Towards a Secure Service Provisioning Framework in a Smart City Environment

Zaheer Khan+,
Department of Computer Science and Creative Technologies, Faculty of Environment and Technology,
University of the West of England, Coldharbour Lane, Bristol, BS16 1QY, United Kingdom,
Tel: +44 - 117 3287216; Email: Zaheer2.Khan@uwe.ac.uk

Zeeshan Pervez,
School of Engineering and Computing, University of the West of Scotland, Paisley, United Kingdom.
Tel: +44 - 141 848 3183, Email: Zeeshan.Pervez@uws.ac.uk

Abdul Ghafoor Abbasi,
School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Islamabad, Pakistan
Email: Abdul.Ghafoor@seecs.edu.pk

+ Corresponding author

Abstract:

Over the past few years the concept of Smart cities has emerged to transform urban areas into connected and well informed spaces. Services that make smart cities "smart" are curated by using data streams of smart cities i.e., inhabitants' location information, digital engagement, transportation, environment and local government data. Accumulating and processing of these data streams raise security and privacy concerns at individual and community levels. Sizeable attempts have been made to ensure the security and privacy of inhabitants' data. However, the security and privacy issues of smart cities are not only confined to inhabitants; service providers and local governments have their own reservations – service provider trust, reliability of the sensed data, and data ownership, to name a few. In this research we identified a comprehensive list of stakeholders and modelled their involvement in smart cities by using the Onion Model approach. Based on the model we present a security and privacy-aware framework for service provisioning in smart cities, namely the 'Smart Secure Service Provisioning' (SSServProv) Framework. Unlike previous attempts, our framework provides end-to-end security and privacy

features for trustable data acquisition, transmission, processing and legitimate service provisioning. The proposed framework ensures inhabitants' privacy, and also guarantees integrity of services. It also ensures that public data is never misused by malicious service providers. To demonstrate the efficacy of SSServProv we developed and tested core functionalities of authentication, authorisation and lightweight secure communication protocol for data acquisition and service provisioning. For various smart cities service provisioning scenarios we verified these protocols by an automated security verification tool called Scyther.

Keywords: Smart city, security, privacy, trust, framework, stakeholders, secure service provisioning

1. Introduction and Context

Smart cities are emerging rapidly due to new technologies such as the Internet of Things (IoTs), e.g., RFIDs, environmental sensors, actuators, smart phones, wearable sensors, cloud computing, etc. New smart city services and applications (e.g. participatory sensing [1][2]) provide the opportunity to collect and effectively use large scale city data for information awareness, urban planning, policy making and decision making [3][4]. As a result, new models of transformed urban governance e.g. open governance are being formed where data from different devices (e.g., things) can be integrated with existing city data (i.e. from various departments and local agencies). This integrated data can be analysed for application specific information and knowledge generation [2]. Such processing and storage of large scale data can be performed in a cloud environment to satisfy quality of service requirements, e.g., response time of end user queries by provisioning of cloud based virtually unlimited elastic computational and storage facilities.

However, with these opportunities and transformational (or open) models of urban governance there exist new threats to user and/or device privacy and confidentiality of data when communicated between two or more devices and/or users, and establishing trust on services and information [5]. In [1] Christin et al performed a state of the art literature survey on privacy issues in mobile based participatory sensing applications and identified open privacy issues with possible solutions. Similarly, other researchers [6] argued that privacy of both data consumers and data producers must be afforded for user participation in participatory applications. In addition, inherent cloud security issues, e.g., storage at remote data centres, physical access, etc. contribute further in dealing with smart cities data security issues [7], [8]. Managing such data and developing new services from a smart city perspective requires proper security and privacy measures which can help in establishing trust and adopting smart services by various stakeholders including citizens [9].

State of the art literature reviews indicate that smart city solutions need a comprehensive approach in dealing with smart city data security, user or device privacy and trust issues. For instance, Symantec published a comprehensive report on security and privacy challenges in smart cities – identifying smart cities as a domain of hyper vulnerability [10]. According to Symantec Internet Security threat report 22% of targeted attacks are aimed at governments and energy/utilities companies; whereas, government and healthcare institutions are the target of 24% of identity breaches. The report stated that Supervisory Control and Data Acquisition systems based on conventional software technologies are subjects of attacks, and vulnerabilities can be exploited to disrupt the service delivery. This can have devastating effects on the security and privacy of the inhabitants as their private and confidential service usage data will be at risk. This report has identified that not only that security and privacy of the users are at risk, but service providers are also facing cyber security threats. This is because attackers can compromise service delivery models to gain illicit access to the service itself or would attack data sensed / accumulated by a service. Numerous attack scenarios are identified in which an attacker can either inject malicious information into the system causing faulty provisioning of a service or can impersonate legitimate service subscribers to gain illicit access to the service and private and confidential data. The authors conclude the report with the recommendation for a secure transition to a resilient smart city - establishing a governance framework, compliance to risk and governance policies, protecting information proactively, authenticating users, managing security services and developing an information management strategy. The report also refers to the World Economic Forum Cyber Resilience Maturity Model – classifying organizations based on their security awareness and willingness to take on proactive measures [11]. These classifications are based on the level of concerns ranging from least to high as: unaware, fragmented, top down, pervasive and networked. This maturity model is very useful in making government rules and regulations for service provisioning in smart cities.

Similarly in [12], J-M et al highlighted security, privacy and trust challenges of using ICT in a smart cities context [12]. These challenges are mainly attributed to the distributed nature of IoTs which require new innovative security mechanisms. For instance, they argue that many devices are no longer protected by well-known mechanisms such as firewalls and can be attacked by wireless channels directly. In addition, due to the pervasiveness of IoT, devices can be stolen and analysed by attackers to reveal internal sensitive mechanisms which can be vulnerable to attacks. They emphasise that establishing trust between multiple data sources to perform data processing and generate required information is another important challenge which also requires the secure exchange of data between devices and/or their consumers.

Likewise, in [13], Correia L M et al identified several characteristics of smart cities and requirements for technologies which pose new challenges to data security and privacy needs. For instance, in a context aware service provisioning, user characterisation and identity needs to be protected for privacy reasons e.g. techniques like pseudonymisation can be used to avoid illicit use of personal information. Similarly, interconnection of various city systems e.g. traffic, energy, utility may introduce unknown vulnerabilities in the systems and require security research in complex distributed systems including advanced encryption, authentication and access control, advance data aggregation techniques and interoperable identity management etc.

It is evident from the literature that many attempts have been made to identify the security and privacy concerns of future cities as indicated in Section 6. However, existing work in the area of smart cities is limited to the security of data or curated services. Also, with the emergence of new or transformed urban governance models such as open governance and open data based citizen services creates new privacy and security challenges.

In the above context, our main contributions in this research include: i) identification of a comprehensive list of stakeholders ranging from inhabitants to local governments and data streams to service providers presented as the Stakeholder Onion Model; ii) identification of stakeholders as entities who are affected by the malicious behaviour of other involved entities; iii) presentation of security and privacy concerns from all angles i.e., stakeholders being a victim and attacker; iv) end to end secure and privacy aware service provisioning in smart cities; v) introduction of a new security framework namely the 'Smart Secure Service Provisioning' (SSServProv) Framework, that covers security, confidentiality and privacy aspects from the perspectives of service providers and service consumers; vi) definition of an example use case of open governance using citizen participation and open data that is used for instantiation of the SSServProv framework; and, vii) a verification model for testing selected components of the security framework as proof of concept against well-known security threats and results are presented through an automated verification tool namely Scyther.

1.1 Rationale

Approximately 50% of the world's population lives in urban areas, a number which is expected to increase to nearly 60% by 2030 [14]. High levels of urbanisation are even more evident in Europe where today over 75% of Europeans live in urban areas and the urbanisation of the European population is expected to increase to over 80% by 2020 [15]. Urbanisation and its associated socio-economic and environmental impacts is one of the key drivers of change that challenges the sustainability of urban environments globally and is placing significant pressure on public

authorities.

Over the past few years the concept of Smart cities has emerged to transform urban areas into connected and well informed spaces. Cities around the world (Vienna, San Francisco, Bristol, etc.) are trying to adopt this new notion of connectivity for better urban planning, disaster recovery and improved quality of life. Driven by the advancements of information and communication technologies the cities of the future will be better planned and well informed from the micro (inhabitants, local businesses) to the macro level (local government). ICT is becoming increasingly pervasive to urban environments and providing the necessary basis for citizen participation in planning decisions. New socio-economic, environmental, health, land use and citizens data collection through crowdsourcing and other IoTs can be used for analysis and decision making for sustainability and resilience of the smart future cities [16].

However, all these advancements come at the cost of "right to security and privacy". The whole concept of smart cities is tightly coupled with "data" and "connectivity" [17]. Services that make smart cities "smart" are curated by using the data streams of cities i.e., inhabitants' location and digital engagement information, transportation and local government data [18]. Accumulating and processing these data streams also raises security and privacy concerns at both the individual and community levels [19]. These security and privacy concerns are not confined to inhabitants only, service providers and local government have their own valid reservations. Therefore, ICT solutions seek suitable platform and data security mechanisms to maintain user privacy, comply with national legislation regarding data sharing, establish trust on these solutions and maintain the integrity and confidentiality of data and secure service provision. Such security measures are needed for wider adoption of smart cities solutions by public administrations, as well as citizens.

1.2 Research methodology

The objective of this work is to identify smart city data and services challenges and propose appropriate end to end security solutions. In this research a mixed method approach is adopted that is based on a literature survey and scenario based model verification. Using this methodology we first identify various smart cities data security related challenges and limitations in existing solutions. Then, we introduce the Smart Secure Service Provisioning (SSServProv) framework that deals with data curation and secure and privacy-aware service provisioning in Smart cities. Since the impact of services in smart cities is at the macro level, it is very important that accurate and traceable data is curated and processed by the service provider. To cater for this SSServProv deals with citizen authentication and data anonymisation. As proof of concept we verify the effectiveness of selected components of the security architecture through a scenario based model verification technique.

The remainder of this paper is structured as follows: Section 2 identifies different stakeholders who can benefit from the proposed solutions. Section 3 briefly introduces smart cities and associated data security challenges. The Smart Secure Service Provisioning' (SSServProv) Framework is presented in Section 4. Proof of concept through Scyther based automated model verification is presented in Section 5. Section 6 presents the related work along with comparative analysis of SSServProv with state-of-art in Smart cities. Section 7 concludes the paper along with future work.

2. Stakeholder Onion model

Data security and privacy aspects need to be dealt with from different stakeholders' points of view to support end-to-end application security. For smart city information security, eight major stakeholder roles are identified. These roles are derived from listing the most possible types of stakeholders who may have direct or indirect vested interest in smart city development. Since such a list is exhaustive, stakeholder roles are defined which are relatively manageable and easy to present. These roles can be used to define role-based access policies using appropriate tools e.g. the eXtensible Access Control Markup Language (XACML) [20]. These roles are:

Service consumers: represent stakeholders who are end users and mostly direct beneficiary of a system, for example, Citizens, Community, Public administration, City planners, Policy makers, NGOs, Service Developers, Domain Experts, Business Organisations, Local Agencies (e.g. Law Enforcement, Environment, Transport, Construction), etc.

Legitimate service providers: represent stakeholders who are registered with a governing body and are authorised to deliver services to service consumers. For example, service developers develop different services such as Information services, Utility services, Environmental services, Transport services, E-Government services, Business services, Economic services, Energy services, Health services, etc.

Untrusted (or Malicious) service providers: represent stakeholders who are not registered with a governing body but still deliver services to service consumers (e.g. marketing/advertising agencies etc.). There is no guarantee that there is no malicious intent behind service provision and these services may be provided by Hackers or Attacker, Identify thieves, Information thieves, etc.

IT experts: represent stakeholders who introduce new systems (e.g. sensors or other hardware) and develop software applications for different stakeholders. These can be IoT designers & builders, thematic application developers, Hackathon programmers, Open data app developers etc.

Data custodians: represent stakeholders who are responsible for city data management. These

can be City administrations, Environmental agencies, Transport agencies, Business organisations, Public security agencies, Social network site, Crowdsourcing users etc.
Standard governing bodies: represent to organisations who develop different standards for smart city, cloud applications and cyber security. Also, institutions which define related regional or national data protection laws and regulations (e.g. EU Data protection law) can be included in this group.
Domain experts: represent members who have domain specific expertise and are interested in development and innovation in specific thematic area, for example, Environmentalists, City planners, Energy experts, Transport/Mobility experts, Socio-economic experts, Policy makers, Health experts, IT experts, etc.
Others: represent any other stakeholder types which do not fit within other seven roles.

The level of trust for the above roles can be different and these roles cannot always be trusted. For instance, it is obvious that services from untrusted service providers cannot be trusted because these services are not registered by a governing authority (in our case governmental domain). In contrast, legitimate service providers, service consumers, IT and domain experts can be trusted after conforming to set security protocols (discussed in the next section). These roles are responsible to build their trustworthy credentials by developing and registering with a governmental domain authority. The level of trust varies for different stakeholder types under data custodian role. Data from the repositories of city administration and agencies can be trusted as mostly such data is acquired from reliable data sources e.g., spatio-temporal data from environmental sensors, crime statistics, land use, transport sensors, etc. However data generated through crowd sourcing or social networking require provenance techniques (e.g. W3C PROV model[1]) to build trust on such data sources.

These stakeholder roles are further extended and mapped onto a Product Onion Model [21] where each circle in Fig. 1 presents specific roles relevant to the development of a certain stage of the overall system. There are four concentric circles:

The Product is the inner circle that provides the Smart Security framework and components proposed in this paper. This provides the basis for handling data security and privacy aspects in a variety of smart city applications from different stakeholders' points of view.
The System is Smart Security components and its human operators, security policies and rules governing its operations. The objective here is to define access, authorisation, secure communication protocols, and confidentiality strategies for prime operators of the product. These prime operators can further delegate credentials to other stakeholders in the smart city

[1] W3C PROV model - URL: https://www.w3.org/TR/prov-primer/ Last Accessed: 20 March 2017

applications layer for the development and usage of a variety of applications.

Smart City Applications encompasses the System and its operators including any human beneficiaries of the System. The objective here is that all operators at this layer must comply with security policies set up in the product layer and perform operations authorised by the system layer.

The External Environment includes secure smart city applications and any other beneficiaries.

