Providing Context-Aware Security for IoT Environments Through Context Sharing Feature

Raut Tejas, Waghmare Swapnil , Shelke Onkar, Dange Shubham, Kharat Pratik.
Vidya Pratishthan's Kamalnayan Bajaj Institute of Engineering and Technology, Baramati.

Abstract

Security and privacy in Internet of Things (IoT) environments is a real issue. Traditional security mechanisms use a non-aware approach, in which static parameters are used to provide secure decisions. IoT is a dynamic environment.Thus a non-static approach for security provision becomes mandatory. Context-aware security appears as a viable choice for this kind of processing. It uses the context information of IoT environments thus pro viding dynamic security. When together with context sharing feature, it can add new dimensions to the IoT security. Context sharing allows the use of domain context infor mation to the security provision. This project defines an Edge-Centric Context Sharing Architecture that provides context aware security by using shared context information.

Keywords:
Context-aware,IoT,Authentication,
Automation.

Introduction

The Internet of Things (IoT) computing paradigm embeds mobile networking and in formation pro- cessing capability into a wide array of gadgets and everyday items As miniaturization continues and computing capacity still increases, IoT devices are be coming more powerful. There is a common sense that IoT devices generate many data.

The context-aware computing helps in interpret and understand these data in a proper way, producing context information.The context information is considered any high-level information, sometimes semantic, that can be used to characterize the situation of an entity (e.g., person, place, or computing device). In most cases, the context information is stored individually by the systems. Context sharing is a feature that allows the sys tems to share context information to heterogeneous entities understand different context information across application domains.

The IoT is a dynamic environment in which en tities are in constant change. In light of this, the traditional static security mechanisms become inadequate.There is a need for platforms that provide context-aware security to integrate different IoT verticals. In this sense, the main contributions are: - A vision of both context-aware security and context sharing technologies, and how the shared context can be used to provide security.

Privacy in IoT is a prime security issue that needs full attention from researchers for better smart home concept . There is a need to propose protocols and management frameworks to handle privacy in IoT. IoT has become an integral part in various appli cations like remote patient monitoring, energy consumption control, traffic control, and Smart Home appliances system. In all of these applications, users require protection of personal information which is related to their movement, habits, and interactions with other people.

One thing to keep in mind when evaluating security needs is that the IoT is still very much a work in progress. Many things are connected to the Internet now, and we will see an increase in this and the advent of contextual data sharing and autonomous machine actions based on that information, So the security to anything which means to have the privacy is the must.we choosed the topic because we can feel the threat that can be caused to the smart home functioning if any other unauthorised member accesses the automation system.keeping the term privacy in mind we need to deal with the security issue of IoT based smart home system

In smart home system privacy being the main issue makes us to think of providing the security .Apart from privacy the other concerns that that can harm the ideal smart home system are actions from the Attackers (unauthorised user).so for se cure routing and forwarding of data, we deal with security issue to ensure the smooth functioning of IoT based Smart Home environment

Related Work

In this section, we have discussed some papers in reference to IoT Automation .

A.Context Aware Computing for The Internet of Things Charith Perera , Arkady Zaslavsky, Peter Christen and Dimitrios Georgakopoulos reserched for the context aware computing and provided the following information. As we are moving towards the Internet of Things (IoT), the number of sensors deployed around the world is growing at a rapid pace. Market research has shown a significant growth of sensor deployments over the past decade and has predicted

a significant increment of the growth rate in the future. These sensors continuously generate enormous amounts of data. However, in order to add value to raw sensor data we need to understand it. Collection, modelling, reasoning, and distribution of context in relation to sensor data plays critical role in this challenge. Context-aware computing has proven to be successful in understanding sensor data. In this paper, we survey context awareness from an IoT perspective. We present the necessary background by introducing the IoT paradigm and context-aware fundamentals at the beginning. Then we provide an in-depth analysis of context life cycle. We evaluate a subset of projects (50) which represent the majority of research and commercial solutions proposed in the field of context-aware computing conducted over the last decade (2001-2011) based on our own taxonomy. Finally, based on our evaluation, we highlight the lessons to be learnt from the past and some possible directions for future research.

B.Context Interoperability for IoT through an Edge-centric Context Sharing Archi tecture. The adoption of the Internet of Things (IoT) demands advances to cope with the large heterogeneity of IoT entities (i.e., systems, applications, and devices). Context informa tion is an essential characteristic of these entities, which can store relevant details about their environments and related events. However, with the integration of different IoT vertical domains, providing isolated context is no longer enough. Sharing the context in formation is mandatory to have interoperability. Edge computing emerges as a promising approach to help in filling the context sharing gap by minimizing information overhead and reducing network latency. In this sense, this paper defines an Edge-centric Context Sharing Architecture able to make context sharing based on edge-to-fog approach. We also discuss the requirements for context sharing and the related work in the area to make clear the novelty of the architecture. .

