Securing the Gadget-Free Digital Services

Tanesh Kumar, Pawani Porambage, Ijaz Ahmad, Madhusanka Liyanage, Erkki Harjula and Mika Ylianttila
Centre for Wireless Communication, University of Oulu, Finland
{tanesh.kumar, pawani.porambage, ijaz.ahmad, madhusanka.liyanage, erkki.harjula, mika.ylianttila}@oulu.fi

***Abstract*—With the recent advancements in sensor and communication technologies, the world is facing a digital transition where nearby environments are intelligent enough to provide user-intended services without using any hand-held gadgets. This article proposes applying a three-tier communication and service architecture for such gadget-free environment, identifies its potential vulnerabilities and proposes a corresponding three-tier security mechanism for enabling secure access to the gadget-free digital services.**

***Index Terms*—Security Architecture; Gadget-Free World; Services Access; Security Threats.**

I. Introduction

THE current way of accessing digital content and services is to carry gadgets everywhere we go, such as services using smartphones, tablets and laptops. However, the proliferation of Internet of Things (IoT) is making our environment more and more connected with the digital world. The examples of current systems include building automation, surveillance systems, smart homes, etc. At the same time, wearable devices such as smart watches or clothes, as well as body-embedded medical devices such as blood sugar sensors, heartbeat sensors, pacemakers, etc. make our everyday activities connected to the digital world. This development is irreversibly changing the relationship between us and the digital world. Furthermore, the advancing communication technologies such as 5G [1] and Edge Computing [2] support this development with increasing performance, reliability and coverage.

Altogether, this development is driving us towards the new digital paradigm of hyperconnected world, where the environment is intelligent enough to offer user intended services that can be acquired in a ubiquitous manner without gadgets (also termed as the Naked World). This vision is under investigation in the Naked Approach project [3]. In the gadget-free world, users live without gadgets in the digital world, accessing their desired services through user interfaces and computational capabilities embedded in the environment. This leads us to the evolution from device-centric to user-centric service approaches.

This gadget-free hyperconnectivity requires radical enhancements in various enabling technologies as highlighted in Fig. 1. For example, user interaction will happen directly between the user and the environment without personal devices. This requires new types of interactive modalities and user authentication mechanisms. In the case of personal gadgets, the user authentication is straightforward (either entering pin-code or pattern, or using fingerprint reader to access the gadget), but with the smart environments it is more complicated. Since it is not feasible to separately authenticate users at each smart object in a smart space, trusted single sign-on (SSO) mechanisms are needed [4]. In the envisioned gadget-free world, authentication needs to be effortless for the user and should happen in a natural way [5]. Thus, the significance of different authentication methods based on recognizing biometric characteristics of persons entering the spaces, such as image/video recognition and implanted chips, will grow.

In the current cloud computing model, the service logic and data are moved from end-user devices to large centralized data centers that have global availability. Due to centralized data management, the systems are more vulnerable for cyber-attacks against privacy, availability of services and even safety. We are living in a world where our data and the data collected from our devices is ruthlessly exploited by different actors around the world. Since IoT is surrounding us almost everywhere, it gives attackers further tools to intrude our daily life activities or even threaten our health (e.g. medical/health-monitoring or driver-assisting car applications). Therefore it would be beneficial to limit the propagation of personal data and computation to local networks when universal availability is not needed. This is also one important driving factor for Edge Computing. The gadget-free hyperconnected world will be built on the concept of Edge and Fog [6] computing that push computational and storage capacity closer to users.

In the nutshell, the evolution from a gadget-centric to gadget-free world, together with rapid technological advancements, requires unified communication architecture that enables secure, flexible, adaptable and autonomous service composition based on the current needs of the users. In this paper, we first briefly introduce the three-level communication and services architecture upon which our security architecture will be built and then we identify the security threats at each layer of that architecture. Based on the threat analysis, we propose three-tier security architecture for secure user accessibility for desired digital services in such gadget-free environment.

II. Three-tier Gadget-Free Communication and Services Architecture

The concept of the gadget-free hyperconnected world mainly refers to the digital society where user centric services can be accessed anytime and anywhere without using any explicit gadgets. Smart sensors, actuators, and potential printed electronics are embedded in the local environment to deliver users some of the basic and the most frequently used services locally. However, since various computational services have different functional requirements for the platform, some of the services and computations are most optimally located at