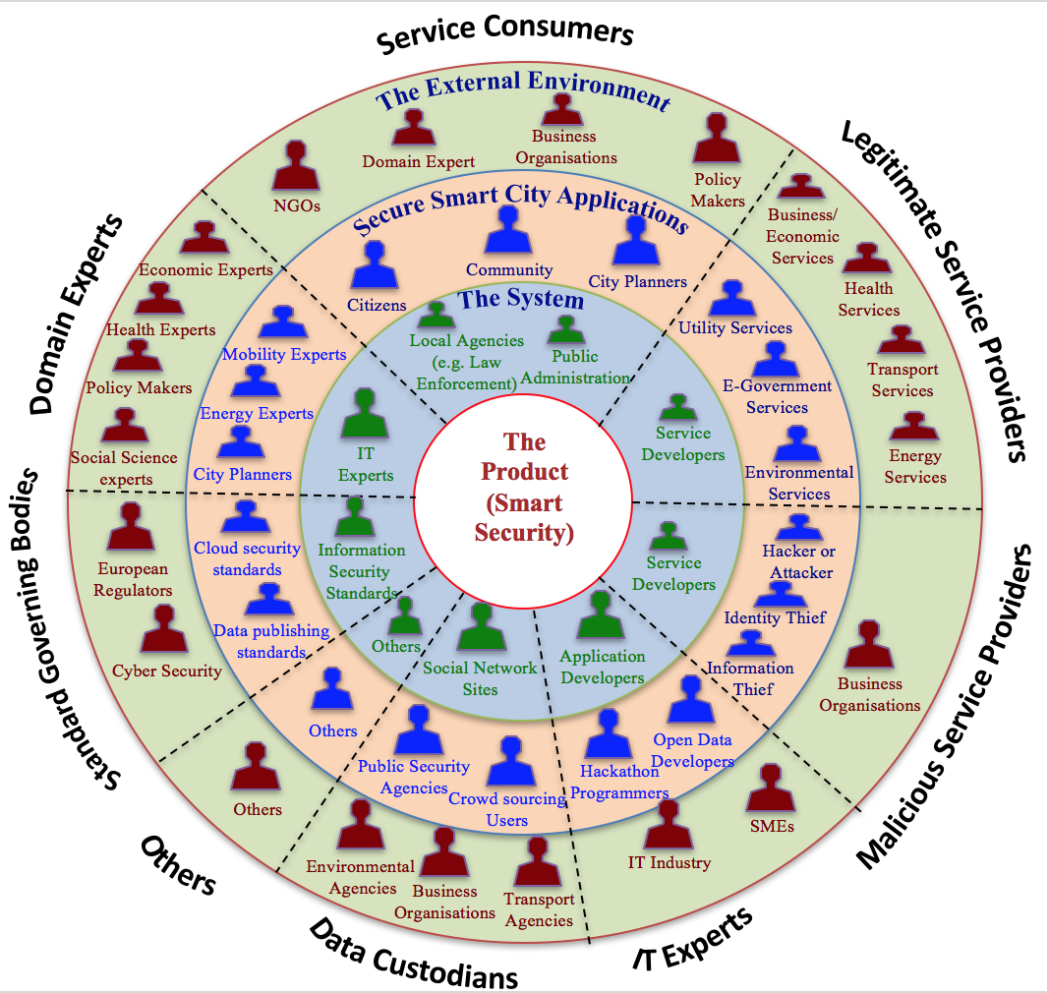


Fig. 1: Onion model for smart cities stakeholders

3. Smart cities and Data security challenges

Smart cities are regarded as “massively connected spaces”. These spaces are intrinsically associated with data, connectivity, and information processing. In smart cities, sensory devices

(smart phones, surveillance camera, IoT device), user generated contents (opinion polls, social media), and institutional records (government agencies, healthcare provider, transport data) are regarded as the main sources of data. From a technological perspective, the whole concept of smart cities evolves with the technological advancement in transmitting and sharing data methodologies from diverse modalities with the consideration of real-time, reliable and robust communication between data sources and data consumption points. The benefits of having massively connected spaces are realised by provisioning intelligent services (e.g. London Airtext[2] service, Moovit[3], SeeClickFix[4], Street Bump[5], ICT-enabled city governance and policy making projects e.g. urbanAPI[6], FUPOL[7], DECUMANUS[8], are a few examples) to the inhabitants of smart cities. These services process data from diverse modalities to make intelligent decisions and consequently improve the quality of life within the context of the environment, open and transparent local government processes, and behavioural change of inhabitants for sustainable cities to name just a few.

Considering the data, connectivity and information processing as enabling factors for smart cities, we have identified the following entities (section 3.1 to 3.4) which are vulnerable to security and privacy attacks. In the following we also consider that these entities can act maliciously, consequently compromising security and privacy of other active and passive entities. Fig 2, presents the security and privacy concerns of smart cities.

[2] London Airtext service: http://www.airtext.info/ . (Accessed: 22 May 2017)
[3] Moovit app: http://moovitapp.com/en-gb/. (Accessed: 22 May 2017)
[4] SeeClickFix: http://en.seeclickfix.com/ . (Accessed: 22 May 2017)
[5] StreetBump: http://streetbump.org/ . (Accessed: 22 May 2017)
[6] urbanAPI: http://urbanapi.eu/ . (Accessed: 22 May 2017)
[7] FUPOL: http://www.fupol.eu/en . (Accessed: 22 May 2017)
[8] DECUMANUS: http://decumanus-fp7.eu/home/ . (Accessed: 22 May 2017)

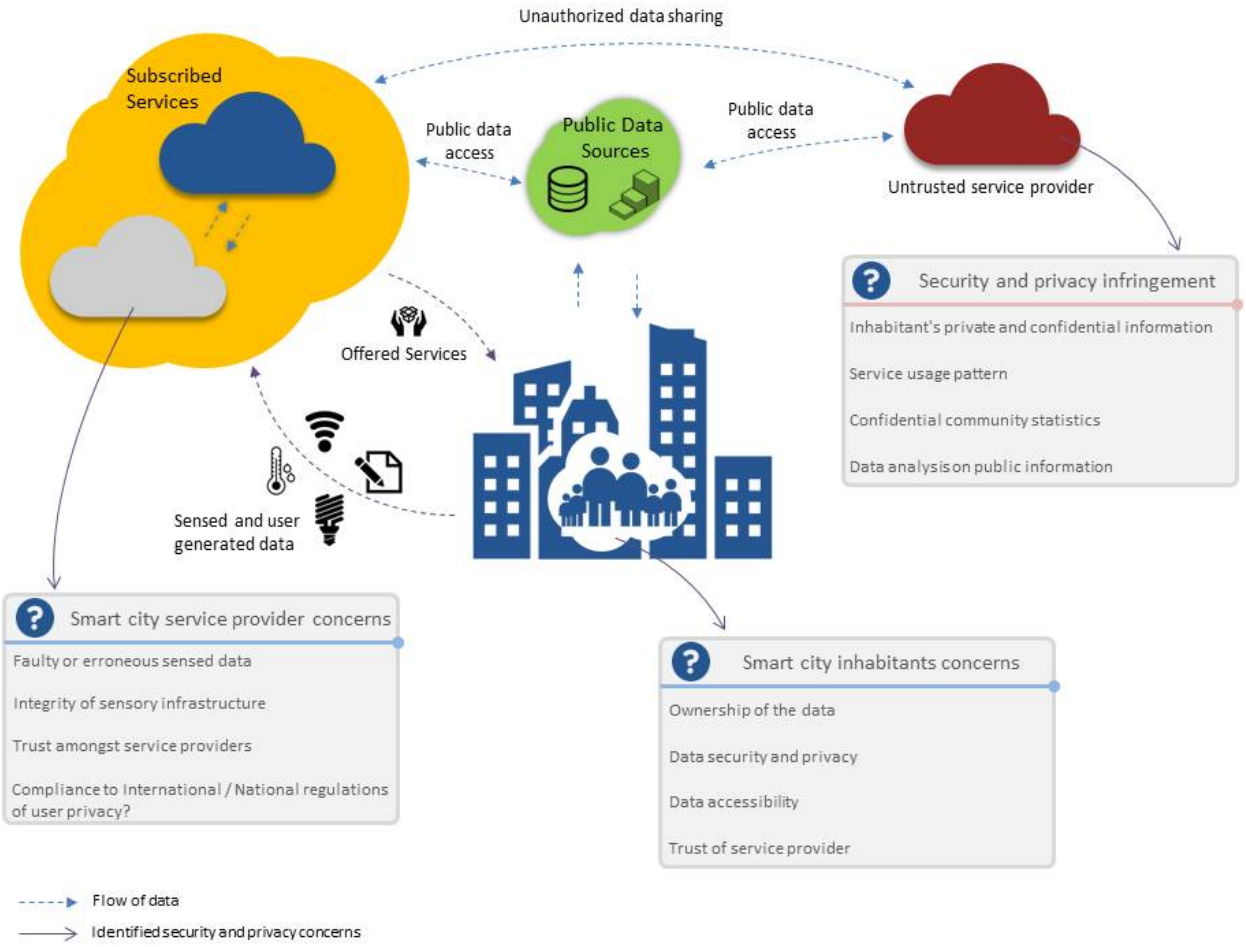


Fig. 2: Smart city: Security and privacy consideration of participating entities.

3.1. User

In the context of smart cities a User is regarded as an entity which contributes in data generation by transmitting and sharing data from sensory devices and daily life interactions / activities. In return a user expects services transforming personal and urban life experience by getting contextual information of their surroundings.

i) Personal information

One of the biggest security and privacy concerns in smart cities is the risk of compromising a user's personal information. A connected environment expects a user to transmit and share sensed and user generated data. Data from different modalities, along with publically available

information, are processed to provide desired services. For example, in a connected environment a user might be interacting with a service which processes location information to recommend nearby dining places based upon user preferences. However there is a great risk of security and privacy infringement, as over a period of time a malicious service provider can accumulate a user's dietary habits and extrapolate his/her health profile. This clearly compromises privacy, potentially having devastating effects on a user's personal life, as extrapolated information can be shared with potential employers and insurance agencies which may have reservations with certain future health conditions , or it could be the case that the extrapolated information is completely wrong.

Furthermore, with the initiations like open and linked data the concepts of smart cities will flourish. We will see new and innovative services exploiting massively connected spaces – consequently elevating the quality of life in smart cities. Smart cities are source of huge volume of data, but there are some serious security and privacy concerns which are associated with it. These concerns range from an individual inhabitant of a smart city to a community level. This is because data generated from the smart cities can reveal unforeseen information, which may not be evident otherwise, and can have associated privacy implications.

ii) Data ownership and control

Another security and privacy concern which is associated with the data generated in connected environments is data ownership and having accessibility control over it. Considering who has the right to transmit, share and process the data can have serious security and privacy implications. Besides this, it also affects the adoption rate for a service, especially for those dealing with private and personal data i.e., healthcare, daily activity information, etc..

The complexity of managing control over data in a smart cities environment is huge, since these are connected spaces having myriad sensory devices collecting private and personal information related to user and its associated interactions – daily life activities, social media interaction, and sensory information. Besides this, the scope of security and privacy concerns of smart cities is huge; it must be considered that not all inhabitants of a connected space are equally concerned about security and privacy, and may be inadequately equipped with the knowledge to control their private and personal data i.e., adolescent and elderly. Consider an example in which a user having more concerns about privacy moves to a connected place which is controlled by a person having less concerns about his/her privacy, how the system will behave if there are conflicting data sensing, transmitting and sharing policies. If there is a case of conflicting policies how the user is informed in advance about the security and privacy implications.

In the subsequent sections we will elaborate that even if access control policies are managed and enforced properly there are possibilities that malicious service providers can still infer personal information which leads to a loss of data and personal privacy.

iii) Identity

Data from diverse sources i.e., location information, user interaction, open and linked data and social media are a few examples of data sources processed in the realm of smart cities. The efficacy of smart cities and the success of services it can offer are directly based on data, which can either be obtained from a public and private domain with the consent of involved entities – users, organizations, government agencies, etc.

However, most of the security and privacy issues are directly concerned with the association between the data and its owner. For example if a location based social networking service which processes user's location information is compromised and looses its data, the attacker can effortlessly learn activity patterns and contextual preferences of the users subscribed to the social networking service.

Depending on the nature of a service some may require to process personal information i.e., healthcare services which require user vital signs information in order to provide appropriate healthcare services. In such services sensed data should be properly anonymised in order to avoid malicious use of the sensed data which enables an attacker to effortlessly associate clinical findings with the user. Data acquisition and its processing should be within legal limits defined by concerned authorities along with the consent of entities having directly security and privacy implications.

Services which are designed for massively connected spaces must persist and process personal data in such a way that in case of an attack it is practically infeasible to track back to the original sources of the data. On the other hand, association between the data and the respective entities is important in order to ensure that data is gathered and processed from credible sources.

3.2. Data

The ecosystem of smart cities is built around data, which is gathered from diverse sources having varied security and privacy requirements. In the subsequent sections we will elaborate security and privacy concerns of data transmission and its storage beyond the federated domain of its owner.

i) Transmission

Smart city is a highly connected environment which expects to obtain data from different modalities – data acquisition through sensory devices (i.e., smartphones, surveillance cameras, traffic data etc.) and processed data (i.e., government data, social network analysis etc.). Each of these data acquisition methodologies has its own security and privacy concerns. For example, in case of sensory devices it is important to ensure that data is securely transmitted between the sensor nodes and central processing unit. Other security and privacy concerns which require a collaborative effort amongst the sensor node and central processing units are authenticating and authorising sensor nodes within a massively connected space. Also, in a space where myriad sensor nodes are working collaboratively it is important to identify malicious behaviour of a sensor node and isolate it from the network. Whereas, to ensure that data acquisition through sensor nodes comply with data security and privacy policy of a particular context, introduces more complexity in management and enforcement of data transmission and sharing policies.

Similarly, for processed data which is shared between services to complement each other's functionality there are great risks of security and privacy infringement. For instance, a location based social network can utilize its user generated contents to identify places which are popular amongst certain groups of people. Local businesses can consume this information in order to define an effective marketing strategy. However, if this information is infamously used, there are great risks of security and privacy infringements for the participating entities.

ii) Cloud based services

With t90% of the world's data generated in the last few years, cloud computing is becoming prevalent [22] – with its on-demand resource provisioning. In smart cities cloud computing can significantly elevate the capabilities of a service to persist, process and provision data. However, with services relying on public cloud infrastructure (i.e., storage, computation, network), there are great risks of security and privacy infringements. Public cloud providers are often considered as untrusted entities because very little technical and management details of the cloud infrastructure are shared by the providers. That is, the internal working of a cloud infrastructure is regarded as a business secret.

