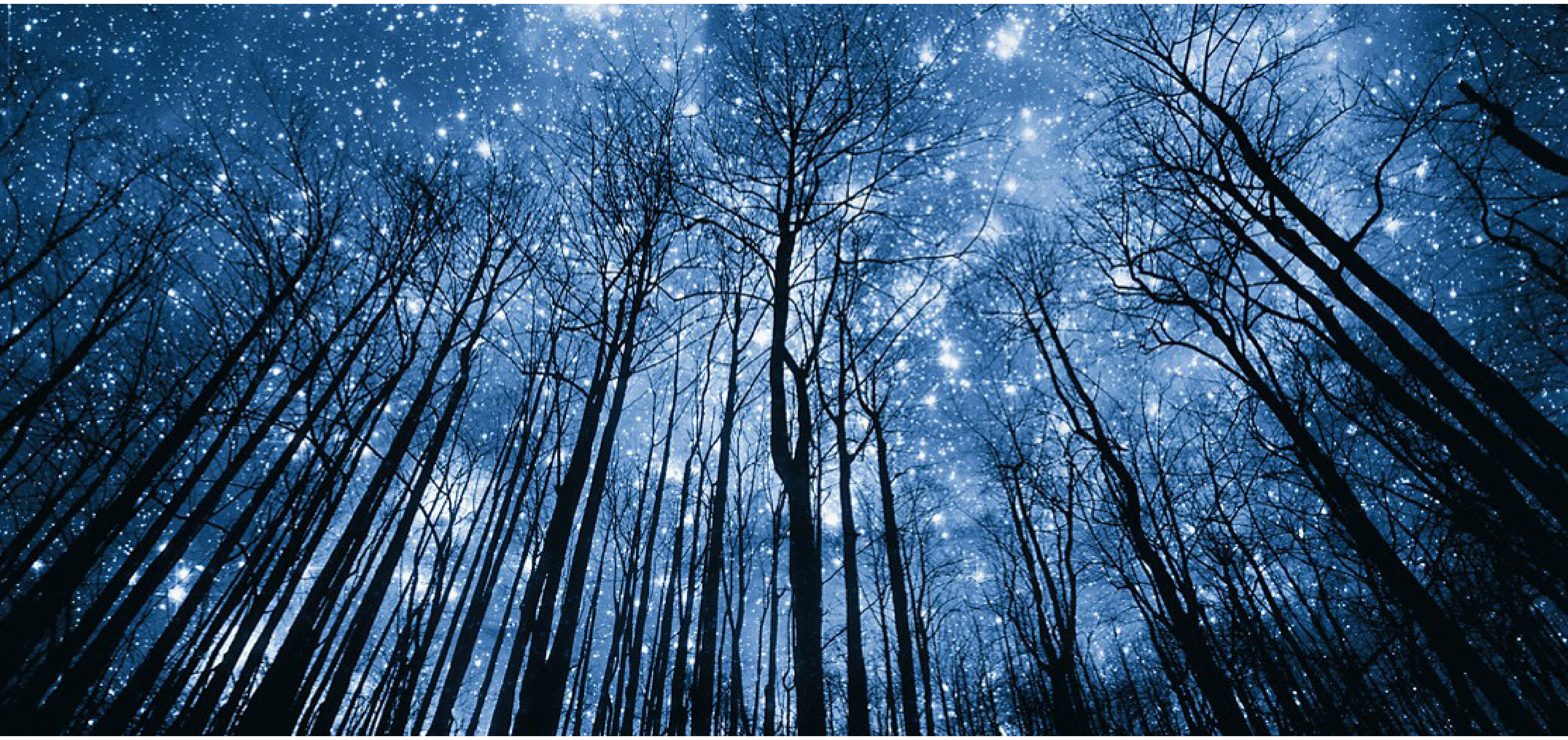
UBIQUITOUS COMPUTING



Ashwani Kumar
Customer Experience Engineer, Data Protection
Dell Technologies
Ashwani_kumar16@dell.com

Honey S
Customer Experience Engineer, Data Protection
Dell Technologies
Honey_s@dell.com

Vibha Choudhary
Vibha.choudhary949@gmail.com

Knowledge Sharing Article

The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across multiple technologies and products.

From Associate, entry-level courses to Expert-level, experience-based exams, all professionals in or looking to begin a career in IT benefit from industry-leading training and certification paths from one of the world’s most trusted technology partners.