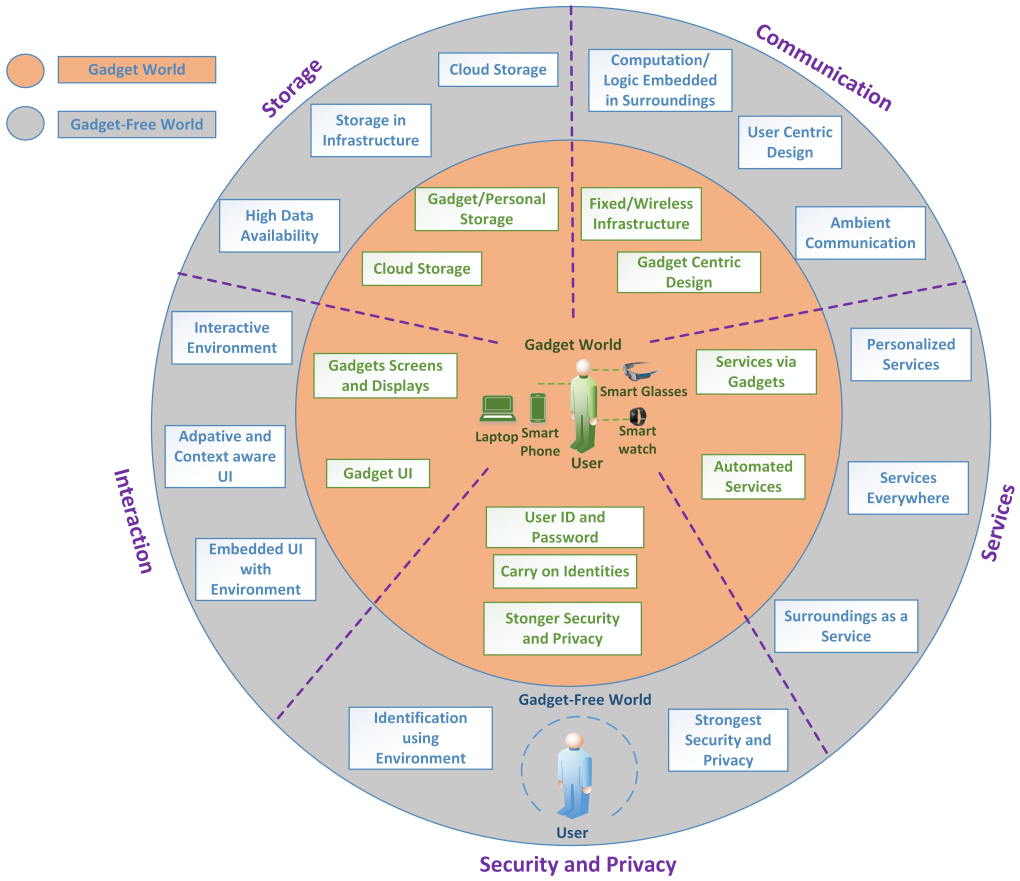

Fig. 1: Various enhancements from gadget to gadget-free world.

data centers whereas for some other services it is most optimal to locate them closer to the edge. These requirements include e.g. maximum allowed latency, minimum bandwidth, range of availability, etc. Therefore, based on various service requirements, we define a three-tier communication and services architecture as presented in figure 2.

Tier 1 - Local Network: This is considered as the lowest tier and refers to the local level network in the proposed architecture. This tier mainly comprises of various types of low power sensor and actuator nodes that can provide various services and functionalities. Some of the local nodes can provide local microservices for other nodes and/or a gateway functionality to connect the local network to the Tier-2 networks as Local Edge Cloud (LEC) services. At the local network, the user will be able to access less-demanding computational services, such as switching on and off the room light based on movement, local shared storage and caching, or sensor data fusion and filtering.

Tier 2 - Edge Network: This tier provides the connectivity from local network to the Internet, and also provides localized computational services requiring more computational capacity than Tier 1 can provide. This tier provides the Radio Access Network (RAN) and the Multi-Access Edge Computing (MEC) services based on Edge Cloud (EC). Tier 2 provides the intermediary Tier for cloud computing between Local Edge Cloud and Centralized Cloud, offering high computational capacity combined with ultra-low latency provided by underlying 5G radio access network. This tier is vital in providing elastic resources and services for gadgetless hyperconnected networking.

Tier 3 - Global Network: This tier includes the traditional Centralized Cloud (CC) service backbone (public internet) that provides globally available service platform for applications requiring high storage and computational capacity.

The local infrastructure will be crucial because most of services are embedded locally nearby proximity of users. In the gadget-free services, low latency and high data rate communications would be the key requirements to consider. In the local infrastructure, network clusters are autonomously established by nearby nodes and they are very dynamic: nodes can join and leave any time. The local network may also contain some more resourceful nodes to perform high computational tasks. For example, these high capability nodes are useful in the user authentication at the local layer and can also act as gateway node for connecting with the edge networks (clouds) for higher computational services. Nodes in the Local infrastructure are also connected to the global infrastructure (public internet) for even higher resourced services.