Since a public cloud infrastructure resides beyond the federated domain of its subscribers, cryptographic methodologies are often employed to ensure data privacy and confidentiality. However, these methodologies can significantly limit the data processing capabilities. For example encrypted data cannot be searched by using conventional content matching algorithms, also processing encrypted data for analytical purposes becomes computationally infeasible as encryption distorts data in order to achieve confidentiality. Search over encrypted data provides

solutions to relevant data access (i.e., search) with trapdoor and index based methodologies [23], [24]. However, those methodologies have limited functionalities; trapdoors can only search for pre-defined words and index based search adds auxiliary data with the original data thus requiring continuous updates and management. Although search over encrypted data ensures security and privacy of the data; however, its usability cannot be compared with conventional search involving rigorously researched relational and NoSQL data management systems.

Another problem of public cloud infrastructure is trust, how to ensure that a public cloud provider is performing the defined task honestly and not colluding with malicious entities to compromise security and privacy. There could be a case in which an access control policy is defined by a subscriber to provision access to processed data to other services e.g., a restaurant recommendation service can request information from a data analysis service which provides a list of dining places based on social network analysis. In this case the issue becomes how to ensure that the public cloud provider is enforcing access control policies honestly and not provisioning access to unauthorised subscribers.

Even if all privacy and security measures are enforced properly, public cloud providers can still compromise the privacy of the data and consequently its subscribers by analysing service usage patterns. Consider an example in which an inhabitant of a connected environment shares its vital signs (e.g., blood pressure, glucose readings, dietary habits etc.) with a medical doctor. If a cloud infrastructure is employed to securely store and process the sensed data, the public cloud provider can still infer the health conditions of the inhabitant, by simply analysing data access patterns i.e., if the data is more frequently accessed by a doctor who specialises in chronic diseases it is likely that the inhabitant is suffering from health condition having long-lasting clinical effects.

3.3. Service provider

In smart cities the core purpose of data acquisition from diverse modalities is to provide services to its inhabitants. The security and privacy concerns of a massively connected space are not confined to its inhabitants (or service consumers) only. Service providers have their own concerns, which mainly arise because inhabitants can behave maliciously by tampering with the hardware and/or software resources which sense and process the data respectively (e.g. crowd sourcing applications). Also, protecting privacy of both data consumers and producers is an essential element to promote participatory applications in smart cities.

For example, a power company relying on smart metering infrastructure may be concerned by the integrity of the smart meters which measure the power usage of its subscribers. This is

because malicious subscribers can tamper with smart meters to provide false readings of power consumption. Since smart metering infrastructure relies upon wireless communications to relay sensed data, security concerns associated with the data transmission need to be addressed as well, from both the service provider and inhabitants' perspective. Service providers are concerned about the integrity of the sensed data. Whereas inhabitants require end-to-end confidentiality ensuring that transmitted data cannot be intercepted by an attacker to learn the power usage pattern.

Service providers relying upon public cloud infrastructure to process the sensed data and provision services to its subscribers may have concerns about the honesty of the cloud provider. For example, a data analysis service which processes publically available data to sell its finding to local businesses for effecting marketing, may be concerned that its analysis results can be intercepted by a malicious cloud provider and sold to its potential customers.

3.4. Citizen (or Information) Services

The concept of smart cities is tightly coupled with the data and services. These services utilize data from diverse modalities to provide useful statistical measures (e.g., geo-tags, pollution, tree count, etc.). The efficacy of smart cities lies in the hand of application developers to make innovative use of data that providing better urban life experiences to its inhabitants and useful statistical measures to policy makers.

However, in a technological ecosystem where myriad developers can utilize seamlessly available data (sensory, social engagement and government data), another security issue that needs to be addressed is how to ensure that services are solely developed to elevate urban life experience and are not with malicious intent to compromise the privacy of a subscriber. For example, one of the sustainable and smart transport solutions to reduce GHG emissions is car or lift-sharing using a specific business model (e.g. Car2Go[9]) where sharing of passenger and financial information may be exploited by different service providers.

In addition, as the concept of smart cities matures, numerous services will be developed, driven by a need to target new business opportunities. For example, in a shopping mall equipped with an indoor positioning system (e.g., Apple iBeacon), a shopping service pushes location specific advertisements based on a user's location and preferences. If a service is malicious, it can collude with sellers offering higher prices, and advertise their products, consequently betraying the subscribers' reliance on the credibility of the advertisements. Similarly, off-the-shelf sensor

[9] Car2Go: https://www.car2go.com/en/austin/ . (Accessed: 22 May 2017)

devices (e.g., surveillance camera, motion sensors) can be developed by a service provider with malicious intent to compromise the privacy of a user or targeted community.

A crucial challenge faced by smart cities is developing a trust framework which can ensure that services driving smart cities are without malicious intent. This problem is similar to App markets for the smartphone industry which are maintained by vendors. In App markets every service is meticulously tested to ensure it complies with policies and regulations. Security and privacy challenges of the "Service Market" for smart cities have many critical implications. Since smart cities is an emerging concept having blurry data usage and service provisioning regulations, and most critically having a myriad of data sources to exploit, there is a great need to realise a trust framework which can test and ensure service is credible and fit for use for its inhabitants.

4. The Smart Secure Service Provisioning (SSServProv) Framework for Smart Cities

In the previous sections we highlighted the fact the security and privacy concerns in smart cities are not confined to inhabitants. Service providers and government agencies have their own concerns ranging from tamper resilient service to enforcement of governmental regulations and policies. Fig. 3 illustrates the conceptual model of the 'Smart Secure Service Provisioning' (SSServProv) Framework for massively connected spaces. It deals with secure and privacy-aware provisioning of services and trusted acquisition of data in smart cities. Besides this, it also ensures that involved entities are working in compliance with governmental regulations and policies.

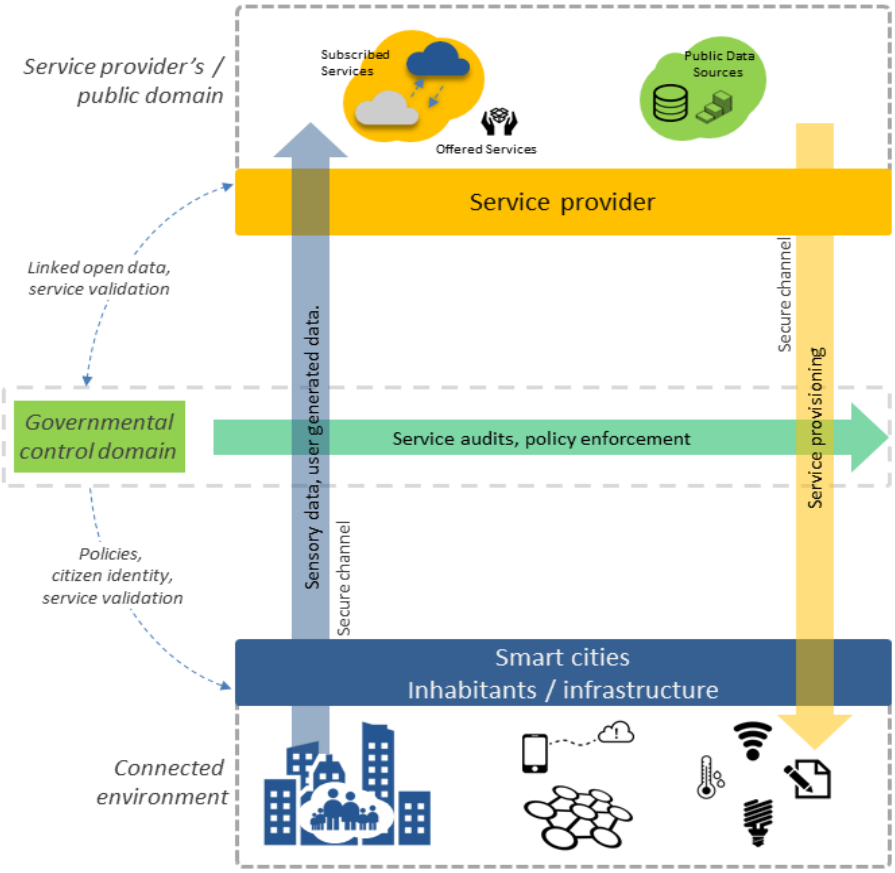


Fig. 3: Concept model of Smart Secure Service Provisioning' (SSServProv) Framework.

Before we present the SSServProv framework in detail (Fig. 4), we first describe a use case for smart cities open data management, followed by descriptive details of the SSServProv framework.

Use Case: Open governance through open data and citizen participation

Like many city administrations in Europe, City council Pesh is moving towards an open governance model by transforming its administrative and decision making processes. One of the steps taken by the Pesh council is to make a large amount of city data open and accessible through its open data web interface which can be exploited by its citizens and other businesses. Due to cuts in the IT budget, the Pesh council wants to reduce the development and maintenance budget and hence decides to deploy its open data system on a cloud platform using a pay as you use model. This cloud platform is owned by Zebr.

Pesh council intends to update and enrich this open data on a daily basis. Therefore it outsources

a web based application to local SME Tanvin to maintain regular updates of city data. The agreement between Pesh and Tanvin enables Tanvin to gain access to some additional city data which is not publicly available and does not violate any data sharing policies (e.g. health data). In return, Tanvin develops an open data management system, namely 'Smartizen', for Pesh council that allows citizens and other local stakeholders to identify new issues by enriching existing data or providing new data through a smartphone app or PC web browser. Citizens and local stakeholders use Smartizen to get access to open data (through a visual application) and participate in city processes by providing new updates on local aspects. Smartizen also offers open interfaces for other service developers to access open data and develop new applications which can also be used to enrich open data through crowdsourcing. The Pesh council uses the updated data for their planning purposes. Tanvin, as a legitimate service developer registered with Pesh council, can use available city data and develops new applications for its business.
However, Pesh council is also concerned about data security aspects. Pesh council wants to ensure that all data integrity, privacy and trust related issues are properly managed. For example, the identity of citizens and other local participants using Smartizen should be hidden from Zebr and Tanvin to: i) comply with the National citizen identity/location publication policy, and ii) avoid any illegitimate exploitation of end user behavioural patterns. Also, only authorised council staff should be able to access the new enriched data. Pesh council also wants to ensure that data enrichments and updates from citizens and other stakeholders are reliable and do not possess malicious intent e.g. wasting council resources on a false alarm. Smartizen should also respect privacy concerns of crowd source participants based on their privacy preferences e.g. anonymised feedback.

It is worth mentioning that the aforementioned use case is a general service provisioning and data accumulation scenario for any smart city, e.g., the pilot studies in the Smarticipate project [25] and IES Cities project [26]. This scenario can be specialised for a particular service, e.g. protecting the privacy of participants in a crowd-sourcing application; or authorised access to data or personalized service; or secure storage of city data in cloud; or secure exchange of data between two or more entities/users, etc. The generic nature of the above scenario indicates various security and privacy requirements for different services and hence it necessitates a structured and flexible design of the proposed framework. In this respect, the proposed SSServProv framework can be scaled to these specialised services, mainly because of its layered approach of service provisioning, adopting standard security solutions, governmental control and service consumption in smart cities. This layered approach covers known security issues as reported in the literature and by deploying various components in three layers, as depicted in Fig. 4. This layered approach is akin to a service oriented approach that can be scaled to handle end-to-end secure and privacy-aware provisioning of new services. The strength of this approach is its

flexibility to accommodate new components in these three layers to handle zero-day security threats or scenarios. For example, the concept of a governmental control domain to implement/enforce policies and regulations under which service providers and consumers can operate can be extended with new policies to handle evolving security parameters or scenarios. In addition to that, the token-based authentication, secure communication protocol, and authorisation mechanisms are included in the form of separate components therefore all these components can be easily scaled to meet the future requirements of city administration, service providers and service consumers.

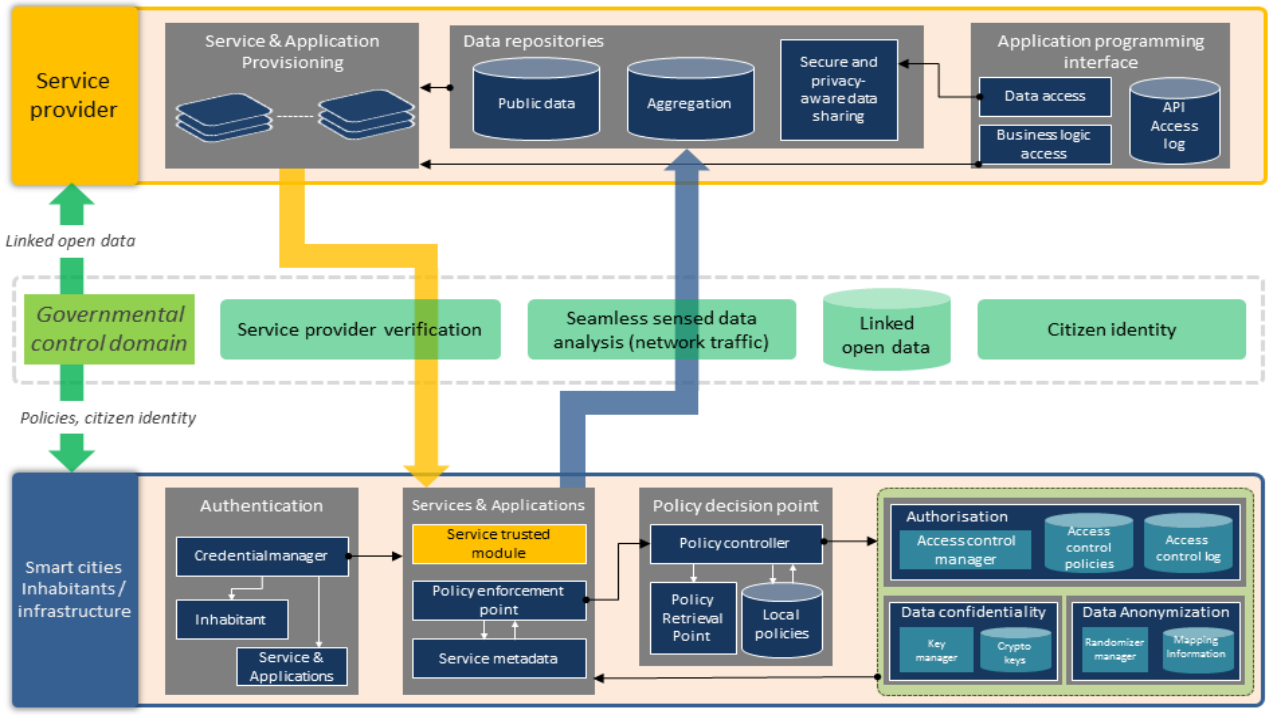


Fig. 4: Smart Secure Service Provisioning (SSServProv) Framework for Smart cities

4.1. Governmental control domain:

In the proposed framework the governmental control domain works as a regulatory authority. Its main goal is to ensure that both the service providers and inhabitants of smart cities are working within the defined regulations and policies.

i) Service provider verification

To ensure legitimate and trustable service provisioning it is very important to verify a service

provider (i.e., organization or individual). This will not only restrain malicious service providers from deluding the inhabitants but also assist in traceability in case of any security breach and privacy infringement.
In the aforementioned scenario Tanvin would first needs to register itself with the Pesh council. By registering, it provides a service descriptor to the council – stating its service contract, intentions and justification for data acquisition. Pesh council can then decide to authorise Tanvin to provision its service to the inhabitants of Pesh or not. It can also order any change in service provisioning according to security and privacy implications.

ii) Seamless sensed data analysis
It is very important that a regulatory authority implements a proper audit trail mechanism. This ensures that involved entities are working within their limits. This component monitors service provisioning and data acquisition channels to identify any unauthorised provisioned services and malicious data access.
Pesh council works in conjunction with Internet Service Providers to seamlessly monitor network traffic. To ensure uninterrupted service provisioning network analysis can be carried out in an offline mode and periodically. Since the council knows Tanvin's service descriptor it can identify if Tanvin tries to maliciously sense data which is not defined in its service descriptor. It can then revoke Tanvin's service verification and informed the inhabitant accordingly.

iii) Linked open data
The regulatory authority takes on the responsibilities to provide open data access to authorised service providers. It leverages service providers to design, develop and provision services elevating life experiences within smart cities.
Tanvin can avail open government linked data access to find new business opportunities for service provisioning within healthcare, transport. Since each service provider is registered with Pesh council it is very convenient to manage fine-grained access.

iv) Citizen identity
Issuing credentials to the inhabitants of smart cities is very important, since inhabitants derive the data generated by massively connected spaces within smart cities. Citizen identities ensure that service providers can trust the data sources, and in case of any data delude can trace back to the source and avoid forging service experience.
Pesh council issues verifiable identity attributes to its inhabitants. Any pseudonym techniques can be used here. For example, Tanvin designs a recommendation service which assists single mothers in raising their newborn. Since Pesh council is providing funding to support the recommendation system, Tanvin needs to ensure that only legitimate single mothers are using it

- Tanvin does not want to misuse the tax payers' money. Each subscriber provides their identity attributes issued by Pesh council, and Travin effortlessly verifies inhabitant's request and provisions service accordingly.