Proven Professional certifications include:

- Cloud
- Converged/Hyperconverged Infrastructure
- Data Protection
- Data Science
- Networking
- Security
- Servers
- Storage
- Enterprise Architect

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Learn more at www.dell.com/certification

Table of Contents

Disclaimer: The views, processes or methodologies published in this article are those of the authors. They do not necessarily reflect Dell Technologies' views, processes or methodologies.

Introduction

Ubicomp is transitioning from conventional computing where a user interacts with a single computing device at a time which is connected to the Internet, to Ubiquitous Computing where all devices could be connected to the Internet, enabling work to be performed collectively for greater advancement. This evolving technology is eliminating the time and position barrier and also becoming intelligent so that we can design a better environment. Ubiquitous Computing is used to mimic and enhance day-to-day human activities as daily tasks, medicine, education, entertainment by making our environment smarter and cooperative.

Devices are integrated with computing abilities. "**Computing everywhere for everything & everyone**". An entire ecosystem for a person is turned into a smart ecosystem and focused on making it automated for the betterment for humanity and saving time and effort to increase efficiency. Electrical devices are made automated and connected with other devices in that network and easy to use by changing use style and automation "Adjust with device without whole knowledge" i.e. someone needing a service is not required to fully understand the system.

With the increase in networks and data the extreme points for attacks and intrusion to privacy are found and fixed with unique security solution. The devices produce tons of data which can be used in both destructive as well as constructive ways and this is leading us towards new and dynamic solutions for dynamic problems. Main issues are security and privacy.

Over the years, machine learning and data mining and analysis techniques have received attention in Ubicomp. This has led to various techniques being used for security purposes.

Literature Review

In this digital era, we are moving through a phase of change in convention of one computing device to multiple computing devices at once.[1] The concept of automation is now connected with other devices of the network and service provider. Ubiquitous Computing enables various services and application and implementations. Users of Ubicomp are provided with access to various networks from remote locations with high portability, reliability and availability of the network with increased complexity.

Some Services of Ubicomp

Context-aware applications – Designed for research and automation purposes and support in mobility and physiology of the user. Sensors are provided to electrical devices with the sensors and recorded data processed for the desired solution [2]

Smart tool-box – Devices with RFIDs and network connectivity are used for reconfiguration and schema selection for the devices.

Ubiquitous Healthcare – An economizing step for healthcare resources by using ubiquitous healthcare devices for tracking, monitoring and suggesting health-related and disease-related data which could lead to a healthy future.

Smart Supply Chain – With the help of Ubiquitous Computing, industries can decrease the error counts and make work faster and more efficient.

Smart Home – Integrating Ubiquitous Computing with homes is creating and further controlling an array of automated household devices remotely whether people are home or not. Smart Homes result in enhanced security, energy efficiency and convenience at all times regardless of location.

Why Ubicomp?

Increased need for automation is creating a need for Ubicomp as the number of devices connected to internet and the data produced multiplies. Figure 1 shows the increase rate of devices.