The public acceptance of this vision can happen only when strong security solutions are in place. The security mechanism must provide various security features such as authenticity, confidentiality, integrity, and availability of data and services. Thus each of the tier in the above defined network architecture

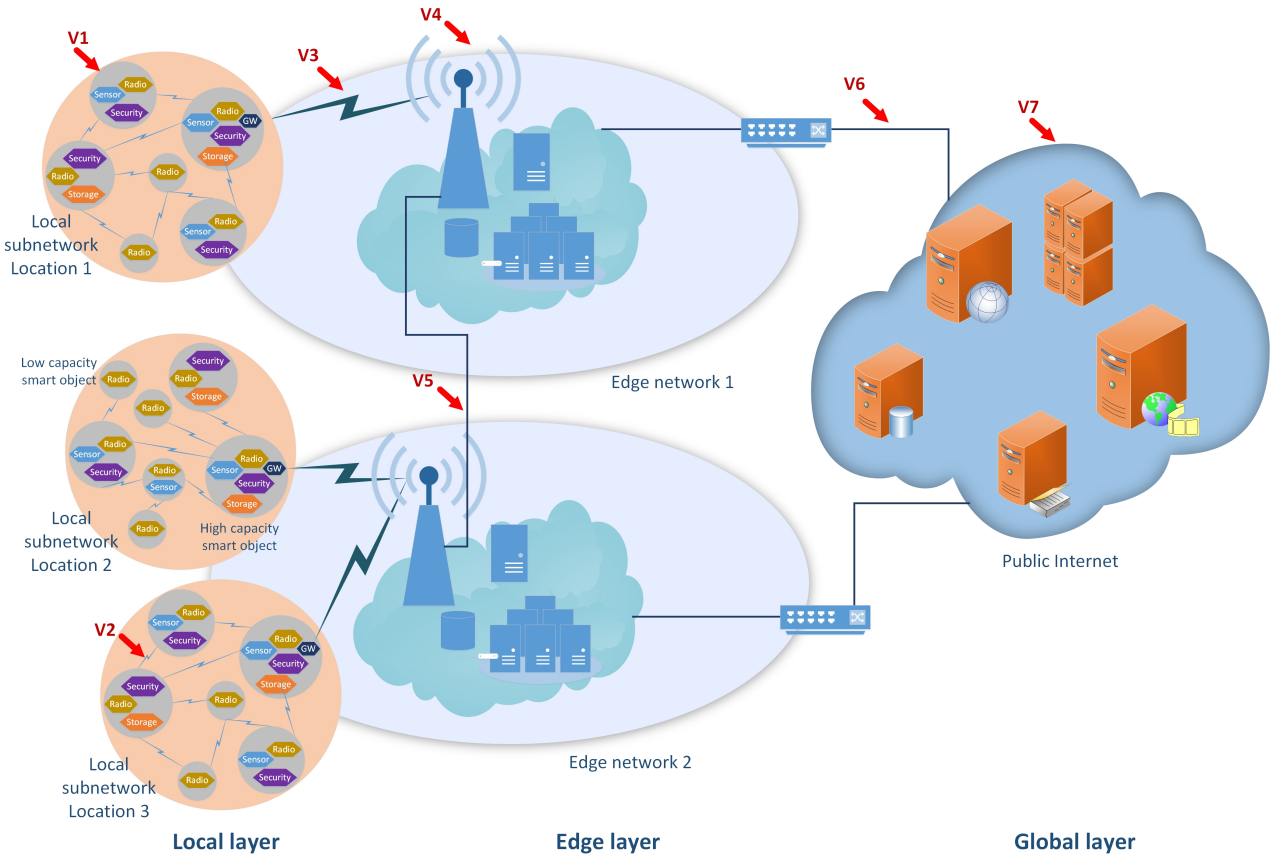

Fig. 2: Gadget-free communication and service architecture.

need to be protected against various attacks. Tier 3 (public internet) is so far the most explored one in terms of security challenges and respective solutions. Security threats at Tier 2 (edge cloud) is current on-going research and various attacks have already been highlighted. The identification of the potential security challenges in the Tier 1 (local edge cloud) is the least explored area at the moment among all.

III. Threat Vectors

We have identified seven major potential threat vectors based on three-tier gadget-free architecture as highlighted in figure 2. As per the scope of this paper, this section focuses only on the threats related to user accessibility and authentication. Moreover, we discuss the possible solutions to mitigate the identified threats. Table I summarizes the potential attacks and their consequences on discussed threat vectors.

*1) **Threat vector 1 (V1) - Vulnerabilities on nodes in local subnet cluster**:* can be triggered by malicious nodes or local adversaries. Invalid low power nodes might get access to the subnet cluster in the local networks. There also might be case where some of the nodes could be more resource constrained and cannot support the high requirement security mechanism/cryptographic operations such as authentication/key management and bootstrapping [7].

To solve these threats, it requires secure lightweight node-to-node authentication mechanism. Considering this architecture, the local nodes cluster should also contain a guard node (also termed as an agent node). This node will be responsible for monitoring the behavior of nodes at local cluster and detect malicious activities and provide necessary security resources to more resource-constrained environments. To assure that only valid nodes should join the local network, a secure bootstrapping mechanism would be needed [7].