4.2. Smart cities Inhabitants / infrastructure

This layer of our proposed framework deals with the security and privacy of inhabitants and data generated from diverse modalities (i.e., sensed data, user generated data). It also ensures that provisioned services are working properly and are not tampered with by malicious entities. Enforcement of governmental regulations and policies is handled by this layer as well.

i) Authentication

Security and privacy measures can only achieve their goals if involved entities are authenticated and possess legitimate credentials to access and provision services, inhabitants and service providers respectively. This component deals with the registration of inhabitants and devices (IoT devices, including smartphones and wearables) using unique identifiers i.e., social security number, and International Mobile Equipment Identities. It ensures that a service provider is acquiring data and provisioning services to legitimate users only. It is also responsible for authenticating provisioned services to guarantee that inhabitants are not engaging with malicious or forged services. After verification, the registration authority issues a certificate or access tokens to the verified inhabitants for consuming services as an authenticated user.

In the context of the aforementioned scenario, Pesh council maintains attribute based credentials of inhabitants. Credentials managers are responsible for checking the legitimacy of credentials, this ensures that inhabitants are consuming service with their real / legitimate credentials, and are not using pseudonyms. A credentials manager also takes on the responsibility of checking the legitimacy of services provided by Tanvin. This restrains provisioning of malicious services as each service would have to undergo an issued credential verification before it can be consumed by inhabitants.

ii) Services & Applications

This component deals with tamper resistant service provisioning and enforcement of governmental regulations. Service providers can be a victim of unauthorised service consumption as malicious users can tamper with services to gain illicit access. Since a service provider is required to abide by the rules and regulations laid down by government this model also takes on the responsibility of ensuring that services are working as delineated by their service descriptor approved by a regulatory authority during the service registration process. After verification, it must be digitally signed so an attacker cannot tamper with it. Furthermore, the software modules

used in various services are also digitally signed by using the credentials stored in the trusted module. With services and applications, a Policy Enforcement Point (PEP) utilises an XACML based access control model in which it uses Roles, Rules,Objects and Permissions. An attributes based model can be used to ensure that applications and services are only provisioned to authorised users. PEP will assist Tanvin to enforce required policies.

Considering the working scenario, Tanvin can deploy tamper resistant sensors and network nodes equipped with trusted modules. It can then run periodic checks on sensors through trusted modules. This can be achieved by requesting each sensor to engage in a challenge which can only be verifiable by the trusted module if the service or sensor has not been tampered with. This challenge is a digital signature of all software modules used in the business logic. A trusted module can also monitor network traffic to ensure that unauthorised users are not consuming services by circumventing any security measure, i.e., credentials or required identity attributes. PEP assists Tanvin to implement the required security and privacy policies accordingly to its service descriptor; for example in a healthcare service user name and identify information is anonymised and the policy defined in the XACML also uses these anonymised IDs which are mapped with the roles.

iii) Policy Decision Point (Policies for context and location)

Risks of security breach and privacy infringement can be significantly reduced if appropriate access control and data confidentiality policies are selected. This component of our proposed framework deals with the selection of policies which ensure that necessary measures are taken before a user's private and confidential information be accessed or shared. Policies are selected based on sensed information and a service descriptor. If a service requires access to private and confidential data, it may be required that to store the data in an untrusted domain either the data must be anonymised or encrypted before it can leave the user controlled domain. The Stakeholder Onion model presented in the Section 2 explicitly identifies entities (or roles) which may request access to a particular resource or the provision of a service within a smart city. PEP can utilise this information to provision access based on their pre-defined interaction with the resources (e.g., data, network, services etc). These access control policies can be defined using role-based profiles in XACML [20].

For example, consider Tanvin's location-aware recommendation system for tourist attractions and hotels. With evolving government regulations Pesh council can declare certain areas as having serious privacy implication i.e., bars, casino, blue light areas to name a few. In this context the policy controller assists Tanvin to select appropriate security and privacy policies which comply

with government regulations. The policy controller works collaboratively with a Policy Retrial Point to select the most suitable policies. Local policies ensure that within Pesh council local communities or stakeholders can define their own data acquisition policies – a bar can decide that wearable cameras (e.g. Google glasses) have serious implications on it business thus prohibits its usage within its premises.

iv) Authorisation

This component complements the capabilities of the Services and Applications to enforce appropriate access control policies. It also maintains access control logs to record data access activity. Furthermore, these log files are encrypted and digitally signed so any malicious software cannot read them and cannot change them for malicious purposes. These log files significantly help in the case of privacy infringements. It is used to store general access control policies which comply with regulatory authority or personalized access control preferences defined by inhabitants. The proposed framework is designed to handle various access models. Access control manager can realise an appropriate access control model e.g. role-based XACML model [20], complying to authorisation requirements specified in the service description and entities interacting with the services and resources.

For example, Pesh council permits authorised service providers to provision activity monitoring services to its inhabitants – assisting them to live a healthy life by learning their calories count and exercise routines. Tanvin does so by analysing data from wearable devices (e.g., smart watch etc.) and location information to learn an inhabitant's meal preferences. However, a user may be conscious about her location and may not wish to share. The authorisation component leverages her to define personalized data access policies restraining Tanvin from access location information from some or all locations, depending upon inhabitant's choice (or contextual preferences).

v) Data confidentiality

This component deals with data security. It ensures that private and confidential data is not accessible to malicious service providers or users. It provides necessary cryptographic primitives enabling inhabitants and authorised service providers to process and persist data in an untrusted domain i.e., public cloud services. It works in conjunction with the Services and Applications to conceal sensitive data according to the security policies selected by the policy decision point. These policies can specify either all data should be protected or only specific parts should be concealed. The data protection policies also provide information about the cryptographic algorithm used for encryption of private and confidential data. Since most of the data storage software provides built-in mechanisms for encryption, in our solution we considered only those

here. For data integrity and non-repudiation, we introduced an extra field which stores the signature of a complete row. When a user or a service tries to access data from the data storage, first it verifies the signature and after that decrypts attributes before presenting it to the requested module.

Tanvin can sense data according to its access privileges; however, Pesh council can require all data outsourced to public cloud storage should be in encrypted form. Through data confidentiality Tanvin obtains the necessary cryptographic keys to encrypt the data and later perform analysis over encrypted data.

vi) Data Anonymization

For accurate and efficient data analysis it is very important the service providers process and access that sensed in a convenient way. However, there are caveats in doing so as private and personal data can end up in the hands of users or service providers having malicious intents. Data anonymization offers the convenience of processing sensed data at the same time it also ensures the inhabitants are decoupled with the sensed data. This significantly reduces the possibilities of privacy infringement as without correct mapping information data cannot be traced back to its data owner or concerned stakeholder. It also assists service providers to explore new business possibilities by sharing anonymised sensed data with other service providers.
Pesh council can permit Tanvin to sense a user's vital signs (i.e., blood pressure, glucose level, respiratory rate). However, when stored in an untrusted domain these vital signs should not reveal the health of the associated inhabitant. Since Tanvin process streams of sensed data it is computationally infeasible to encrypt the sensed data and process it in a concealed form. Data anonymization assists Tanvin in storing and processing vital signs without compromising privacy. For each user it assigns a randomized pseudonym and also replaces specific values with range values, which restrain malicious entities to link private and confidential data with the inhabitant. The mapping between real and randomized information is stored in a secure location.

4.3. Service provider

This layer of our proposed framework is designed to deal with service provisioning and secure and privacy-aware data sharing in an untrusted domain. It enables service providers to collaborate on public and citizen data to find new possibilities of service provisioning consequently elevating life experiences in smart cities.

i) Service & Application Provisioning

This component represents the execution environment for services in smart cities. It can be regarded as a public cloud management portal enabling service providers to manage their

services. Service providers can scale their services according to their network and computational load.

ii) Data repositories

This component enables service providers to access public data repositories and also to share application/services specific data with other service providers. Since public cloud computing is utilized to persist, process and provision data, security and privacy measures are employed to prevent illicit data access. These measures include encrypted data search and processing in an untrusted domain, fine-grained control over shared data, guaranteed user revocation, and secure key management. These measures enables service providers to securely collaborate with each other whilst maintaining control of their data without relying on untrusted cloud service provider.

For example in the aforementioned scenario Tanvin can access open government transport data to provision a bus route recommendation service. It future post-processing of the data, identifying the most frequently used bus routes depending upon inhabitants' occupations and demographic it can then securely share its processed data with other service providers who are interested in such analysis. Since Tanvin does not want any illicit data access, it shares the encrypted data through public cloud storage services. Authorised service providers can then search, access and consume their shared data accordingly to their access privileges, where necessary cryptographic keys and access token are maintained by Tanvin.

iii) Application programming interface

This framework leverages service providers to open an application programming interface to their business logic and accumulate application/specific data, whilst maintaining fine-grained control over accessibility. It also maintains an access log to ensure that every access request is recorded. It serves two purposes, billing service providers with respect to number of access requests and audit trail in case of illicit or malicious access.

For example, Tanvin develops a localization algorithm based upon an inhabitant's mobile phone and Wi-fi signals. Tanvin provides an application programming interface, which triangulates an inhabitant's location with a precision of a couple of meters. Its algorithm can be utilized by other service providers to develop auxiliary recommendation services e.g., restaurant, hotels, tourist attractions. To ensure the application programming interface is used by authorised service providers only, Tanvin issues verifiable cryptographic access token and maintains an access log. Access tokens are valid for a specific period of time, and once revoked subscribers would not be able to use application programming interface.

5. Proof of Concept through Automated Verification

As a proof of concept, an automated verification tool, namely 'Scyther'[10] is used to verify selected architectural components and security protocols. The verification model aims to protect private and confidential data of citizens. Mainly three components of the SSServProv framework are verified against different types of security vulnerabilities. These components are: i) authentication protocol, ii) secure communication protocol and iii) protection of services and applications. These components (i) and (ii) are represented in the proposed architecture (Fig. 3) as 'Authentication' and 'Services and Applications' in smart city and infrastructure layer and (iii) represents flow of information between different layers.

In order to fully understand verification models and acquired outputs, the following Fig. 5 illustrates a basic open data scenario adapted from an open governance use case (Section 4). In Fig. 5, potential security attacks and verified proposed solutions are shown when different actors are communicating and/or accessing resources. For example, Pesh council authorise Tanvin's Smartizen app to access specific resources e.g. city data. Different stakeholders e.g. citizens and local businesses can register with the Smartizen app. The app verifies registration credentials through Pesh council and resource permissions are updated in the user permission database. When a user login, the Smartizen app authenticates user credential through Pesh council's authorised users database. Smartizen app ensures that trusted module is not tampered and provides different services to authenticated and authorised users. For example, users can collect data or provide new data to be stored through Smartizen app. The Pesh council collects data through different data sources e.g. sensors, city data repositories, and manages it using Zebr cloud. All data communication between data sources and Zebr cloud is performed using secure communication protocol. Smartizen app also provide Open API service for application developers or service providers. Like citizens, service providers or application developers can register with the Smartizen app and their credentials are verified through Pesh council's legitimate service provider component. They can collect data through Smartizen app and can develop new apps which can communicate with Zebr cloud for data provision using secure communication protocol.

