Towards Cloud based Smart Cities Data Security and Privacy Management

Zaheer Khan
Department of Computer Science and Creative Technologies
University of the West of England, Bristol, UK
Zaheer2.Khan@uwe.ac.uk

Zeeshan Pervez
School of Engineering and Computing
University of the West of Scotland, Paisley, UK
Zeeshan.Pervez@uws.ac.uk

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

***Abstract*— Smart cities accumulate and process large amount of data streams which raise security and privacy concerns at individual and community levels. Sizeable attempts have made to ensure security and privacy of inhabitants' data. However, security and privacy issues of smart cities are not confined to inhabitants only; service provider and local government have their own reservations – service provider trust, reliability of the sensed data, and data ownership, to name a few. In this research work we identified a comprehensive list of stakeholders and model their involvement in smart cities by using Onion Model approach. Based on the stakeholder model we presented a security and privacy framework for secure and privacy-aware service provisioning in smart cities. Our framework aims to provide end-to-end security and privacy features for trustable data acquisition, transmission, processing and legitimate service provisioning. As a proof of concept we tested core functionalities of authentication protocol for data acquisition and service provisioning using Scyther automated verification tool that demonstrated that the proposed framework mitigates security and privacy concerns of different stakeholders identified in the stakeholder model.**

Keywords*— *data security, privacy, trust, smart cities, cloud computing, stakeholders

I. INTRODUCTION

With the emergence of smart cities and new technologies e.g. Internet of Things (IoTs) such as RFIDs, environmental sensors, actuators smartphones, wearable sensors, cloud computing and their applications in a city environment provide the opportunity to collect and effectively use large scale city data for information awareness and decision making [1]. Data from these devices and/or new sources can be integrated with existing city data that is stored by various departments and local agencies and be analysed for application specific information and knowledge generation. 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 computational and storage facilities [2]. However, with these opportunities 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 [3]. In addition, inherent cloud security issues e.g. storage at remote data centres, physical access etc. can contribute further in dealing with smart cities data security issues [4]. Managing such data from a smart city perspective require proper security and privacy measures which can help in establishing trust and adopting smart solutions in a city environment by various stakeholders including citizens.

State of the art literature review indicates that smart city solutions e.g. SMARTIE [3], IoT-A [4] etc., require a comprehensive approach in dealing with smart city data security, user privacy and trust issues. A few attempts have been made to identify security and privacy concerns of future cities [5-13]. However, existing work in the area of Smart cities is limited to security of data or curated services. Unlike them, in this research we identified a comprehensive list of stakeholders ranging from inhabitants to local governments and data streams to service providers presented using Stakeholder Onion Model technique [14]. We consider these stakeholders as entities who are affected by malicious behaviour of other involved entities – presenting security and privacy concerns from all angles i.e., stakeholder being a victim and attacker as well.

In this research we first identify various smart cities data security related challenges. Then, we present a security and privacy framework for data curation and service provisioning in smart cities. The proposed framework deals with secure and trusted service provisioning in Smart cities. Since, the impact of services in Smart cities is at macro level it is very important that accurate and traceable data is curated and processed by the service provider. To cater this proposed system deals with citizen authentication and data anonymisation. As proof of concept we verify effectiveness of selected components of the security architecture through a model verification technique using Scyther tool [15].

The remainder of this paper is structured as followed: next section presents the rationale for this research. Section 3 identifies different stakeholders who can benefit from the proposed solutions. Onion model technique is adapted to indicate various categories and roles interacting with the smart cities solutions. After this we briefly introduce smart cities and associated data security challenges and then a security framework/architecture is proposed followed by a proof of concept through model verification followed by conclusion and future research direction.