*2) **Threat vector 2 (V2) - Attacks on communications channel among local subnet nodes**:* can cause due to the attacks on short range radio communications protocols such as, Bluetooth Low Energy (BLE), ZigBee and Near Field Communication (NFC) among others. In the case of BLE, Denial of Sleep attacks can be especially devastating to the local node clusters. These attacks can reduce the lifespan of the sensing nodes by several orders of magnitude, rendering the network largely unusable. Other attacks on BLE includes: eavesdropping attacks, treacherous attack, Denial of Service (DoS) attacks, hostile intrusion in piconet, Man-in-the-Middle (MITM) attack using unit key and relay attacks. These attacks may vary according to the category of short range communication protocol used at the local network [8].

To tackle these challenges, some of the solutions are already proposed: e.g, using the keyed hash of the link key could avoid MITM attacks in BLE technology. The idea of cookies would be useful in countering the DoS attacks where multiple authentication request are sent. The detection mechanism for hostile intruder can be provided in such a way that information related to particular piconet is added to the messages and thus,

TABLE I: Potential attacks and their consequences

Potential Attacks	Consequences	Threat Vectors							Tiers		
		V1	V2	V3	V4	V5	V6	V7	Local	Edge	Global
Advanced Persistent Threat (APT)	A continuous computer hacking processes often targeting a specific entity					✓	✓	✓		✓	✓
Bandwidth stealing and Reduction of Quality (RoQ) attacks	Enabling a particular set of flows to acquire more than their fair share of bandwidth		✓	✓		✓	✓		✓	✓	✓
Denial of Service (DoS) attack	To deny resources of network/loss of data availability	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Denial of Sleep attack	Prevent IoT devices to be entered in to sleep mode	✓	✓						✓		
Eavesdropping	Data confidentiality is compromised in network	✓	✓	✓	✓		✓	✓	✓	✓	✓
Radio Jamming attack	Deliberately jam, block or interference the authorized wireless communications		✓	✓		✓	✓	✓	✓	✓	✓
Impersonation attacks	Successfully assumes the identity of one of the legitimate parties	✓	✓		✓		✓	✓	✓	✓	✓
Man-in-the-Middle (MITM) attack	Attacker secretly alters communication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reflection attack	Attacking challenge-response authentication systems by using the same protocol in both directions		✓	✓		✓	✓		✓	✓	✓
Relay attack	Loss of data confidentiality and integrity	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sinkhole attack	Generates fake routing information	✓	✓	✓			✓	✓	✓	✓	✓
Spoofing attack	Loss of data confidentiality and integrity			✓	✓	✓	✓	✓		✓	✓
Sybil attack	Creating a large number of pseudonymous identities	✓		✓	✓			✓	✓	✓	✓
Virtual machine (VM) manipulations	Unauthorized modification of VM to malicious activities				✓	✓	✓	✓		✓	✓
Wormhole attacks	Capture traffic from one region and direct to another/Loss of data integrity	✓	✓		✓	✓	✓	✓	✓	✓	✓

adversaries can not retrieve the secret message [8].

*3) **Threat vector 3 (V3) - Attacks on communications channel between local network and edge network**:* Wi-Fi and cellular (i.e. 3G/4G) are among the potential communication ways between local and the edge networks. Wi-Fi usually faces dome of well explored security attacks such as data interception, DoS, rogue and misconfigured access points (APs), eavesdropping, and end-points attacks among others[9]. In the case of cellular networks (3G/4G), DoS signaling attack is quite common in signaling/control plane in 3G/4G wireless networks. 4G Long-Term Evolution (LTE) networks are also vulnerable to radio jamming, flooding, spoofing and bandwidth stealing attacks [9].

The use of strong wireless authentication and encryption mechanisms in Wi-Fi and cellular can resist the major security attacks such as DoS, reset, spoofing and also the impact of MitM attacks [9].

*4) **Threat vector 4 (V4) - Attacks on edges of the networks**:* An adversary can target network/communication infrastructure of the edges using various attacks such as DoS attack, MItM and rogue gateway attacks. The virtualization infrastructure at the edge network may also face major security challenges such as DoS attack, misuse of resources, privacy leakage and virtual machine (VM) manipulations[10]. Physical damage, privacy leakage, privilege escalation and rogue data center are some of the vulnerabilities that can impose various threats to the edge data centers [10].

At the edge network, trust management and authentication mechanism is crucial because multiple entities at the edge (actors, services and infrastructures) do coexist. Moreover, the availability of authorization mechanism is also vital in order to verify the credentials of particular entities requesting for certain actions. Apart from above methods, intrusion detection and prevention mechanisms are needed to detect the internal and external malicious entities and propose corresponding defense mechanism. Moreover, countermeasures such as isolation policies, hypervisor hardening and separation of VM roles should be implemented in all commodity servers to protect the virtualization platforms [10].