[10] Scyther Tool: https://www.cs.ox.ac.uk/people/cas.cremers/scyther/ . (Accessed: 22 May 2017)

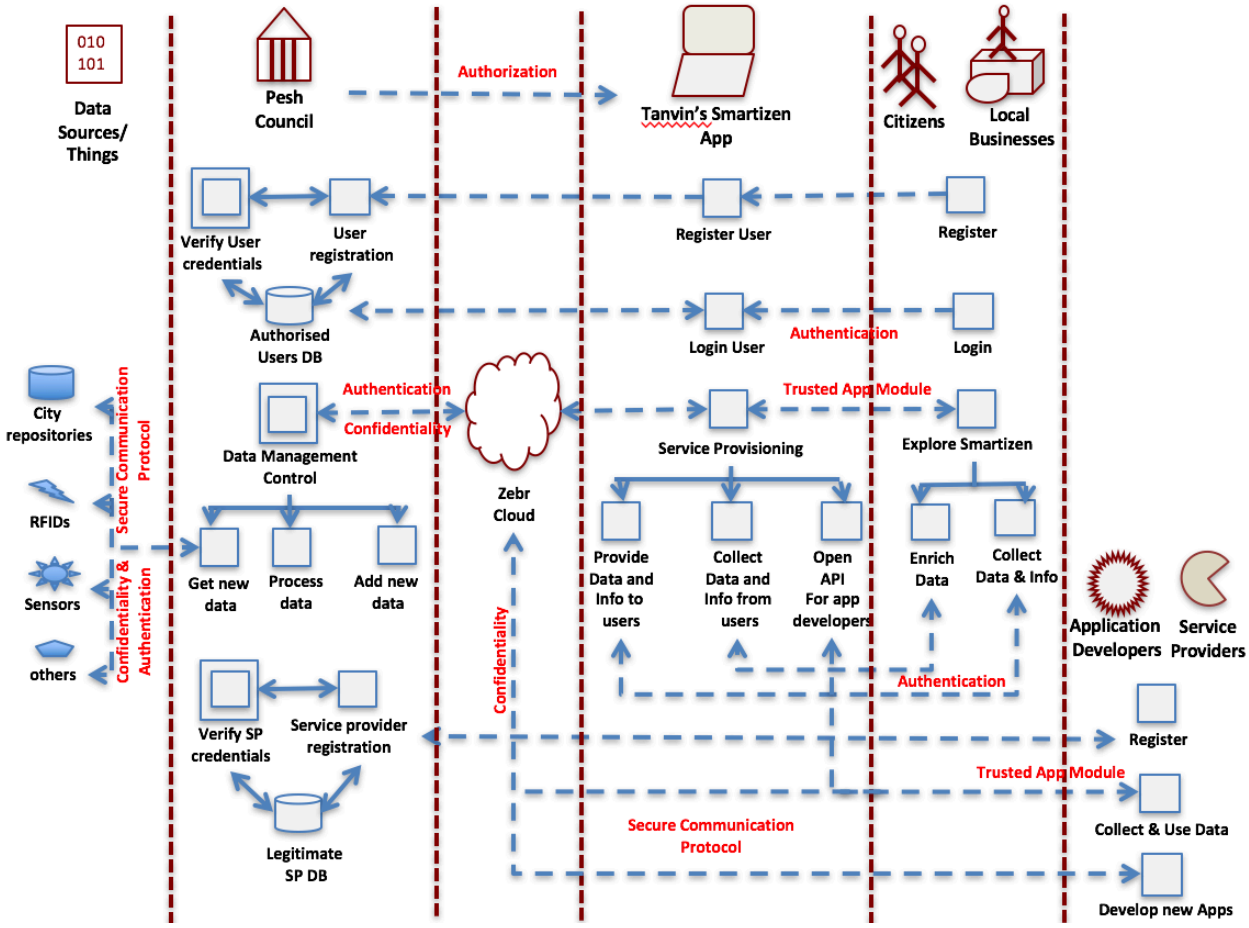


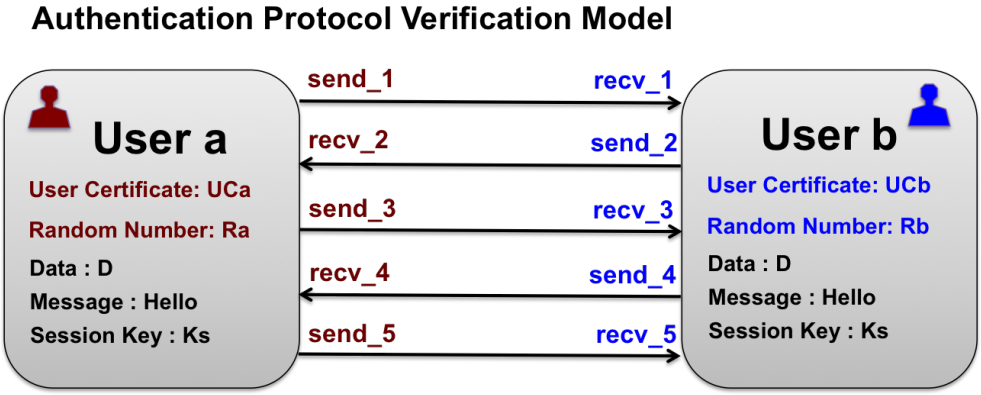
Fig. 5: A generic open data based scenario

The above potential security attacks and solutions are modelled in Scyther and verified revealing reliability of the above components. For authentication, it is assumed that most of the entities or actors involved in a smart city ecosystem authenticate each other before starting actual communication. For authentication, we implemented a certificate based authentication protocol [27]. For secure communication Secure Socket Layer (SSL) and newly designed secure communication protocol for securely fetching data from different sources including connected repositories and/or sensors is used. Since these data sources have different capabilities and/or properties we designed a secure communication protocol by considering their computing power and other resources. SSL is selected as it is a well-accepted standard web protocol for secure communication. In this section we modelled and verified authentication protocol, designed protocol for protection of services & applications; and verified secure communication protocol

between low-end devices and services.

5.1. Authentication Protocol

In an ideal environment, most of the devices and clients in smart city ecosystem possess certificates from a certified authority e.g. components in governmental control domain layer of the SSServProv framework. Such devices and users use these credentials for strong authentication using certificate based an authentication protocol, as discussed above. This certificate based authentication protocol can be considered an extension of FIPS-196. Various steps involved in strong authentication process are described in the formal language presented in Annex-C.1, that is modelled and verified by Scyther, an automated formal verification tool for security protocols. Fig. 6 illustrates the authentication verification model and shows communication between two entities (users or devices) which then undergo number of injected attacks.



Attack Injection Model: **(Alive, Weakagree, Niagree, Nisynch, Commit)**

Fig. 6: Authentication Protocol Verification Model

In the literature, *man-in-the-middle, replay attack, message tampering, and information leakage (identity)* are some of the potential attacks that can be launched on an authentication protocol. Therefore, from the sender's point of view, we specified following claims in the verification model (Fig. 6) to analyse the behaviour of our designed authentication protocol against above mentioned attacks.

claim(Ua,Alive);
claim(Ua,Weakagree);

claim(Ua,Commit,Ub,Hello);
claim(Ua,Commit,Ub,Hello);
claim(Ua,Niagree);
claim(Ua,Nisynch);

The claim Weakagree is essential to check if authentication is successful. The claim with attribute *Nisynch* provides the verification that the messages are received from a legitimate sender in the specified sequence e.g. in the above illustration, a Citizen registration message to Smartizen and Pesh Council. Since, in our protocol, we encrypted the challenge using the private key of the sender so only the corresponding public key can be used to extract the challenge. In our implementation, this public key is encapsulated in certificate with identity of the owner. Therefore, the creator of messages can be easily verified using certificate verification function.

The attribute *Alive* is another claim which is used to verify the aliveness of the system. This property shows that the messages exchanged between authentication parties are consistent and not tampered by the adversary to include its own challenge e.g. communication between service developers and smartizen through APIs. In our used protocol, challenge numbers are digitally signed which holds the properties of tamper resistance and source authentication.

The attribute *Niagree* ensures that the sender and receiver both are agreed to exchange the messages safely and according to the predefined sequence e.g. data management between Pesh council and Zebr cloud.

We also analysed through Scyther that our protocol satisfied the *Commit* attribute which shows that the designed protocol confirms the correct response received from authenticating party on corresponding running event e.g. login activity by business organizations to access Smartizen.

The verified results of the above mentioned properties are shown in Fig. 7. The results show that the authentication protocol satisfied all properties and resists against *man-in-the-middle, replay attack, and message tampering*. This authentication protocol does not preserve the privacy of the user so during authentication an attacker can extract the identity of the users. For this it is recommended that instead of using an identity based certificate, an *anonymous certificate* may be used but the sequence and procedure of the protocol remains same.

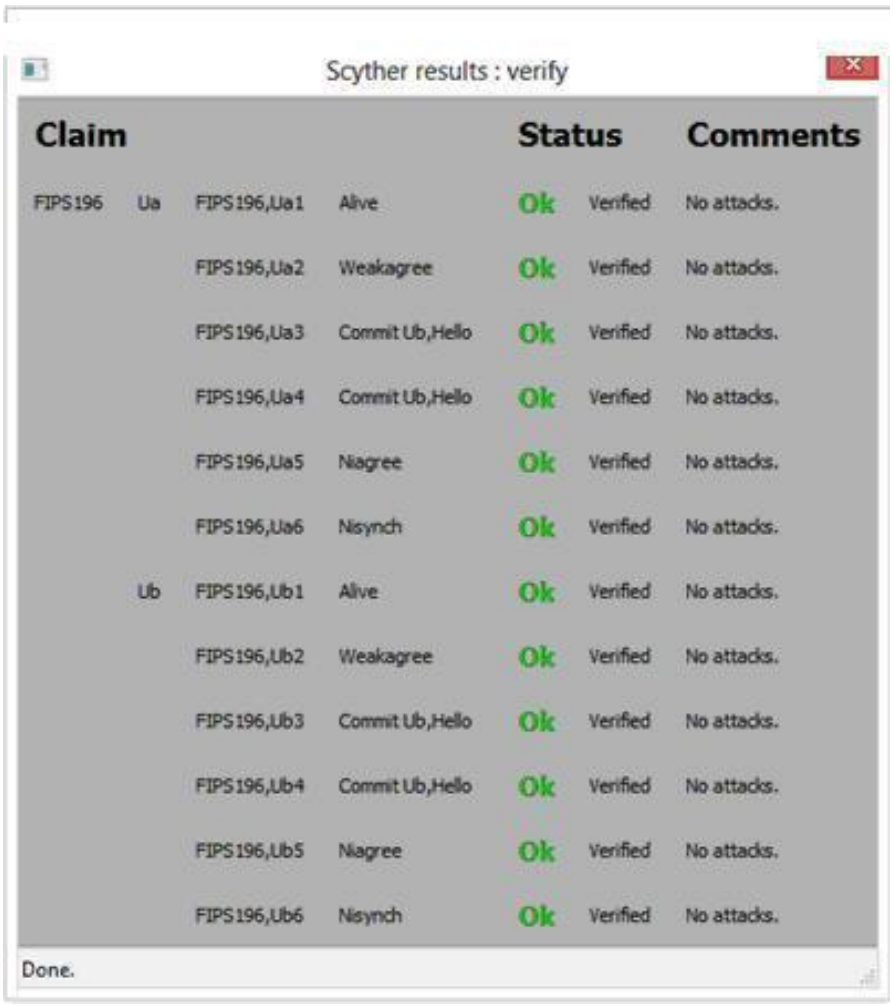


Fig. 7: Scyther based verification results for authentication protocol

5.2. Lightweight Secure Communication Protocol

A smart city service client machine may have different capabilities. For example, a user can use their mobile device for fetching healthcare related information or any other service through a Smartizen app. Another may use his laptop to fetch tax related information. So based on their capabilities we defined two different secure communication protocols. If a device has limited resources then a user may use username and password for initial authentication and then exchanges secure session key to send encrypted messages. If a user already has credentials then he/she may use Strong Authentication for authentication and then use asymmetric key

cryptography to share session key. Fig. 8 illustrates secure communication protocol verification model that uses three roles service provider and two sensors (or service consumers i.e. devices or users). The complete protocol is further modelled in Scyther for model verification and presented in Annex-C.2.

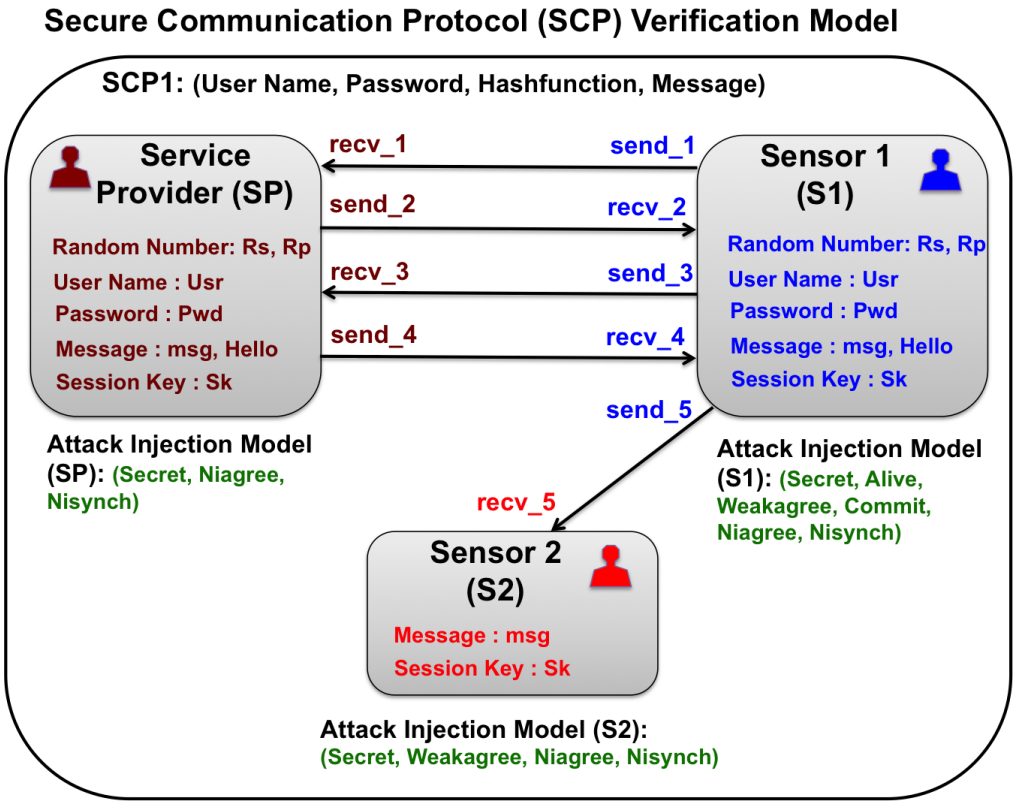


Fig. 8: Secure Communication Protocol Verification Model

The verification result of the above specified secure communication protocol is shown in Fig. 9. This figure shows that our secure communication protocol ensures the privacy of the Session Key (Sk), Service Provider and Sensor (or device) Challenges, that is, Rp and Rs respectively, during the execution of the protocol. Furthermore, the *aliveness* claim of the protocol describes that the communicating entities response could not be tampered which is considered the basic property of a good authentication protocol. The *Commit* claim shows that both Sensor and Service Provider are receiving correct responses during the execution. The other property of the authentication protocol which protects the system from replay attack as shown in the *Synchronization* claim. The *Secret* property shows that the message is secure between sensor and service provider. If a user

has digital certificates then he/she uses RSA keys to share the session key and then uses the above process to exchange secure messages.

Fig. 9: Scyther based verification results for secure communication protocol

5.3. Protection of Services & Applications

In the SSServProv framework (Fig. 4), the trusted platform/module (in the services and

application component of the smart cities inhabitants/infrastructure layer) keeps a copy of hashed libraries in local storage which is only accessible to the authenticated users. If the owner of services and applications is interested to ensure the integrity of their libraries, then he/she sends a request to the verifier module which generates the digital signature of all libraries and classes of used services and applications. After that it sends this digital signature to the trusted module which extracts the hash value and if the hash value is not same then it sends a request to the verifier to generate an alarm for possible tampering in the services and applications modules. In the above scenario, they use a digital signature technique which is already verified against well-known attacks in above verification steps. The trusted platform/module will be integrated in sensing and actuating devices deployed by a service provider, ensuring security of the device.