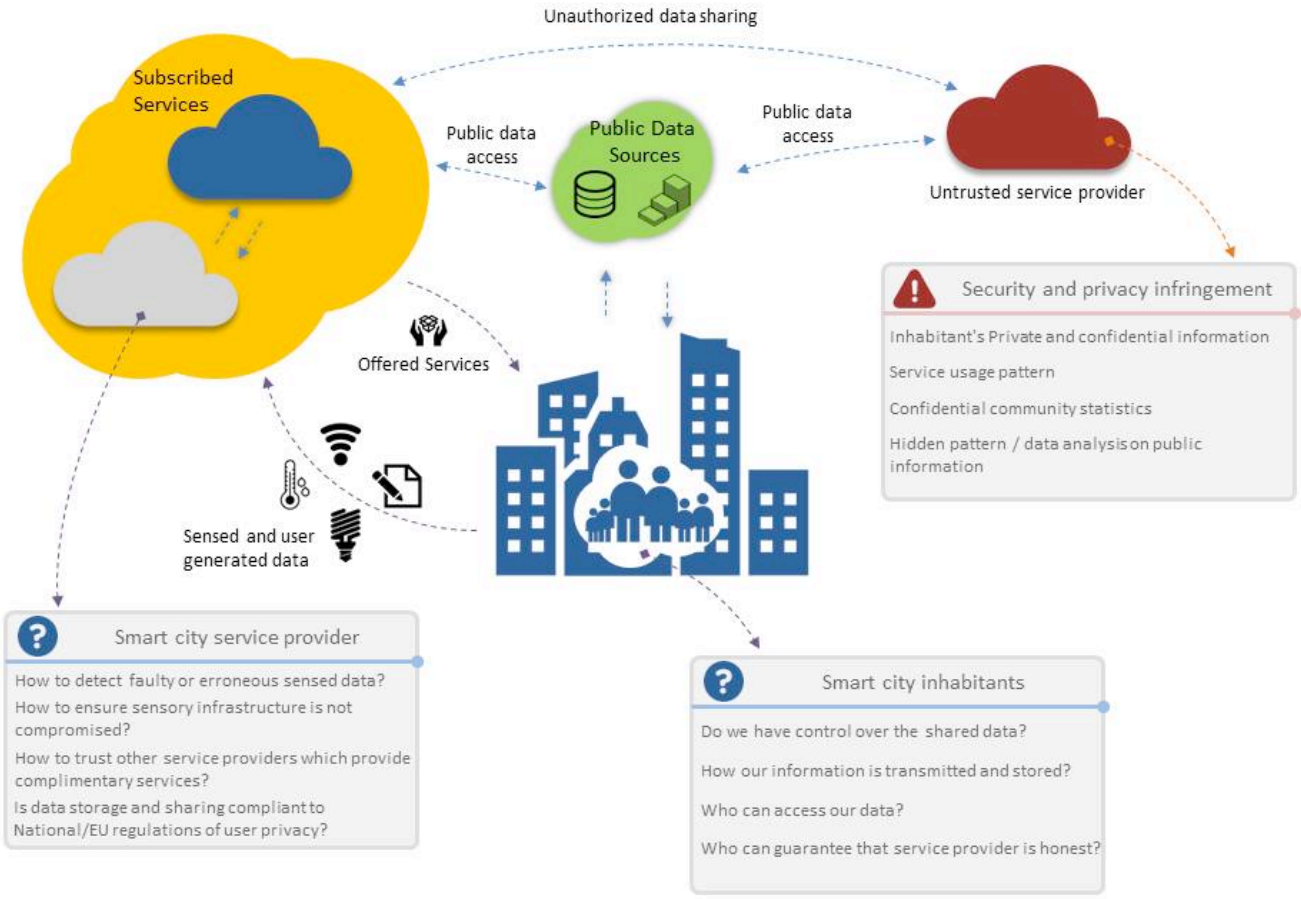

Fig. 1. Smart City Data Security Challenges

II. RATIONALE

Over the past few years the concept of Smart cities has emerged to transform urban areas into connected and well-informed spaces. Driven by the advancements of information and communication technologies the cities of future will be better planned and well informed from micro (inhabitants, local businesses) to 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 crowd-sourcing and other (i.e. Internet of Things – IoTs) can be used for analysis and decision making for sustainability and resilience of the smart future cities [1].

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". Services that make smart cities "Smart" are curated by using data stream of Smart cities i.e., inhabitants' location and digital engagement information, transportation and local government data. Accumulating and processing of these data stream raises security and privacy concerns at individual and community level as well. These security and privacy concerns are not confined to inhabitants only, service provider and local government has their own valid reservations. Therefore, ICT solutions seek suitable platform and data security mechanisms to maintain user privacy, comply with national legislations of data storage & sharing, establish trust on these solutions and maintain integrity & 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. In this respect, the objective of this work is to identify smart city data and services security challenges in a cloud environment and propose appropriate security solutions.