*5) **Threat vector 5 (V5) - Vulnerabilities on communication channel between two edge network**:* The current IP based communication between edge networks is vulnerable to a full range of IP and web based attacks such as IP spoofing, Transmission Control Protocol (TCP) SYN (Synchronization) DoS, TCP reset, Poodle attacks and Botnets[9]. Specifically, MEC architecture is vulnerable to DoS attacks when the combination of multiple VM spread across several mobile edge hosts. Moreover, a public IP network such as Internet or mobile network or wide area network might be used as the underlay network to provide the connectivity between edges. The security holes in underlay network will also jeopardize the connectivity between edges [9].

Strong authentication mechanisms and encrypted communication should be enabled inter-edge communication channel to prevent unauthorized access to channel. Secure tunneling mechanisms such as IPsec or secure Virtual Private LAN

Services (VPLS) can be used to prevent the impact of security weaknesses in underlay network [9].

*6) **Threat vector 6 (V6) - Attacks and vulnerabilities on communication channel between edge and global network**:* Similar to the previous threat vector V5, The current IP based communication channel between edge and global network is also vulnerable a full range of IP and web based attacks. Specifically, the global network side will be exposed to millions of untrusted devices, particularly in the Internet.

Secure tunneling mechanisms such as IPsec or secure VPLS can be used to provide strong authentication mechanisms and encrypted communication to prevent these IP based attacks. However, the preliminary method to protect the edges from the attacks that are initiated from the Internet is to filter and drop the malicious traffic at the entry point to the edges. Hence, a security gateway should be implemented at the edges. This security gateway should contain security functions such as firewalls, Deep Packet Inspection (DPI), Intruder Prevention Systems (IPS), Intelligent DDoS mitigation systems and uniform resource locator (URL) filtering application control.

*7) **Threat vector 7 (V7) - Attacks and vulnerabilities on global networks (Public Internet)**:* The global network (i.e. Internet) consists of millions of cyber attackers, cyber-criminals and malicious users. As a result, the proposed system is vulnarable to traditional Internet based attacks such as DDoS, Advanced Persistent Threat (APT), SYNful knock" attacks etc. Targeted attacks such as APT can also do severe damage when the system becomes a highly desirable target for cyber-criminals and attackers. On the other hand, unaddressed software vulnerabilities or service misconfiguration can also leads to system failures. If the firewall is not configured correctly, the system becomes an easy target for unauthorized access [11].

As we discussed earlier, strong authentication mechanisms and encrypted communication are the key requirement to protect End-to-End (E2E) data transmission. Thus, a comprehensive, multi-layered security solution is required to mitigate these Internet based attacks. Apart from that, the edges should be protected with high capable security gateways. Moreover, system firewalls and software firmware should be updated regularly to eliminate the known vulnerabilities [10], [11].

IV. Proposed Three Tier Security Architecture

In order to mitigate the highlighted security vulnerabilities, we propose corresponding three-tier security architecture to counter several attacks at different tiers for example, DoS attack, replay attack and sinkhole attacks among others. Note, there are some attacks which are not addressed by this security architecture, for example, in some cases intrusion detection and prevention mechanisms are required to detect few attacks at local and edge networks. Thus, in the above section, we already highlighted some of these attacks and their potential solutions. The main focus of this paper is to analyze the possible attacks caused due to lack of proper authentication and authorization mechanism at various tiers in proposed three-tier architecture and thus we proceed with solutions for such attacks only. Our proposed solution provides not only authentication/authorization but also many other security implications including access control, secure E2E communication, and secure node bootstrapping. The secure architecture for gadget-free services is vital from two perspectives: 1. Smart object bootstrapping, and 2. Secure user accessibility to the required services.

A. Smart Object Bootstrapping

Bootstrapping[12] follows certain methodologies and processes through which one smart object can join a local network. This process will ensure that only authorized smart objects should be able to join the network. Initially, a low capacity smart object requests for joining local network using root identity (O1.1, O1.2) as shown in Fig. 3. Root identity is a statically configured cryptographic material, which is embedded by the manufacturer for bootstrapping mechanism. Next, using the root identity, authentication (O1.3) and authorization (O1.4) mechanisms are performed and eventually the smart object is added to the local network. Once the bootstrapping is successfully done, it generates some further cryptographic material (also known as domain identity (O1.5)). The domain identity is associated with additional characteristics of the smart node that are related to deployment domain, such as the owner and thus, it can be used for management tasks. Also domain identity permits smart object to get identified for the next processes within the local network. The complete identity of the smart object can be described by the domain and root identities.

If the smart object fails to authenticate and authorize itself at the the local network, the error request is reported to Error Control Unit (ECU) (O1.3.1, O1.4.1) at the local layer. ECU is responsible for error detection and control mechanisms. Moreover, after bootstrapping, the smart object should also be registered with the local network, so that it can be discovered by other available objects within the network. For the registration of particular smart object, it uses the domain identity (O1.5) for authentication (O1.6) and authorization (O1.7). Having the authorized domain identity, the key managements unit derives group keys (O1.8) for further secure communications.