C.Context-Aware Service Provisioning via Agentized and Reconfigurable Multimodel Cooperation for Real-Life IoT-Enabled Smart Home Systems. Ching-Hu lu worked on the CaSP system. For the upcoming Internet of Things (IoT) enabled era, context-aware service provisioning (CaSP) can be realized by first analyz ing new input data, followed by inferring contexts from the input data, and providing new services based on the inferred contexts. Over time, further new contextual models will also be incorporated into CaSP due to growing data collected by existing or new IoT devices. Furthermore, these contextual models require ongoing adaptation because a real-life environment is dynamic in nature. It becomes more challenging to maintain and adapt these ever-increasing contextual models as the system evolves. To address these concerns, this paper proposes a CaSP infrastructure along with an agentized and reconfigurable design to improve system adaptability and extensibility. The proposed middleware-enhanced CaSP infrastructure can keep as much previously learned knowl edge as possible to share among all integrated components. This design reduces the overhead from integrating and adapting multiple contextual models in response to in evitable uncertainties in a dynamically changing IoT-enabled smart home environment. Our agentized design generalizes the scheme of all smart components integrated with the CaSP infrastructure, thus facilitating reciprocal cooperation among all initially in dependent components. The CaSP infrastructure can facilitate multilevel rather than single-level information reuse via message queues residing in the middleware.

D.Context-as-a-Service Platform: Exchange and Share Context in an IoT Ecosystem. The paper proposes the context as a service .Context-awareness has become a hot trend in the last decade, especially in the realm of the Internet of Things (IoT). As IoT evolves, the need for accessing contextual information in real time is becoming a crucial factor for the improvement of IoT services. According to the widely accepted definition of context proposed by Dey, context is "any information that can be used to characterise the situation of an entity, where an entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves" [1]. Since early 1990's, a large body of research has been conducted on context/context-awareness in pervasive computing to enable in telligent adaptation of applications allowing them to perform their tasks in an efficient, proactive and autonomous manner [2], according to the context of its users or other involved entities.

Methodology

Home Automation System gains popularity due to communication technology advance ment. Smart home is one of the Internet of Things (IoT) applications that facilitates the control of home appliances over the Internet using automation system. This paper proposes a low-cost Wi-Fi based automation system for Smart Home in order to monitor and control home appliances remotely using Android-based application. In all of these applications, users require protection of personal information which is related to their movement, habits, and interactions with other people.

In smart home system privacy be ing the main issue makes us to work on providing the security.Thus making the smart home automation system safe .

Scope And Constraints

Future scope for the home automation systems involves making homes even smarter. Standardization enables smart homes that can control appliances, lighting, environment, energy management and security as well as the expandability to connect with other networks.The concept of home automation aims to bring the control of opertaion of your everyday home elec trical appliances to the tip of your finger, thus giving user adordable lightning solutions, better energy conservation with optimum use of energy.

The home automation systems are used for controlling the indoor and outdoor lights, heat, ventilation, air conditioning in the house, to look or open the doors and gates, to control electrical and electronic appliances and so on using various control systems with appropriate sensors.

constraints:
1.Dependent in internet cannot work without internet.

2.Professionals are needed if there is any problem in the system.

Acknowledgements

We would like to express my special thanks of gratitude to our principal Dr. R. S. Bichkar, Head of Dept. Dr. S. A. Takale mam as well as to our supervisor of this project, Mr. S.A.Shinde ,His willingness to motivate us contributed tremendously to our project. We are highly indebted to VPKBIET for their guidance and constant supervision as well as for providing necessary information regarding the project and also for their support in completing the project, who gave us the golden opportunity to do this wonderful project on the topic Providing Context-Aware Security for IoT Environments Through Context Sharing Feature, which also helped us in doing a lot of Research and we came across so many new things we are really thankful to them. Secondly we would also like to thank our parents and friends who helped us a lot in finalizing this project within the limited time frame and also to all colleagues for sharing the literature and invaluable assistance.

References

[1] Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010..

[2] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware com puting for the internet of things: A survey," Communications Surveys Tutorials, IEEE, vol. 16, no. 1, pp. 414–454, 2014.

[3] J. Al-Muhtadi, A. Ranganathan, R. Campbell, and M. D. Mickunas, "Cerberus: a context-aware security scheme for smart spaces," in Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003.

[4] P. Brezillon and G. K. Mostefaoui, "Context-based security policies: a new modeling approach," in IEEE Annual Conference on Pervasive Computing and Communica tions Workshops, 2004.

[5] Ching-Hu lu,Context-Aware Service Provisioning via Agentized and Reconfigurable MultimodelCooperation for Real-Life IoT-Enabled Smart Home Systems.

[6] E. Hayashi, S. Das, S. Amini, J. Hong, and I. Oakley, "Casa: Contextaware scalable authentication," in Proceedings of the Ninth Symposium on Usable Privacy and Security, ser. SOUPS '13.