5.4. Enforcing XACML based Access Control policies

Role based access control, RBAC [20], can be directly mapped on the roles identified in the onion model (Fig. 1). In this regard, we implemented such roles and associated policies in XACML which are used by the PDP for access control decisions and enforced by the PEP. In this paper, we present simple examples of the definition of roles, associated access control policy sets and their enforcement using access tokens acquired during our authentication process (as shown in Fig. 6) to show *Permissions* and *Roles* policy sets for different actions and resources. In the following examples, the service provider role is authorised to send requested report whereas service consumer role is authorised to request a resource (or report).

Role policy set for service provider - An Example

```
<!-- Role <PolicySet> for Service Provider role -->
<PolicySet PolicySetId="RPS:serviceprovider:role">
        <Target>
                <Subjects>
                        <Subject>
                                <SubjectMatch MatchId="&function;anyURI-equal">
                                        <AttributeValue DataType="&xml;anyURI"> &roles;serviceprovider
                                        </AttributeValue>
                                        <SubjectAttributeDesignator AttributeId="&role;" DataType=
                                        "&xml;anyURI"/>
                                </SubjectMatch>
                        </Subject>
                </Subjects>
        </Target>

        <!-- Use permissions associated with the service provider role -->
        <PolicySetIdReference>PPS:serviceprovider:role</PolicySetIdReference>
</PolicySet>
```

Role policy set for service consumer - An Example

```
<!-- Role <PolicySet> for Service Consumer role -->
<PolicySet PolicySetId="RPS:serviceconsumer:role">
        <Target>
                <Subjects>
                        <Subject>
                                <SubjectMatch MatchId="&function;anyURI-equal">
                                        <AttributeValue DataType="&xml;anyURI">&roles;serviceconsumer
                                        </AttributeValue>
                                        <SubjectAttributeDesignator AttributeId="&role;" DataType=
                                        "&xml;anyURI"/>
                                </SubjectMatch>
                        </Subject>
                </Subjects>
        </Target>

        <!-- Use permissions associated with the service consumer role -->
        <PolicySetIdReference>PPS:serviceconsumer:role</PolicySetIdReference>
</PolicySet>
```

Another working example is provided in Annex-B, where service provider-consumer permission policy set is used by the Pesh City Council to define access rights of consumer and services providers e.g., to send/open various activities of citizens like calories-count for their exercise routines.

We opted for component based testing/verification approach to ensure that individual components work properly and are providing required functionality under different security settings. These components have to be integrated to provide end-to-end security. It is our assumption that chaining these components into a workflow should logically provide the desired results. This means that once authenticated, a user should be able to use lightweight secure communication protocol to get access to resources based on the authorisation protocol. The protection of services and applications protocol ensures that any tampering with applications or services are notified to service providers.

These verification components are directly mapped to different components of the SSServProv Framework. The authentication protocol maps to the authentication component in the smart cities/inhabitants Infrastructure layer and ensures that users or other services at authenticated. The services and applications protocol maps to the services and applications component of the smart cities/inhabitants infrastructure layer to ensure that trusted module can detect any illegitimate tampering to services or applications. Similarly, the authorisation protocol maps to the authorisation component of the same layer to ensure that only authorised users should be able

to access specific resources e.g. services or applications. The lightweight secure communication protocol is followed for intra and inter layer communication to ensure protected data exchange. Though these verified components cover only selected components of the SSServProv framework, they provide reasonable proof of concept towards ensuring end-to-end security of smart city services. A fully implemented framework will be covered as part of the future work.

6. Related Work and Discussion

Smart city solutions where citizens also play a major role in data collection are implicitly expected to be secure and preserve users' privacy and establish trust on technological innovations in an urban living environment. Most of the related work presented in this section indicates that other researchers has dealt with various aspects of security, privacy and trust individually but a holistic approach to deal with smart cities based data security, privacy and trust issues is missing. In contrast to conventional smart city security and privacy frameworks, SServProv as a whole ensures confidentially of the smart cities' sensed, persisted and processed data, ensuring end-to-end security. It provides authentication for service providers and subscribers, warranting legitimacy of the services and gathered inhabitants' data. With SServProv, privacy of the smart city inhabits remains intact and services are provisioned in compliance with validated service manifesto, consequently ensuring higher level of trust amongst service providers, inhabits', smart city's stakeholders. We present related work with the objective to assess the effectiveness of our proposed framework as summarised in Table 1 (Annex-A).

In [28] and [29], other researchers highlight trust, privacy and security issues related to IoTs in smart city context and present various solutions provided by different previous and on-going projects e.g. iCore Access Framework, IoT@Work CapBAC, GAMBAS Adaptive middleware, IoT-A, SMARTIE, etc which provide useful insights about IoT related security and privacy issues in smart cities. Some of these are presented in this section.

In [30], researchers highlighted security and privacy concerns which may arise due to smart software applications in a city environment. They highlighted sensor tracking, hacking, data source authentication and exchange of data between devices over unsecured network as potential security issues that may lead to smart city software security and privacy aspects. Authors concluded that smart software should only be used if software operations and network communication is secured. However, three component based security model presented by authors is too obscure to cover all identified security and privacy issues in smart cities ICT infrastructure and applications.

In [31], authors highlighted data security, authorisation and privacy issues that can arise in an integrated city management platform which uses various ICT technologies such as Internet of Things (IoT), cloud etc. In particular they highlighted cloud security issues including service availability, authorisation, access, audit, monitoring, secure transmission, viruses and risks from other users of the cloud system. Their proposed security strategy attempts to deal with the abovementioned security threats by applying various information security techniques such as encryption, authentication access. However, authors' proposed security model for management system of a smart city does not clearly indicate how necessary information about security measures can be applied at different levels of governance by acquiring and sharing cross-departmental data for necessary information processing and decision making in a city environment.

In [32], researchers mainly proposed an open sensor cloud platform to facilitate use of IoT for smart city applications. Suciu [32] argued for cloud and IoT paradigms integration and emphasised on privacy management in cloud environment. However, the proposed framework do not explicitly cover security and privacy aspects.

In [33], authors highlighted the importance of handling security and privacy challenges of smart cities right from the beginning. The authors discussed key challenges, emerging technologies and issues to watch. In their work the authors advised that by introducing strict security standards on new technologies most of the security and privacy issues can be resolved. They also suggested that private and confidential information must be decoupled from its owner in order to avoid any privacy infringement; thus, in case of a successful attack compromised data can be trace backed to its owner – consequently ensuring user's privacy. The authors presented security and privacy issues in Smart grid environment. They identified privacy as the most critical issue that must be addressed. They emphasized on the importance of configurable privacy settings – putting users in control of their data according to their preferences. Network connectivity is also considered as an issue having serious consequences on users' privacy. The authors pointed out that private communication can provide protection against most attacks; however, it is not feasible since isolated systems cannot offer personalized services to the inhabitants of a smart city. It is also presented that smart city prophecies the concept of system-of-systems; however, it significantly increases the number of vulnerabilities in a final system then each of the participating sub-system. The authors also highlighted that availability of services is a key challenges as adversary can prevent authorised users from consuming services by launching denial-of-service attacks. The authors also suggested that scalability of key management solutions is very important as in Smart city millions of sensing devices would be spread across hundreds of organizations. A key management solution that can keep track of skewed keys and issue legitimate access key would

play a critical role in securing private and confidential information.

In [34], authors suggested that ability of a Smart city to gather unprecedented amount of data and massively deployed sensing devices connected through heterogeneous networks are main causes of citizen privacy. The authors claim that privacy is a fundamental right of a citizen, the success of smart cities is directly associated with it. In their work the authors highlighted that existing privacy preserving methodologies can be employed to ensure citizen privacy. Techniques like statistical disclosure can be employed to allow release of data for secondary use. Similarly, private information retrieval methodologies can be used to access data without revealing data access pattern to data custodian and privacy-preserving data mining can leverage collaborative service providers to learn interesting pattern from each other's data without compromising privacy of the involved entities. Location privacy and pseudonym can be employed to ensure service provider cannot relate private and confidential data with the data owner (i.e., data owner). Privacy in RFID and video surveillance can be utilized to realize Smart city ecosystem in which sensing devices and actuators cannot be exploited to compromise privacy of its inhabitants. Based on existing models of database privacy [35] and location based service privacy [36], the authors proposed 5D model for privacy in smart cities – encompassing five dimensions of identity, query, location, footprint and owner privacy. The authors highlighted the fact that the existing technologies can be leveraged to ensure privacy in all of those fundamental dimensions. For instance, users' identities can be protected if geographically separated pseudonymizers are used. Similarly, user queries can be secured by the use of private information retrieval. Location and footprint privacy can be ensured by masking user's location and statistical disclosure of information respectively. Owner privacy can be achieved by the means of privacy-preserving data mining and even by the use of statistical disclosure of information.

Smart cities are driven by the advancements in information and communication technologies. In [37], researchers highlighted the fact that these advancements put security of citizens at risk and most importantly challenges the privacy expectations of Smart city's inhabitants. The authors pointed out that with massively connected environments the societies are embracing full-connectivity namely "Internet-of-things". There are unprecedented opportunities to improve quality of life, city infrastructure, intelligent transport system to name a few. However, the authors argue that hidden in this full-connectivity, citizens are inadvertently sharing data about their location and activity; in such a case, privacy seems to be disappearing. To ensure citizen privacy the authors presented an interaction model involving smart cities entities namely: persons, servers and things. The interaction model is described as a graph whose vertices are involved entities. The authors emphasised on the fact the stronger privacy and security mechanisms are needed to protect edges interconnecting vertices. In their work the authors identified that in Smart

cities not only private and confidential data is at risk, security of its inhabitants faces escalating challenges. This is because malicious service providers can collude to exploit available information inadvertently shared by the inhabitants.

IoT@Work [38] project aims at developing IoT-based plug and play concept on industrial automation. Due to potentially unbounded number of IoT (resources and objects) and more fine-grained control requirements over service orchestration, Access Control List based authorisation frameworks are not scalable. This project envisions Capability based Authorisation framework for IoT, having support for capability delegation, revocation and information granularity. Unlike conventional authorisation frameworks Capability based Authorisation can adopt to collaborative environment enabling data / service owners to define multiple level of capabilities handling access requests from different users. IoT@Work defines functional element of capability based authorisation as: resources, authorisation capability, capability renovation, operation request, resource Policy Decision Point, resource manager and revocation service. For privacy consideration within untrusted network / collaboration IoT@Work supports Encrypted Capability Chain and Anonymous Capabilities.
SMARTIE project[11] [38] has ambitious objectives and aims to provide a distributed framework for sharing large scale smart city heterogeneous data from multiple sources by ensuring security, privacy and trust in information to promote reusability across multiple applications. SMARTIE provides a layered architecture (applications, information services, network, smart objects) for smart cities applications (transport, energy, public safety, utilities etc) and different security, privacy and trust related requirements are identified. SMARTIE project aim to build on existing solutions from UbiSec&Sense, SENSEI etc. They identify various techniques for trust (e.g. transitive trust, FAIR - fuzzy-based aggregation providing in-network resilience, two-step aggregate-and-confirm approach), privacy (authorisation and authentication mechanisms including policy language, minimal disclosure technique), security (e.g. SPINS protocols for confidential communication and authenticated broadcast in wireless sensor networks, lightweight cryptography techniques due to resource constraints of IoT e.g. asymmetric cryptography etc).

Internet of Things Architecture (IoT-A) [38] project proposes a dynamic and flexible architecture allowing determining new IoT resources at runtime and hence needs necessary level of security measures. IoT-A aims to adapt different solutions from wireless sensor networks to flexibly support multiple possible IoT scenarios. The project introduces a secure and trustworthy resolution infrastructure to support resolution of names & identities to addresses and locators used by the services in an IoT environment. Others [39] have defined number of security requirements for system dependability, communication structure and user & service privacy. At

[11] SMARTIE: http://www.smartie-project.eu/ . (Accessed: 22 May 2017)

the core of IoT-A security functionalities, there are five logical security components: Authorisation, Authentication, Identity Management, Key Exchange and Management, and Trust & Reputation. For example, the authorisation component is used to perform access control decisions based on access control policies and models (e.g. role based access control model or attribute based access control model) implemented in eXtensible Access Control Markup Language (XACML) - a policy decision language based on XML and standardised by OASIS. Also, it defines a Policy Administration Point interface that allows any new service to register with resolution infrastructure. Like any typical security model Authentication is also one of the necessary component of IoT-A resolution infrastructure implemented in Security Assertion Markup Language (SAML). For Identity management, IoT-A issues Pseudonyms and accessory information to trusted subjects so that they can operate anonymously. IoT-A's Key Exchange and Management component ensures secure communication between two or more IoT-A peers including users and service e.g. by setting up tunnel between gateways. IoT-A's adopts a generic trust and reputation architecture which consists of five steps: gathering information, scoring & ranking entities, entity selection, transaction and rewarding & punishing entities.

7. Conclusions and Future Work

This paper presents a detailed security and privacy concerns for smart city stakeholders – service providers, service consumers (citizens) and governing bodies. The security and privacy threats we are explicitly presented from each stakeholder's point of view; careful analysis of these treats fed in the proposed service provision framework for smart city. The stakeholder onion model identifies different stakeholders' roles and actors which help in deriving different components of the 'Smart Secure Service Provisioning' (SSServProv) Framework. The SSServProv framework focuses on end-to-end security and privacy covering the entire service provision model of smart cities. The framework is designed to ensure only legitimate service providers can provision their services; whilst ensuring citizen private and sensitive data is never compromised. Similarly, the framework also protects services from being compromised by malicious citizen – ensuring service providers are making use of accurate citizen data to curate services.

The layered architecture of the SSServProv framework is flexible and hence can be scaled to handle various smart city security scenarios. The efficacy of the proposed framework is tested in Scyther verification tool for the selected components of the SSServProf framework: authentication, light weight secure communication protocol and protection of services and applications using trusted module against different security attacks. Also, XACML based role and permission sets are defined and used with SAML for resource authorisation. These automated verification results are promising as they indicate successful service provisioning in the presence

of selected security threats. Whilst these tests results of individual components prove usefulness of the framework to a certain extent, more testing and verification of all integrated components of SSServProv framework will provide more sound basis for adoption and development in a smart city infrastructure. For the future research work, the authors will extend this framework to configurable security and privacy services. The focus will be on services that can comply with evolving government regulations considering new technological advancements and escalating cyber security threats.