In order to access higher computational services, the smart object needs to be connected with the edge layer. For that purpose, the complete identity (O2.1) is sent by the local IdM to the edge layer (O2.2). The authentication (O2.3) and authorization (O2.4) processes are executed at the edge layer. If the smart object is successfully authorized, the access control (O2.5) mechanism is granted (O2.5), corresponding session keys (O2.6) are initiated, and respective services (O2.7) are enabled. Otherwise, in case of failure, errors are reported to ECU at the local layer (O2.3.1, O2.4.1).

B. User Service Accessibility

The secure user accessibility mechanism for the required services can be three-fold depending upon the type of services requested as mentioned in Fig. 4, i.e, authentication with local layer; authentication at edge layer and authentication with global layer.

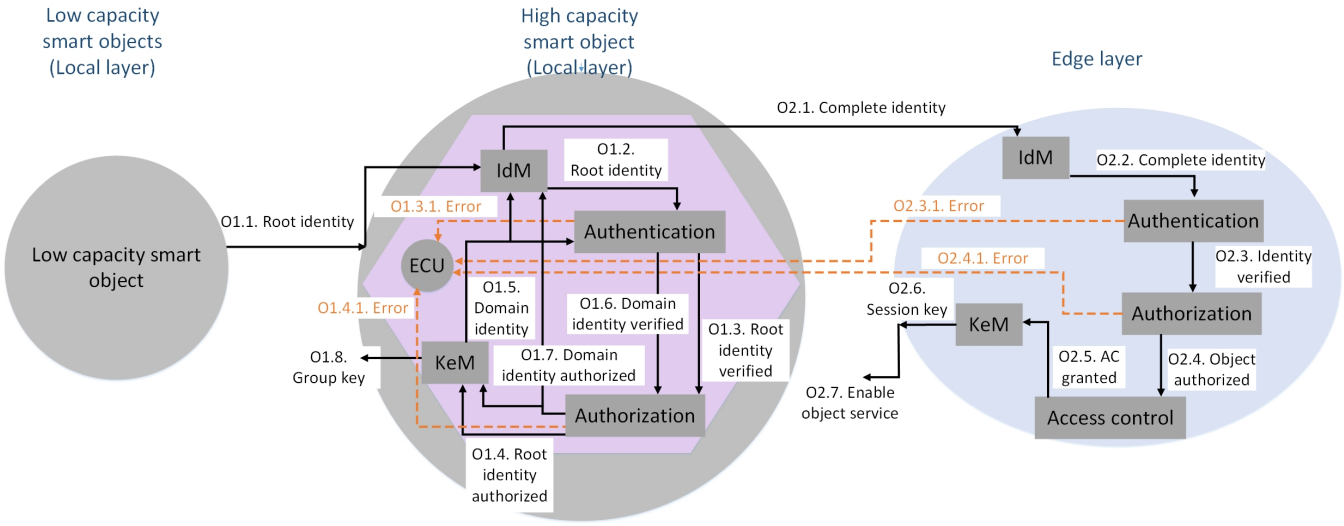

Fig. 3: Smart object bootstrapping and registration mechanism

1) Initialization of users accessibility to local layer services: The services offered at the local layer tend to be very basic i.e. services having less storage and processing/computations. Therefore, in this case, the local level authentication will be sufficient and no further authentication is required at edge or global levels (i.e. as marked by the red cross in Fig 4). The secure service accessibility of the user in local infrastructure will potentially comprises of the following steps: the new user first request for particular services from local infrastructure using the biometrics credentials (U1.1). A high capacity smart object fetches the users biometrics features for the identification mechanism (U1.2). Next, the user is authenticated (U1.3) and authorized (U1.4) for the local services. On the successful authorization, requested services are enabled (U1.6) for the user. If the user is unable to authenticate or authorize at the local network, the request is passed to ECU (1.3.1, 1.4.1).

2) Initialization of users accessibility to edge layer services: If the user's request services are more computational intensive and are not available at the local network, the user should be authorized to edge layer to access those services. The credentials (U2.1) of the new user are fetched and passed to local network. Afterwards, the user identity (U2.2.1) is passed for authentication at the local network. If the requested services are present at local layer then it will follow similar steps mentioned in above subsection. If not, then the user identity (U2.2) is passed to edge network. Since the service requires further authentication at the edge layer, the user identity needs to be forwarded from the local layer (U2.2.2 and U2.2.3). The authentication (U2.3) and authorization (U2.4) are performed and access control (U2.5) is granted. The session is initiated and group keys (U2.7) from edge network are shared with KeM at the local network. Also the domain identity (U2.6) is generated and shared with the IdM at the local layer for further necessary actions. Finally, the services are enabled (U2.8) for the respective user.