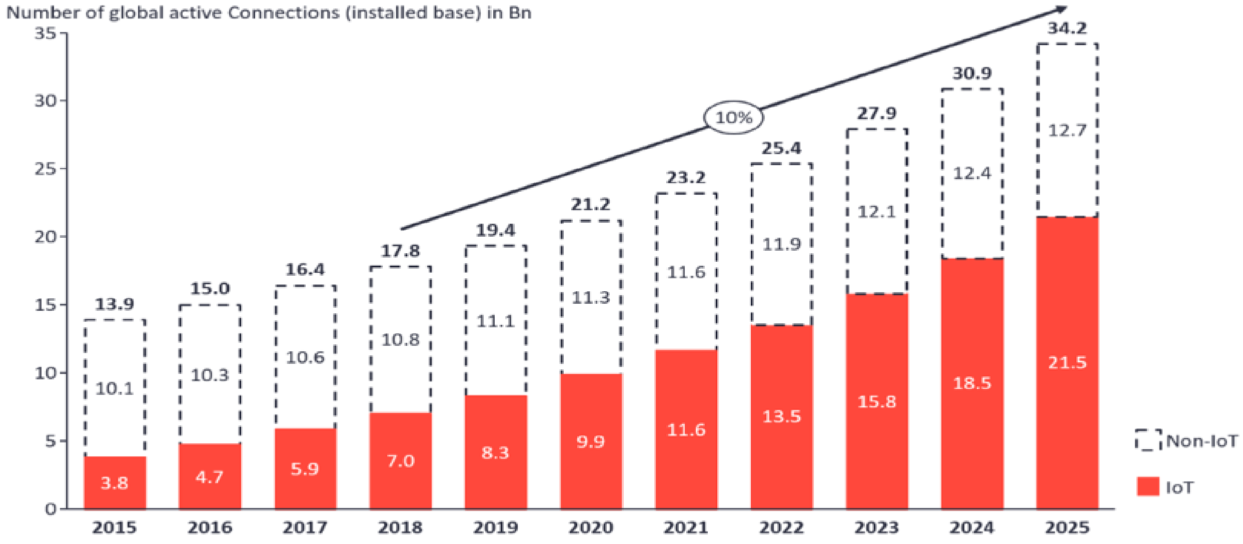


Figure 1 - Total Number of Active Device connections worldwide

As the number of devices increase, so too are the number of networks multiplying which makes all these changes possible. Along with these positive developments comes the heightened chance for network intrusion and threats for data loss and privacy issues. [4]

Security Challenges

The field of automation is booming and Ubiquitous Computing is contributing to the growth as more devices become automated to produce higher efficiency and availability. This increases the number of networks and number of devices in the network.[3] With the high demand of IoT devices for pervasive computing, quantity has taken over from quality when producing a high number of products that are often coded poorly and are less secure and unreliable. Data flowing among Ubicomp devices can be sensitive and used for destructive purposes.

Examples of Security Challenges

Device Reliability

While the requirement for automation in growing, the lack of technology keeps us from creating a secure and fully automated and connected environment.

The investment is done of making the device work functionally and serve its purpose but the data flowing from that device could be sensitive and needs to be secured. The devices are produced in quantity but are poorly coded from a security point of view and can be a vulnerable point in a secure network which can eventually cause drastic breakdown.[1] This lack of making data secured and unaltered need to be covered.

Network Intrusion

- **Man in Middle –** In security terms Man in Middle (MIM) is a known kind of attack where the attacker acts as a mode of connection between two parties whereas they think they are directly connected. Man in Middle can alter, manipulate and capture all the sensitive data without other parties knowing about the tampering of data. [2]

- **Access Network Attack –** Home gateway and Service provider are connected through the access network. Attack is performed on the data packets at the household connection points to capture sensitive data such as codes, passwords and other crucial credentials. [3]

- **Denial of Service (DoS) –** Attacker makes request with many hosts with malicious data to intrude the network and degrade it to make the service unavailable. An ecosystem based on services and connection among other devices can be destroyed by such attacks ad completely lose control over the data.

- **Password Attack –** In ubicomp the authentication process is used to build the network. Password attack is done to get authentication keys and combinations by sniffing and performing brute force attack and by using a password dictionary. [2]

Service Provider Authentication

In Ubiquitous Computing all the devices are connected to a close network as well as the head network of Service Provider or individual network service provider for operating and working dynamically and to be controlled from a remote location.[5]

Service Provider plays an important role in making Ubicomp possible as all the data transferred using services and operations are performed using network among the devices for minimum delay and quick services. Even the data can be altered if service gets downgraded or attacked.

After the Authentication with the service provider the main role is played by the network access gateways for securing the network and data flowing in network.

Security Solution

Security in Ubicomp is securing the network along with connection points by dividing networks and making the data secure.