Acknowledgement
Icons used in Fig. 2 and 3 are provided by The Noun Project at https://thenounproject.com/, distributed under creative common license. We also acknowledge Professor Bull of the University of X for proof reading this paper.

Conflict of interest
All authors declare that there is no conflict of interest.

Contributors
First author initiated this collaborative research and presented security and privacy issues in the context of smart cities, defined stakeholder onion model and open governance use case that sets the basis for the development of SSServProv framework. Second author described security challenges of smart city in detail along with the development of SSServProv framework. Both first and second authors presented related work to identify gaps in existing solutions. Third author contributed to various components of SSServProv framework and developed and presented proof of concept for framework verification. First author also illustrated verification models which are used to develop proof of concept and finalised the manuscript.

References
[1] D. Christin, A. Reinhardt, S. S. Kanhere, M. Hollick, A Survey on Privacy in Mobile Participatory Sensing Applications, Journal of Systems and Software, 84(11), 2011, 1928-1946. DOI: 10.1016/j.jss.2011.06.073, ISSN: 0164-121
[2] Z. Khan, D. Ludlow, W. Loibl, K. Soomro, ICT enabled participatory urban planning and policy development: The UrbanAPI project. Transforming Government: People, Process and Policy, 8 (2). 2014, 205-229. ISSN 1750-6166
[3] Z. Khan, S. L. Kiani, K. Soomro, A framework for cloud-based context-aware information services for citizens in smart cities. Journal of Cloud Computing: Advances, Systems and Applications, 3, 2014, ISSN 2192-113X
[4] Z. Khan, A. Anjum, K. Soomro, M. Tahir, Towards cloud based big data analytics for smart

future cities", Journal of Cloud Computing: Advances, Systems and Applications 4:2, 2015. doi:10.1186/s13677-015-0026-8
[5] Y. I. Cho, Designing smart cities: Security issues. In Computer Information Systems and Industrial Management. Proceedings of 11th IFIP TC 8 International Conference, CISIM 2012, Venice, Italy, September 26-28, 2012, pp. 30-40, Springer Berlin Heidelberg.
[6] E. De Cristofaro, C. Soriente, Participatory Privacy: Enabling Privacy in Participatory Sensing, IEEE Network, pp. 32-36, 2013.
[7] M. Ouedraogo, S. Mignon, H. Cholez, S. Furnell, E. Dubois, Security transparency: the next frontier for security research in the cloud, Journal of Cloud Computing: Advances, Systems and Applications, 4:12, 2015, doi:10.1186/s13677-015-0037-5.
[8] T. K.L. Hui, R. Simon Sherratt, DD. Sánchez, Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies, Future Generation Computer Systems, Available online 1 November 2016, ISSN 0167-739X.
[9] R. Roman, J. Lopez, M. Mambo, Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges, Future Generation Computer Systems, Available online 12 November 2016, ISSN 0167-739X.
[10] Executive Report (2013): Smart Cities. "Transformational 'smart cities': cyber security and resilience". Symantec 2013. (Accessed 9 Nov 2015), URL: http://eu-smartcities.eu/sites/all/files/blog/files/Transformational%20Smart%20Cities%20-%20Symantec%20Executive%20Report.pdf
[11] World Economic Forum (2012): Risk and Responsibility in a Hyperconnected World Pathways to Global Cyber Resilience (2012), (Accessed: 9 Nov 2015), URL: http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf
[12] J-M. Bohli, P. Langendorfer, A. Skarmeta, Security and Privacy Challenge in Data Aggregation for the IoT in Smart Cities, In Vermesan. O, Friess, P., (Eds) Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, p.p 225-244. 2013. River Publishers.
[13] Correia L M., Wünstel, K. (Eds), (2011), Smart Cities Applications and Requirements, White paper, Net!Works Europea n Technology Platform. (Accessed 22 May 2017), URL: http://grow.tecnico.ulisboa.pt/wp-content/uploads/2014/03/White_Paper_Smart_Cities_Applications.pdf.
[14] UN Habitat report, (2011), Cities and Climate Change: Global Report on Human Settlements, United Nations Human Settlement Programme. (Accessed: 9 Nov 2015), URL Access: http://unhabitat.org/books/cities-and-climate-change-global-report-on-human-settlements-2011/
[15] EEA (2006), European Environment Agency, Urban sprawl in Europe – The ignored challenge. Office for Official Publications of the European Communities, 2006, ISBN: 92-9167-

887-2. (Accessed: 9 Nov 2015), URL Access:
http://www.eea.europa.eu/publications/eea_report_2006_10
[16] A. Urbieta, A. González-Beltrán, S. Ben Mokhtar, M. A. Hossain, L. Capra, Adaptive and context-aware service composition for IoT-based smart cities, Future Generation Computer Systems, Available online 2 January 2017, ISSN 0167-739X,
[17] A. Abella, M. Ortiz-de-Urbina-Criado, C. De-Pablos-Heredero, A model for the analysis of data-driven innovation and value generation in smart cities' ecosystems, Cities, Volume 64, April 2017, Pages 47-53, ISSN 0264-2751.
[18] H. Ben Sta, Quality and the efficiency of data in “Smart-Cities”, Future Generation Computer Systems, Available online 26 December 2016, ISSN 0167-739X,
[19] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, X. Yi, Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation, Future Generation Computer Systems, Available online 18 March 2017, ISSN 0167-739X.
[20] RBAC, Core and hierarchical role based access control (RBAC) profile of XACML v2.0, OASIS Standard, 1 February 2005. Last Accessed: 12 November 2016. URL Access:
http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf
[21] I. Alexander, A taxonomy of stakeholders: Human Roles in System Development, International Journal of Technology and Human Interaction, 1(1), 2005, pp.23-59.
[22] IBM, (2011), IBM Big Data Success Stories - A note from Rob Thomas, Last Accessed: 9 Nov 2015 http://public.dhe.ibm.com/software/data/sw-library/big-data/ibm-big-data-success.pdf
[23] S. Dawn Xiaoding, D. Wagner, A. Perrig, Practical techniques for searches on encrypted data, Security and Privacy 2000 (S&P 2000).
[24] Z. Pervez, M. Ahmad, A.M. Khattak, S. Lee, T.C. Chung, Privacy-aware relevant data access with semantically enriched search queries for untrusted cloud storage services, PloS one 11.8 (2016): e0161440.
[25] Smarticipate project, smart open data services and impact assessment for open governance, H2020 European Commission Grant Agreement: 350460. (Accessed: 22nd May 2017), URL Access: https://www.smarticipate.eu/
[26] IES Cities project, Internet-Enabled Services for the Cities across Europe, FP7 European Commission Grant Agreement: 325097.
[27] A. G. Abbasi, S. Muftic, Cryptonet: security management protocols, published in the proceedings of the 9th WSEAS international conference on Data networks, communications, computers, World Scientific and Engineering Academy and Society (WSEAS), 2010, Faro, Portugal.
[28] O. Vermesan, P. Friess, P. Guillemin, H. Sundmaeker, M. Eisenhauer, K. Moessner, F. Le Gall, P. Cousin, Internet of Things Strategic Research and Innovation Agenda, Eds: O. Vermesan, P. Friess, Internet of Things: Converging Technologies for Smart Environments and

Integrated Ecosystems, River Publishers. p.92-95, 2013. (Accessed 22 May 2017). URL Access: http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf Last Accessed 9 Nov 2015.
[29] G. Baldini, T. Peirce, M. Handte, D. Rotondi, S. Gusmeroli, S. Piccione, B. Copigneaux, F. Le Gall, F. Melakessou, P. Smadja, A. Serbanati, J. Stefa, Internet of Things Privacy, Security and Governance, Eds: O. Vermesan, P. Friess, Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, River Publishers. p207-241, 2013, URL Access: http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf Last Accessed 9 Nov 2015.
[30] M. Sen, A. Dutt, S. Agarwal, A. Nath, Issues of Privacy and Security in the Role of Software in Smart Cities, (2013), International Conference on Communication Systems and Network Technologies (CSNT), p.p. 518-523 6-8 April 2013, Gwalior.
[31] L. Wang, C. Jing, P. Zhou, Security Structure Study of City Management Platform Based on Cloud Computing under the Conception of Smart City (2012), Fourth Int. Conference on Multimedia Information Networking and Security (MINES), p.p. 91-94, 2-4 November 2012, Nanjng.
[32] G. Suciu, A. Vulpe, S. Halunga, O. Fratu, G Todoran, V. Suciu, Smart cities built on resilient cloud computing and secure internet of things, 19th International Conference on Control Systems and Computer Science (CSCS), p.p. 513-518, 29-31 May 2013, Bucharest, Romania.
[33] A. Bartoli, J. Hernández-Serrano, M. Soriano, M. Dohler, A. Kountouris, D. Barthel, Security and privacy in your smart city. In Proceedings of the Barcelona Smart Cities Congress, 29-2 December 2011, Barcelona, Spain.
[34] A. Martínez-Ballesté, A. Pérez-Martínez, A. Solanas, The pursuit of citizens' privacy: a privacy-aware smart city is possible, Communications Magazine, IEEE 51(6). 2013.
[35] J. Domingo-Ferrer, A three-dimensional conceptual framework for database privacy. SDM 2007, LNCS 4721, pp: 193-202, Springer Berlin Heidelberg. DOI: 10.1007/978-3-540-75248-6_14
[36] A. Pérez-Martínez, A. Solanas, W3-privacy: the three dimensions of user privacy in LBS, 12th ACM Int'l. Symp. Mobile Ad Hoc Networking and Computing. 2011, Paris, France, May 2011.
[37] A. Elmaghraby, M. Losavio, Cyber security challenges in Smart Cities: Safety, security and privacy, Journal of Advanced Research, Volume 5, Issue 4, July 2014, Pages 491-497, ISSN 2090-1232, http://dx.doi.org/10.1016/j.jare.2014.02.006.
[38] O. Vermesan, P. Friess (Eds), Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, River Publishers. 2013.

[39] A. Serbanati, A. S. Segura, A. Olivereau, Y. Ben Saied, N. Gruschka, D. Gessner, F. Gomez-Marmol, IoT-A, Internet of Things Architecture, Eds: N. Gruschka, D. Gessner, Project Deliverable D4.2 - Concepts and Solutions for Privacy and Security in the Resolution Infrastructure, Feb, 2012. (Accessed: 9 Nov 2015). URL Access: http://www.meet-iot.eu/deliverables-IOTA/D4_2.pdf

Annex – A: Table 1: Range of features in SServProv Framework

	Confidentiality	Encryption	Authentication	Availability	Access control	Authorisation	Security	Privacy	Trust	others
SSServProv Framework	✓	✓	✓	✓	✓	✓	✓	✓	✓	Stakeholder specific, and end-to-end security and privacy.
[30]	No related capability identified but it covers other aspects									Device vulnerability detection, Antivirus, Spam filter, and Firewall.
[31]		✓	✓		✓ (key-based)					Electromagnetic shielding, Key-based audit, and Antivirus
[32]								✓		
[33]				✓				✓ (decoupling private information from owner)		Key management
[34]	✓							✓		
[37]								x		
SMARTIE Project [38]		✓	✓			✓	✓	✓	✓	
IoT-A Project [38]			✓			✓	✓		✓	Identity and key management
IoT@Work Project [38]					✓	✓		✓		

Note: Tick (✓) indicates presence of a feature, an empty cell in the table presents absence of a particular feature.

Annex-B: Permission policy set for service provider and consumer- An Example

```
<Policy PolicyId="serviceconsumer-provider" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
  <Description>Service consumer-provider policy is used by the Pesh (City council) to define access rigths of consumer and services provides to send/open various activities of citizens like calories-count and their exercise routines</Description>

  <Target>
    <Subjects>
      <Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">serviceprovider</AttributeValue>
          <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </SubjectMatch>
      </Subject>
    </Subjects>
    <Resources>
      <Resource>
        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">calories-count</AttributeValue>
          <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </ResourceMatch>
      </Resource>
    </Resources>
    <Actions>
      <Action>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Send</AttributeValue>
          <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </ActionMatch>
      </Action>
    </Actions>
  </Target>

  <Rule RuleId="Rule1" Effect="Permit">
    <Description>permit basic rule</Description>
    <Target>
      <Subjects>
        <Subject>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
```

```
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">serviceprovider</AttributeValue>
        <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
      </SubjectMatch>
    </Subject>
  </Subjects>
  <Resources>
    <Resource>
      <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">exercise-routines</AttributeValue>
        <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
      </ResourceMatch>
    </Resource>
  </Resources>
  <Actions>
    <Action>
      <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">send</AttributeValue>
        <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
      </ActionMatch>
    </Action>
  </Actions>
 </Target>
</Rule>


<Target>
  <Subjects>
    <Subject>
      <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">serviceconsumer</AttributeValue>
        <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
      </SubjectMatch>
    </Subject>
  </Subjects>
  <Resources>
    <Resource>
      <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">exercise-routines</AttributeValue>
        <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
      </ResourceMatch>
    </Resource>
```

```
    </Resources>
    <Actions>
      <Action>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Open</AttributeValue>
          <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </ActionMatch>
      </Action>
    </Actions>
  </Target>
</Rule>

<Rule RuleId="Rule2" Effect="Permit">
  <Description>permit basic rule</Description>
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">serviceconsumer</AttributeValue>
          <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </SubjectMatch>
      </Subject>
    </Subjects>
    <Resources>
      <Resource>
        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">exercise-routines</AttributeValue>
          <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </ResourceMatch>
      </Resource>
    </Resources>
    <Actions>
      <Action>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Open</AttributeValue>
          <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </ActionMatch>
      </Action>
    </Actions>
  </Target>
</Rule>
</Policy>
```

In the above framework, we are following XACML based enriched authorisation solution, therefore Security Assertion Markup Language (SAML) Authorisation request and service response are also following the same rules. The SAMLAuthorisation request is simple but services response is cryptographically protected. It uses XML based security standard to protect SAMLAuthorisationResponse as show in the following examples.

