting proximity-based login in pervasive computing environment. The authors introduced a concept of proximity-based user authentication in a pervasive computing environment. User identification is performed through a Java smart card and a context-aware system.

5) Logical modelling:

Zhang et al. [32] presented the context-aware access control model for pervasive applications using dynamic role based access control scheme. Based on the context information, the operation of the model extends the role based access control model to dynamically adjust the role assignments, and permission assignments. However, their access control scheme may not be sufficient alone until it is combined with feasible authentication mechanisms to secure pervasive applications.

To improve existing network security protocols in an Intranet environment, Wullems et al. [33] introduced context-aware authorization architecture. The proposed architecture is an extension to role based access control mechanism facilitating context-aware access control policy. They described the implementation of the architecture using dynamic context services and also presented the description of an application utilising their proposed architecture.

An adaptive access control model for medical data in body and wireless area network is designed and developed by Maw et al. [34]. They evaluated the framework using medical scenario in which they included a user behaviour

 ISBN: 978-1-61208-405-3

trust module along with the access control module. They concluded that the overriding policy is useful to handle unanticipated situations and showed that by incorporating user behaviour into access control model, one can make better security decisions.

Malek et al. [35] presented a framework for context-aware authentication services in context-aware computing environments. The proposed framework is capable of enabling the users to take initiatives in the context-aware computing environments depending on their desired confidence level. To establish trust and to share secrets between parties, the context-aware authentication service uses context-data.

Hulsebosch et al. [36] described the theoretical background for a context-sensitive adaptation of authentication. The authors designed and validated the system to adaptively authenticate a user on the basis of the location of his sensed identity tokens. The authors argued that authentication and access control can be made less intrusive, more intelligent, and able to adapt to the rapidly changing contexts of the environment.

Brosso et al. [37] presented a continuous authentication system based on user behaviour analysis. The system utilises environmental context information, user' behaviour analysis, and neuro-fuzzy logic. The authors verified the system with tests and simulations to authenticate a person's identity using behaviour analysis and trust restriction. They used contextual information to establish evidence of user behaviour. The trust levels were decided based upon user behaviour.

6) Ontology modelling:

To provide a security framework suitable for people with disabilities, Mhamed et al. [38] suggested using various contextual data monitored through sensors. The approach shows how to model trust and access control based on user behaviour and capabilities that can be extracted from the monitored data through sensors. The proposed access control model is based on the semantic web technologies.

Wrona and Gomez [11] investigated different aspects of security related to context information. According to them, security challenges in context-aware systems include integrity, confidentiality, availability of context information, and end user's privacy. Trustworthiness of context information is also an important element, which a context information requester can put in the delivered context information.

V. DISCUSSION

Understanding the contextual information is an important element for the IoT. A context-aware system can be considered different from traditional systems because of their capabilities to capture and incorporate environmental factors into decision making process. Particularly, in case of the IoT where device and user attributes such as, location, time, and behaviour can change rapidly, it may be very important for security mechanisms to react based on the changing parameters and adapt accordingly.

Authentication and access control are important security services for the IoT that are needed to check the identity of users and to decide which resources they can access to. The existing authentication mechanisms that are developed for traditional computer network environments are mostly context unaware, and usually do not incorporate contextual information while authenticating a user and a device. But due to dynamic environment and changed context, the threat profile can vary and static authentication mechanism may not be sufficient enough to continue securing a system. Contextual information can help authentication system to know user state and make better identification decisions. The strength of an authentication mechanism can be improved if we broaden our authentication scope beyond the identification of user credentials. Rather, if we can also incorporate the context information, such as user location, user state, and surrounding environmental state, along with user credentials.

While adding context into authentication and access control mechanisms, sometimes incomplete or imprecise context can lead to false positives and false negatives. For example, user and environmental context may be inaccurately determined or context determination may be affected by environmental conditions, etc. Thus, if context acquisition is performed wrongly, it can possibly generate false positives and false negatives. However, if context acquisition and reasoning are performed correctly, and proper context composition techniques are used, then adding context into security decision can reduce the rate of false positives.

VI. CONCLUSION AND FUTURE WORK

Although, developing authentication and access control mechanisms has been an active research areas among researchers, but mostly the existing mechanisms work on the principles of user credential based approach. Context-awareness has a tendency to enhance the effectiveness of those mechanisms by incorporating contextual data into a decision making process. In this paper, we highlighted the necessary concepts of context, context awareness, and context based security. In addition, the approaches proposed in the existing literature, regarding incorporating context-awareness into authentication and access control mechanisms in the IoT are presented.