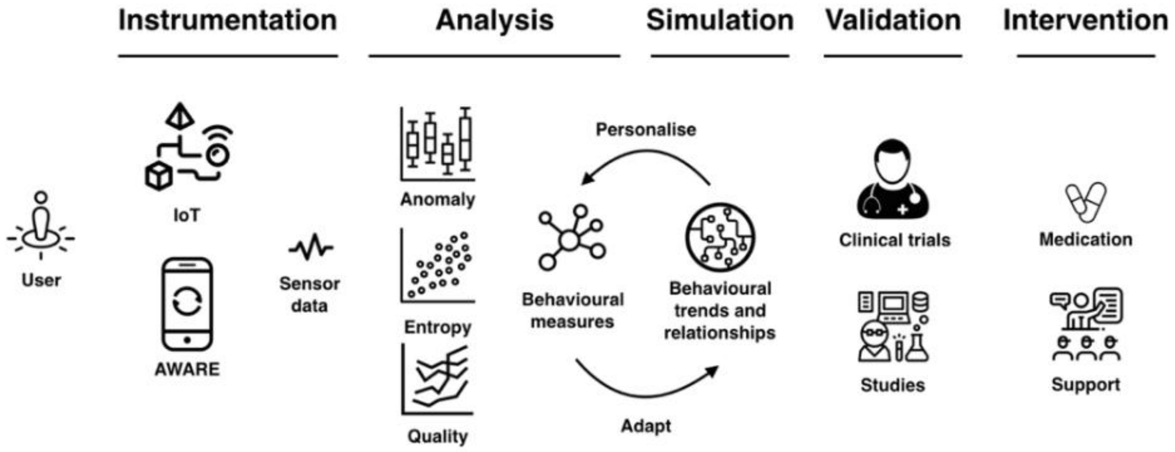


Figure 3 - Services Offered by Ubicomp

Device Reliability – As much of the functionality is focused the security should be focused to proper programming paradigm and security algorithms should be used. Suitable cryptography algorithm and security protocols should be established to secure the network and prevent data leakage. [4]

Real Time Intrusion Detection – Real time intrusion detection systems record and monitor malicious activity in the network. Previously it was done by various methods such as Intrusion Detection System (IDS) but because of various weaknesses it's now the era of Service-Oriented and User centric Intrusion Detection System (SUIDS).[2]

Role-Based Access Control – Each individual is responsible for particular roles in Role Based Access Control System. Roles are opted after assigning process according to the hierarchy of the system. It is done by mapping User Role Assignment and Role Permission Assignment for individual user and permission are granted according to the RBAC. [6]

The role is achieved according to the privileges related to the role for obtaining normal action and privileges under the role are controlled for allowances in acceptable situations.

Local Proof of Secret – The procedure for localization of credentials and secrets to avoid MIM attacks. It shows how user and entity interacts and involves verification of the attributes.

RFID Authentication – Radio Frequency Identification are microchips (also called RFID tags) used for sharing data in a secure manner in Ubiquitous Networks. Chips have a static address used for identifying the tag and the access granted to the tag holder from the database.

Traceability – Sets a network link with the opponent that can trace the content and extract location information of a potentially threatening user.

Biometrics – Should all other authentication processes fail to be the solution for authentication issues, biometrics offers a more secure and fast recognition by scanning the iris, fingerprints or face detection of the user. [2]

Such security is easy to use and secure but if someone manages to get the same biometrics, then security is compromised for every instance.

Conclusion

This study examined in depth the nature of Ubiquitous Computing and its security issues along with the miracles it can do when implemented suitably according to the need and inventions. With Ubiquitous Computing, data flow is feasible anytime, anywhere and openly among devices.

With the increase of ubiquitous networks, the major concern is data security and privacy of data from threats. This article presented and explored the applications, devices and network problems and solutions for various problems.

Key Findings

Ubiquitous Computing is the future of computing and, along with AI and Machine Learning techniques, will invisibly integrate in our environment to become part of daily life.

Pervasive computing is leading towards enabling devices to sense the situation, process the data and provide suitable results.[2] Microprocessors will be a significant game changer in making it possible for devices to gain computing power.[5] Networks continue to improve over time and will continue to be the backbone of every system to operate.

References

Scientometrics March 2011, Volume 86, Issue 3

https://link.springer.com/article/10.1007/s11192-010-0283-8

IEEE Xplore Digital Library – Proposed embedded security framework for Internet of Things

https://ieeexplore.ieee.org/abstract/document/5940923

Security Issues in Ubiquitous Computing∗ Frank Stajano

https://www.cl.cam.ac.uk/~fms27/papers/2008-Stajano-ubiquitous.pdf

Semantic Scholar – Security Related Research (Ema Kusen, Mark StrembeckPublished in ArXiv 2017)

IOT Analytics – State of UbiComp – Knud Lasse Lueth - August 2019

Ali A Ghorbani, Wei Lu and Mahbid Tavallaee: "Network Intrusion Detection and Prevention", Springer, Edition 2009.

J. P.Anderson, "Computer security threat monitoring and surveillance", 1980.

Ubicomp.oulu.fi Sensate:Entrophy Aware

Dell Technologies believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” DELL TECHNOLOGIES MAKES NO RESPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying and distribution of any Dell Technologies software described in this publication requires an applicable software license.