SAML Authorisation request:

```
<Request>
  <Subject SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"   DataType=
                "http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>serviceconsumer</AttributeValue>
    </Attribute>
  </Subject>
  <Resource>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType=
                "http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>exercise-routines</AttributeValue></Attribute>
  </Resource>
  <Action>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType=
                "http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>Open</AttributeValue></Attribute>
  </Action>
</Request>
```

SAML Authorisation Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<Response xmlns="urn:oasis:names:tc:SAML:1.0:protocol" xmlns:samlp="urn:oasis:names:tc;SAML:1.0:protocol"
xmlns:xsd="http://www/w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/SMLSchema-instance"
IssueInstant="2016-07-23T21:01:35.921Z" MajorVersion="1" MinorVersion="1" Recipient="PEP"
ResponseID="IM1ISMNAUrnx">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <ds:SignatureMethod SignatureMethod="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <ds:Reference URI="#IM1ISMNAUrnx">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n" />
        </ds:Transforms>
```

```
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <ds:DigestValue>JV8eYPnHeh1A4ViSXoFMrkEQcDLx</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>

<ds:SignatureValue>nv0ZMjR1w/9grdi4l2llb0CWYMh/5y42LRbJmyNQx8pTEEWrRO6bv69kbkx+/EHeG+mkWE6OK
mlf0GkJGPsLabT/WUH2B54OaV3ZwtOI6G9r4HA50emrjcHWjQfSX2/Bp6Ot45SkO2Jb0A2FNMDdgOa1yZ53UrXSTe
lPajoU8EPx</ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data>

<ds:X509Certificate>MIIE8zCCBFygAwIBAgIBFTANBgkqhkiG9w0BAQUFADCBqTEMMAoGA1UEBhMDVVNBMQs
wCQYDVQQIEwJNRDEXMBUGA1UEBxMOTm9ydGggQmV0aGVzZGExJTAjBgNVBAoTHFNFVEVDUyBTZWN1cm
l0eSBUZWNobm9sb2dpZXMxHDAaBgNVBAsTE1NFVEVDUyBTZWN1cml0eSBVU0ExEzARBgNVBAMTCkxDQSB
TZXJ2ZXIxGTAXBglghkgBhvhCAQITCjEwLjAuMS4yNDAwHhcNMTIwMTIwMTcxOTA0WhcNMTMwMTE5MTcxOTA
0WjBlMQswCQYDVQQGEwJVUzEOMAwGA1UECBMFU29sbmExEjAQBgNVBAcTCVN0b2NraG9sbTEPMA0GA1U
EChMGU0VURUNTMQwwCgYDVQQLFgNSJkQxEzARBgNVBAMTClBEUCBTZXJ2ZXIwgZ8wDQYJKoZIhvcNAQE
BBQADgY0AMIGJAoGBAL2iY+Wy87ysRw/G1WVJNXgil52DKxO4he6VRL4XmV2AlacwS7vL2pPm/5C7KkOJwNzj7
MflXemQQz3f7XHwXKOtHOcdBr6eDsGXvM/0UdHpy8GeXFXOg6HQ1Ql4lVKt4RGpIr2UZAqBzfUsadLStG7E3xsRy
9iLh2lv8V44vaqBAgMBAAGjggJsMIICaDAOBgNVHQ8BAf8EBAMCBsAwDwYDVR0TAQEABAUwAwIB/zATBglghkg
BZQMGCQEBAQAEAwEBATBABgNVHREBAQAENjA0gTJMb2NhbCBDQSBTZXJ2ZXIsTmV0d29ya2luZyBEaXZpc
2lvbixTRVRFQ1MgSW5jLixVUzCBwwYDVR0jAQEABIG4MIG1oYGvpIGsMIGpMQwwCgYDVQQGEwNVU0ExCzAJ
BgNVBAgTAk1EMRcwFQYDVQQHEw5Ob3J0aCBCZXRoZXNkYTElMCMGA1UEChMcU0VURUNTIFNlY3VyaXR5IFRlY2hub2xvZ2llczEcMBoGA1UECxMTU0VURUNTIFNlY3VyaXR5IFVTQTETMBEGA1UEAxMKSENBIFNlcnZlcjEZ
MBcGCWCGSAGG+EIBAhMKMTAuMC4xLjI0MIIBATCBkQYDVR0gAQEABIGGMIGDMD8GCWCGSAFlAwEwATAy
MDAGCCsGAQUFBwIBFiRodHRwOi8vd3d3LnNldGVjcy5jb20vQ2VydFBvbGljeS5odG0wQAYKYIZIAWUCAQwBAT
AyMDAGCCsGAQUFBwIBFiRodHRwOi8vd3d3LnNldGVjcy5jb20vQ2VydFBvbGljeS5odG0wQAYDVR0SAQEABDYw
NIEyTG9jYWwgQ0EgU2VydmVyLE5ldHdvcmtpbmcgRGl2aXNpb24sU0VURUNTIEluYy4sVVMwPQYDVR0fAQEAB
DMwMTAvoi2kKzApMScwJQYJYIZIAYb4QgECExhsZGFwOi8vMTI4LjE2NC44Mi41MjozODkwEwYJYIZIAWUDBgkB
AQEABAMBAQEwDQYJKoZIhvcNAQEFBQADgYEAwInX8ATR22UqCN7qUV+Bhjx58BguA1RMuNhe1dKJcg4BXibf
TWPLpV/+h4cuFyo+0CD+CnW7EAOl0JggFZ0vrcigLNALiCwFpSIpKG+ECaOcwCKivGeRF69eMM9DTxyb2hlgwTs6
9/B0b+4XjG/wPP2vh15jcGq2qoWnB2nX3VDx|$|1|$|1271</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
 </ds:Signature>
 <Status xmlns="">
  <StatusCode Value="samlp:Success" />
 </Status>
 <Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion" AssertionID="yc6yjOr7nVTx" Issuer="192.168.1.10"
IssueInstant="2016-07-23T21:01:36.015Z" MajorVersion="1" MinorVersion="1">
  <Conditions xmlns="" NotBefore="2016-07-23T21:01:36.031Z" NotOnOrAfter="2016-07-23T21:06:36.031Z">
    <AudienceRestrictionCondition>
      <Audience>Pesh-council</Audience>
    </AudienceRestrictionCondition>
  </Conditions>
  <AuthenticationStatement xmlns="" AuthenticationInstant="2080-01-04T18:08:47.109Z" AuthenticationMethod="
```

```
            urn:oasis:names:tc:SAML:1.0:am:X509-PKI">
    <Subject>
     <NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">
            GaJurYm3cNvx</NameIdentifier>
     <SubjectConfirmation>
      <SubjectConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</SubjectConfirmationMethod>
     </SubjectConfirmation>
    </Subject>
    <SubjectLocality IPAddress="" />
   </AuthenticationStatement>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
     <ds:SignatureMethod SignatureMethod="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
     <ds:Reference URI="#yc6yjOr7nVTx">
      <ds:Transforms>
       <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
       <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <ds:DigestValue>k/siAyoR3q7TPfbQk8jeB2+Yzdbx</ds:DigestValue>
     </ds:Reference>
    </ds:SignedInfo>

<ds:SignatureValue>P4KfPxYuQ23C8a43l/loGO+g4u7cVHMaYxBtSSElVklAQcKOihb9JbRTE422IbvQDfX2dG7T+/B
AR8m8Xn4fYyM9+dSzp34351UoXKgGoFQUjUOilybXh+Wm1h28172l2al4pA0rs8uz+vrVMj2f6vV9ilK+iRm+rKdsZ2oj
nnzx</ds:SignatureValue>
    <ds:KeyInfo>
     <ds:X509Data>

<ds:X509Certificate>MIIE8zCCBFygAwIBAgIBFTANBgkqhkiG9w0BAQUFADCBqTEMMAoGA1UEBhMDVVNBMQs
wCQYDVQQIEwJNRDEXMBUGA1UEBxMOTm9ydGggQmV0aGVzZGExJTAjBgNVBAoTHFNFVEVDUyBTZWN1cm
l0eSBUZWNobm9sb2dpZXMxHDAaBgNVBAsTE1NFVEVDUyBTZWN1cml0eSBVU0ExEzARBgNVBAMTCkxDQSB
TZXJ2ZXIxGTAXBglghkgBhvhCAQITCjEwLjAuMS4yNDAwHhcNMTIwMTIwMTcxOTA0WhcNMTMwMTE5MTcxOTA
0WjBlMQswCQYDVQQGEwJVUzEOMAwGA1UECBMFU29sbmExEjAQBgNVBAcTCVN0b2NraG9sbTEPMA0GA1U
EChMGU0VURUNTMQwwCgYDVQQLFgNSJkQxEzARBgNVBAMTClBEUCBTZXJ2ZXIwgZ8wDQYJKoZIhvcNAQE
BBQADgY0AMIGJAoGBAL2iY+Wy87ysRw/G1WVJNXgil52DKxO4he6VRL4XmV2AlacwS7vL2pPm/5C7KkOJwNzj7
MflXemQQz3f7XHwXKOtHOcdBr6eDsGXvM/0UdHpy8GeXFXOg6HQ1Ql4lVKt4RGpIr2UZAqBzfUsadLStG7E3xsRy
9iLh2lv8V44vaqBAgMBAAGjggJsMIICaDAOBgNVHQ8BAf8EBAMCBsAwDwYDVR0TAQEABAUwAwIB/zATBglghkg
BZQMGCQEBAQAEAwEBATBABgNVHREBAQAENjA0gTJMb2NhbCBDQSBTZXJ2ZXIsTmV0d29ya2luZyBEaXZpc
2lvbixTRVRFQ1MgSW5jLixVUzCBwwYDVR0jAQEABIG4MIG1oYGvpIGsMIGpMQwwCgYDVQQGEwNVU0ExCzAJ
BgNVBAgTAk1EMRcwFQYDVQQHEw5Ob3J0aCBCZXRoZXNkYTElMCMGA1UEChMcU0VURUNTIFNlY3VyaXR5I
FRlY2hub2xvZ2llczEcMBoGA1UECxMTU0VURUNTIFNlY3VyaXR5IFVTQTETMBEGA1UEAxMKSENBIFNlcnZlcjEZ
MBcGCWCGSAGG+EIBAhMKMTAuMC4xLjI0MIIBATCBkQYDVR0gAQEABIGGMIGDMD8GCWCGSAFlAwEwATAy
MDAGCCsGAQUFBwIBFiRodHRwOi8vd3d3LnNldGVjcy5jb20vQ2VydFBvbGljeS5odG0wQAYKYIZIAWUCAQwBAT
AyMDAGCCsGAQUFBwIBFiRodHRwOi8vd3d3LnNldGVjcy5jb20vQ2VydFBvbGljeS5odG0wQAYDVR0SAQEABDYw
```

NIEyTG9jYWwgQ0EgU2VydmVyLE5ldHdvcmtpbmcgRGl2aXNpb24sU0VURUNTIEluYy4sVVMwPQYDVR0fAQEAB
DMwMTAvoi2kKzApMScwJQYJYIZIAYb4QgECExhsZGFwOi8vMTI4LjE2NC44Mi41MjozODkwEwYJYIZIAWUDBgkB
AQEABAMBAQEwDQYJKoZIhvcNAQEFBQADgYEAwInX8ATR22UqCN7qUV+Bhjx58BguA1RMuNhe1dKJcg4BXibf
TWPLpV/+h4cuFyo+0CD+CnW7EAOl0JggFZ0vrcigLNALiCwFpSIpKG+ECaOcwCKivGeRF69eMM9DTxyb2hIgwTs6
9/B0b+4XjG/wPP2vh15jcGq2qoWnB2nX3VDx|$|1|$|1271
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
</Assertion>
</Response>

Annex-C: Scyther Code Snippets for Verification Models

C.1 Authentication Protocol - Setup

```
// Initiator
fresh UCa: UserCert;
fresh UCb: UserCert;
fresh Ra:RandomNumber;
fresh Rb:RandomNumber;
fresh D:Data;
fresh Hello:Message;
fresh Ks:SessionKey;

send_1(Ua,Ub,Hello);
recv_2(Ub,Ua, UCb);
send_3(Ua, Ub, Ra, Rb, {{Ra,Rb}H}sk(Ua));
recv_4(Ub, Ua, Ra, Rb, {{Ra,Rb}H}sk(Ub));
 send_5(Ua,Ub,{D, {D}H}Ks);

// Responder
fresh UCa: UserCert;
fresh UCb: UserCert;
fresh Ra:RandomNumber;
fresh Rb:RandomNumber;
fresh D:Data;
fresh Hello:Message;
```

```
fresh Ks:SessionKey;

recv_1(Ua,Ub,Hello);
send_2(Ub,Ua, UCb);
recv_3(Ua, Ub, Ra, Rb, {{Ra,Rb}H}sk(Ua));
send_4(Ub, Ua, Ra, Rb, {{Ra,Rb}H}sk(Ub));
 recv_5(Ua,Ub,{D, {D}H}Ks);
```

C.2 Lightweight Secure Communication Protocol - Setup

```
/*   * Secure Communication Protocol (SCP)  */ // The protocol description
usertype RandomNumber;
usertype SessionKey;
usertype UserName;
usertype  Password;
hashfunction H; usertype Message;
protocol SCP1(Sensor1,ServiceProvider,Sensor2)
{
        role Sensor1
        {
                fresh Rs: RandomNumber;
                fresh Rp: RandomNumber;
                fresh msg: Message;
                fresh Sk: SessionKey;
                var Usr: UserName;
                var Pwd: Password;
                var Hello: Message;

                send_1(Sensor1,ServiceProvider,Hello);
                recv_2(ServiceProvider,Sensor1, Rp );
                send_3(Sensor1,ServiceProvider, Usr,Rs,{{Rs, Rp} H } Pwd );
                recv_4(ServiceProvider,Sensor1,{Sk}Pwd);
                send_5(Sensor1,Sensor2, {msg,{msg}H}Sk);

                claim(Sensor1,Secret,Sk);
                claim(Sensor1,Secret,Rp);
                claim(Sensor1,Alive);
                claim(Sensor1,Weakagree);
                claim(Sensor1,Commit,ServiceProvider,Sensor2);
                claim(Sensor1,Niagree);
```

```
        claim(Sensor1,Nisynch);
    }

    role ServiceProvider
    {
        fresh Rs: RandomNumber;
        fresh Rp: RandomNumber;
        fresh msg: Message;
        fresh Sk: SessionKey;
        var Usr: UserName;
        var Pwd: Password;
        var Hello: Message;
        recv_1(Sensor1,ServiceProvider,Hello);

        send_2(ServiceProvider,Sensor1, Rp );
        recv_3(Sensor1,ServiceProvider, Usr,Rs,{{Rs, Rp} H } Pwd );
        send_4(ServiceProvider,Sensor1,{Sk}Pwd);

        claim (ServiceProvider, Secret, Hello);
        claim (ServiceProvider,Secret, Rs);
        claim (ServiceProvider,Secret, Rp);
        claim(ServiceProvider,Niagree);
        claim(ServiceProvider,Nisynch);
    }

    role Sensor2
    {
        fresh msg: Message;
        fresh Sk: SessionKey;
        recv_5(Sensor1,Sensor2, {msg,{msg}H}Sk);

        claim(Sensor2,Secret,msg);
        claim(Sensor2,Weakagree);
        claim(Sensor2,Niagree);
        claim(Sensor2,Nisynch);
    }
}
```