3) Initialization of users accessibility to global layer services: Global level user authentication is required for accessing the central cloud or public internet (Global tier) to accomplish higher computation and resourced services.

This phase is crucial, when the authorized user could not find requested services at local or edge network. Following will be the probable steps for this case: the new user first needs to authorize with the local and edge network through similar process as described in above subsections. Then the user credentials (U3.1) is fetched from smart object and from IdM (U3.2) at the local network is passed to the global network (using U3.2.1 to U3.2.5). The authentication (U3.3) and authorization (U3.4) process are performed at the global and corresponding access control (U3.5) is granted. ECU is again responsible unit, if any error is reported in these processes (U3.3.1 and U3.4.1). Next, the session is initiated and group keys are shared with KeM at both the edge and local networks (U3.7 and U3.9) respectively and services are enabled (U3.10). Also corresponding domain identities are generated and shared with IdM at the edge and local networks (U3.6 and 3.8).

V. Discussion

The proliferation of IoTs and availability of diverse services will enable new modes of accessing digital services, for example, interaction of users in smart environments. This paper extends the mode of service interaction further by enabling users to access services without gadgets through intelligent interfaces embedded in the nearby surroundings. Therefore, new service architectures and infrastructures will be required to detect a user, project user interfaces in user vicinity, initiate user identification, and offer the user-intended services accordingly. The user interfaces fade away into background once the user completes the tasks and securely terminates the session. Provisioning such services will need fool-proof security architecture to avoid security lapses of user information, restrict the services to legitimate users and maintain high level of user privacy. Henceforth, a tier-specific security architecture has been proposed that ensure the security of the service infrastructure by using e.g. secure bootstrapping

of nodes or smart objects and ensuring end-to-end security between the user and the system while the user uses the services. The authentication and key management mechanisms proposed in three-tier security architecture are useful and capable in countering most of the above identified potential security vulnerabilities. However, new security challenges may also arise when such architectures are deployed and used in practice. Therefore, security-by-design will be the key requirement to mitigate the possibility of security lapses as much as possible.

Since there will be no gadgets that maintain running sessions while the user is moving, continuity of services during mobility will be highly challenging. From security point of view, the most prominent challenge will be single-sign-on authentication during roaming from one point of access to another. This means that sessions will be disrupted during mobility since the users will need to authenticate themself every time they start interaction with the surrounding interactive objects. The limitation of the proposed architecture is that the user will always need to restart authentication with the first tier and go gradually to the global services, unlike traditional service architectures which do not require stepwise re-authentication with mobility. Henceforth, the future of such systems will rely on highly context-aware biometric authentication system coupled with user tracking to directly recognize the user without going through all the steps, and provide the services which the user intends to use. One possibility will be the service and security credentials movement with the movement of the user-anchoring point such as interactive connected car that the user uses to interact with systems while moving from one place to another.

VI. CONCLUSIONS

With the digitalization of everyday life activities, there is a clear need of various modes of secure and smart services access mechanism. The gadget-free hyper-connected environment promises an intelligent and highly context-aware surrounding, where users can access required services anytime without using hand-held gadgets. However, to realize this vision completely, there are a number of issues that need to be addressed and more specifically security of whole the service architecture. This work proposes a secure three-tier service architecture for such smart and gadget-free environments, enlist its security challenges and proposes the solutions for them.

ACKNOWLEDGMENT

This work was supported by TEKES and Academy of Finland, under the Naked Approach, Towards Digital Paradise and WiFiUS: Massive IoT Projects.

REFERENCES

[1] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of things in the 5g era: Enablers, architecture, and business models," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510–527, 2016.

[2] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, Jan 2017.

[3] I. Ahmad, T. Kumar, M. Liyanage, M. Ylianttila, T. Koskela, T. Braysy, A. Anttonen, V. Pentikinen, J.-P. Soininen, and J. Huusko, "Towards gadget-free internet services: A roadmap of the naked world," *Telematics and Informatics*, vol. 35, no. 1, pp. 82 – 92, 2018.

[4] M. Surya and N. Anithadevi, "Single sign on mechanism using attribute based encryption in distributed computer networks," *Procedia Computer Science*, vol. 47, pp. 441–451, 2015.

[5] T. Kumar, A. Braeken, M. Liyanage, and M. Ylianttila, "Identity privacy preserving biometric based authentication scheme for naked healthcare environment," in *2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–7.

[6] A. V. Dastjerdi and R. Buyya, "Fog computing: Helping the internet of things realize its potential," *Computer*, vol. 49, no. 8, pp. 112–116, Aug 2016.

[7] H. J. Kim, H. S. Chang, J. J. Suh, and T. s. Shon, "A study on device security in iot convergence," in *2016 International Conference on Industrial Engineering, Management Science and Application (ICIMSA)*, May 2016, pp. 1–4.