Previously, we have developed an authentication framework based on biometric and radio fingerprinting for the IoT in eHealth. In future, the work in this paper will be used as a basis for the development of context-aware authentication mechanisms for the IoT in eHealth. Precisely, we will carry out context-awareness modelling for our earlier developed framework.

ACKNOWLEDGMENT

The work presented here has been carried out in the research project ASSET – Adaptive Security for Smart Internet of Things in eHealth (2012–2015) funded by The Research Council of Norway.

REFERENCES

[1] A-C. Pierre, "A dynamic trust-based context-aware secure authentication framework for pervasive computing environments," PhD thesis, Computer Science, Institut National des Télécommunications, France, 2010.

[2] RSA Risk-based Authentication, white paper, November 2013, pp. 1-4.

 ISBN: 978-1-61208-405-3

[3] K. Habib, A. Torjusen, and W. Leister, “A Novel Authentication Framework Based on Biometric and Radio Fingerprinting for the IoT in eHealth,” In proceedings of SMART 2014, July 20 - 24, 2014, pp. 32-37.

[4] S. Poslad, “Ubiquitous Computing: Smart Devices, Environments and Interactions,” Wiley Publishing, 2009.

[5] B. Schilit and M. Theimer, “Disseminating active map information to mobile hosts,” IEEE Networks, 8(5): , pp. 22-32, 1994.

[6] B. Schilit, N. Adams, and R. Want, “Context aware computing applications,” In Proceeding of 1st International Workshop on Mobile Computing Systems and Applications, 1995, pp. 85-90.

[7] A. K. Dey, “Providing Architectural Support for Building Context Aware Applications,” PhD thesis, Computer Science, Georgia Institute of Technology, Atlanta, November, 2000.

[8] N. Ryan J. Pascoe, and D. Morse, “Enhanced reality fieldwork: the context aware archaeological assistant,” In V. Gaffney, M. van Leusen, and S. Exxon (eds) Computer Applications in Archaeology, British Archaeological Reports, 1997.

[9] A. K. Dey and G. D. Abowd, “Towards a better understanding of context and context awareness,” In Proceedings of the (HUC '99), 1999, pp. 304-307.

[10] D. Kirsh, “The Context of Work, Human-Computer Interaction,” vol. 16, 2001, pp. 305-322.

[11] K. Wrona and L. Gomez, “Context-aware security and secure context-awareness in ubiquitous computing environments,” XXI Autumn Meeting of Polish Information Processing Society, 2004, pp.255-265.

[12] A. Bernardos, P. Tarrio, and J. Casar, “A data fusion framework for context-aware mobile services,” IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems, 2008, pp. 606 –613.

[13] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, “Context aware computing for the internet of things: A survey,” IEEE, 16, 2014, pp. 414-454.

[14] W. Liu X. Li, and D. Huang, “A survey on context awareness,” International Conference on Computer Science and Service System (CSSS), 27-29 June 2011, pp. 144-147.

[15] G. K. Mostéfaoui and P. Brézillon, “Modeling Context-Based Security Policies with Contextual Graphs,” In Proceedings of (PERCOMW '04). IEEE Computer Society, 2004, pp. 28-32.

[16] P. Brezillon and G. K. Mostefaoui, “Context-based security policies: a new modelling approach,” Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, March 2004, pp.154,158.

[17] P. Shetty and S. W. Loke, “Context-Based Security (and Safety) Meta-Policies for Pervasive Computing Environments: the case of Smart Homes,” In the Workshop on Context and Safety at Context, 2005, pp. 1-14.

[18] T. Strang and C. Linnhoff-Popien, “A Context Modelling Survey,” In Workshop on Advanced Context Modelling, Reasoning and Management, UbiComp 2004, pp. 1-8.

[19] S. Vuppala et al., “uBiquitous, secUre inTernet-of-things with Location and contEx-awaReness,” BUTLER project, D2.1 - Requirements, Specifications and Security Technologies for IoT Context-Aware Networks, October 2012, pp. 1-171.

[20] C. Bettini et al., “A survey of context modelling and reasoning techniques,” Pervasive Mob. Comput. 6, (2), April 2010, pp. 161-180,.

[21] K. Halunen and A. Evesti, “Context-Aware Systems and Adaptive User Authentication,” Evolving Ambient Intelligence, Springer International publishing, 413, 2013, pp.240-251.

[22] E. Hayashi, S. Das, S. Amini, J. Hong, and I. Oakley, “CASA: context-aware scalable authentication,” In Proceedings of (SOUPS '13). ACM, Article 3, 2013, pp. 1-10.

[23] H. Witte, C. Rathgeb, and C. Busch, “Context-Aware Mobile Biometric Authentication based on Support Vector Machines," In proceedings of the (EST), 2013, pp.29-32.

[24] S. B. H. Said, K. Guillouard, and J-M. Bonnin, “On the benefit of context-awareness for security mechanisms in LTE/EPS networks,” In proceedings of the (PIMRC), 2013, pp. 2414-2428.

[25] D. Goel, E. Kher, S. Joag, V. Mujumdar, M. Griss, and A. Dey, “Context-Aware Authentication Framework Mobile Computing, Applications, and Services,” Springer Berlin Heidelberg, 35, 2010, pp. 26-41.

[26] J. Hu and A. C. Weaver, “A Dynamic, Context-Aware Security Infrastructure for Distributed Healthcare Applications,” In Proceedings of the (PSPT), 2004, pp. 1-8.

[27] M. B. Kjægaard and J. Bunde-Pedersen, “Towards a Formal Model of Context Awareness,” In proceedings of the (CTSB), 2006, pp. 1-8.

[28] T. Feng, J. Yang, Z. Yan, E. Tapia, and W. Shi, “TIPS: context-aware implicit user identification using touch screen in uncontrolled environments,” In Proceedings of the (HotMobile '14), ACM, Article 9, 2014, pp. 1-6.

[29] G. Lenzini, “Trust-Based and Context-Aware Authentication in a Software Architecture for Context and Proximity-Aware Services Architecting Dependable Systems” VI, Springer Berlin Heidelberg, 5825, 2009, pp. 284-307.

[30] M. Bandinelli, F. Paganelli, G. Vannuccini, and D. Giuli, “A Context-Aware Security Framework for Next Generation Mobile Networks Security and Privacy in Mobile Information and Communication Systems,” Springer Berlin Heidelberg, 17, 2009, pp. 134-147.

[31] J. Bardram, R. Kjær, and M. Pedersen, “Context-Aware User Authentication- Supporting Proximity-Based Login in Pervasive Computing,” Ubiquitous Computing, Springer Berlin Heidelberg, 2864, 2003, pp.107-123.

[32] G. Zhang and M. Parashar, “Context-aware dynamic access control for pervasive applications,” Proceedings of the Communication Networks and Distributed Systems Modelling and Simulation Conference, 2004, pp. 21-30.

[33] C. Wullems, M. Looi, and A. Clark, “Towards context-aware security: an authorization architecture for intranet environments,” In proceedings of the (PERCOMW’04), March 2004, pp.132-137.

[34] H. A. Maw, H. Xiao, and B. Christianson, “An adaptive access control model for medical data in Wireless Sensor Networks," IEEE 15th International Conference on e-Health Networking, Applications & Services, 2013, pp.303-309.

[35] B. Malek, A. Miri, and A. Karmouch, “A framework for context-aware authentication," 4th International Conference on Intelligent Environments, IET , 21-22 July 2008, pp.1-8.

[36] R. Hulsebosch, M. Bargh, G. Lenzini, P. Ebben, and S. Iacob, “Context Sensitive Adaptive Authentication,” smart sensing and context,” Springer Berlin Heidelberg, 4793, 2007, pp. 93-109.

[37] I. Brosso, A. La Neve, G. Bressan, and W. V. Ruggiero, “A Continuous Authentication System Based on User Behavior Analysis,” In proceedings of the (ARES '10), Feb. 2010, pp. 380-385.

[38] A. Mhamed, M. Zerkouk, A. El Husseini, B. Messabih, and B. El Hassan, “Towards a Context Aware Modelling of Trust and Access Control Based on the User Behaviour and Capabilities Inclusive Society, Health and Wellbeing in the Community, and Care at Home,” Springer Berlin Heidelberg, 7910, 2013, pp. 69-76.

 ISBN: 978-1-61208-405-3