[8] M. M. W. Iqbal, F. Kausar, and M. A. Wahla, "Attacks on bluetooth security architecture and its countermeasures," in *Information Security and Assurance*. Springer Berlin Heidelberg, 2010, pp. 190–197.

[9] G. Chopra, R. K. Jha, and F. Lone, "A survey on wireless security: Ip security concern," in *Proceedings of the International Conference on Data Engineering and Communication Technology*. Springer, 2017, pp. 711–722.

[10] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[11] H.-C. Huang, Z.-K. Zhang, H.-W. Cheng, and S. W. Shieh, "Web application security: Threats, countermeasures, and pitfalls," *Computer*, vol. 50, no. 6, pp. 81–85, 2017.

[12] J. L. Hernandez-Ramos, J. B. Bernabe, and A. Skarmeta, "Army: architecture for a secure and privacy-aware lifecycle of smart objects in the internet of my things," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 28–35, September 2016.

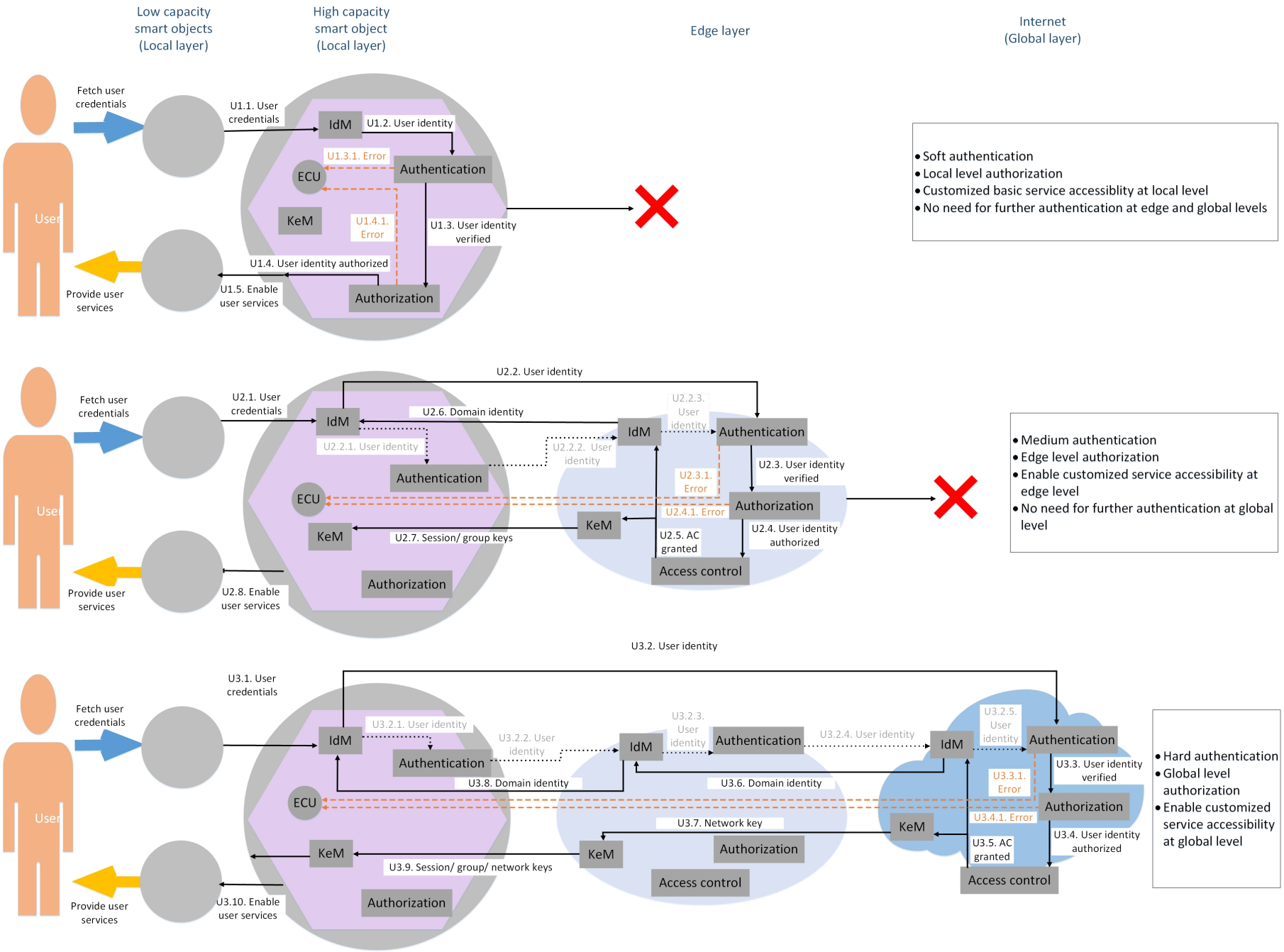

Fig. 4: Secure user accessibility for gadget-free services.