A crucial challenge faced by smart cities is developing a trust framework which can ensure that services driving smart cities are not having malicious intent. This problem is similar to App markets for 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 "Service Market" for smart cities have many critical implications. Since, smart cities is an emerging concept having blurry data usage and service

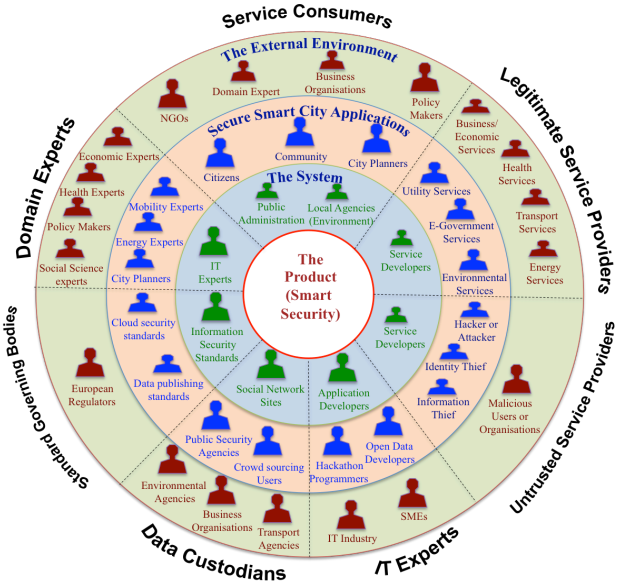

Fig. 2. Stakeholder Model

provisioning regulations, and most critically having myriad 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. Figure 1 depicts various entities which are vulnerable to security and privacy related attacks in a smart city environment. These entities comprise security challenges related to users (i.e. personal information, data ownership & control, identity), data & information (public administration data, open/sensed data, data transmission, cloud based services), service providers and citizen services.

III. Stakeholder Model

Data security and privacy aspects need to be dealt from different stakeholders' point of view to support end-to-end application security. Mainly seven major stakeholder categories are identified to better understand security and privacy concerns from different stakeholders' perspective. These include data custodians, IT experts, malicious service providers, legitimate service providers, service consumers, domain experts, standard governing bodies. These categories are further extended and mapped on to a Product Onion Model [14] where each circle in the above diagram presents specific roles relevant to the development of certain stage of the overall smart city system and applications. Using the Product Onion Model approach, Figure 2 depicts that there are four concentric circles:

The Product is the inner circle that provides Smart Security framework and components proposed in this paper. This provides the basis for handling data security and privacy aspects in variety of smart city applications from different stakeholders' point of view.

The System is Smart Security components and its human operators, security policies and rules governing its operations for specific applications.

Smart City Applications encompasses the System and its operators including any human beneficiaries of the System.

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

IV. Proposed Service Based Conceptual Framework for Smart Cities

Figure 3 illustrates the conceptual model of proposed security and privacy framework for massively connected spaces. It deals with secure and privacy-aware provisioning of services and trusted acquisition of data through various sources (e.g. citizen participation) in smart cities. Besides this, it also ensures that involved entities are working in compliance with governmental regulations and policies.

Figure 4 depicts architectural framework of data security for smart city applications. In the proposed framework ***governmental control domain*** works as a regulatory authority. Its main goal is to ensure that both service provider and inhabitants of smart cities are working within the defined regulations and policies. The service provider verification component ensures legitimate and trustable service provisioning. The seamless sensed data analysis component implements a proper audit trail mechanism to ensure that involved entities are working within their limits. The regulatory authority also ensures that authorised service providers can get access to linked open data. The integrity checker issues credential to devices, services and inhabitants of smart cities as these derive the data generated by massively connected spaces within smart cities. These credentials ensure that service providers can trust the data sources, and in case of any data delude can trace back the source and avoid forge service experience.

The ***smart city inhabitants/infrastructure*** layer deals with 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 by malicious entities. Enforcement of governmental regulations and policies is handled by this layer as well. The authentication component is used to authenticate validity of inhabitants or service providers. The services and application component deals with tamper resistant service provisioning and enforcement of governmental regulations. Service provider can be a victim of unauthorized service consumption as malicious users can tamper services to gain illicit access. Since, service provider is required to abide by rules and regulations laid 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 service registration process.

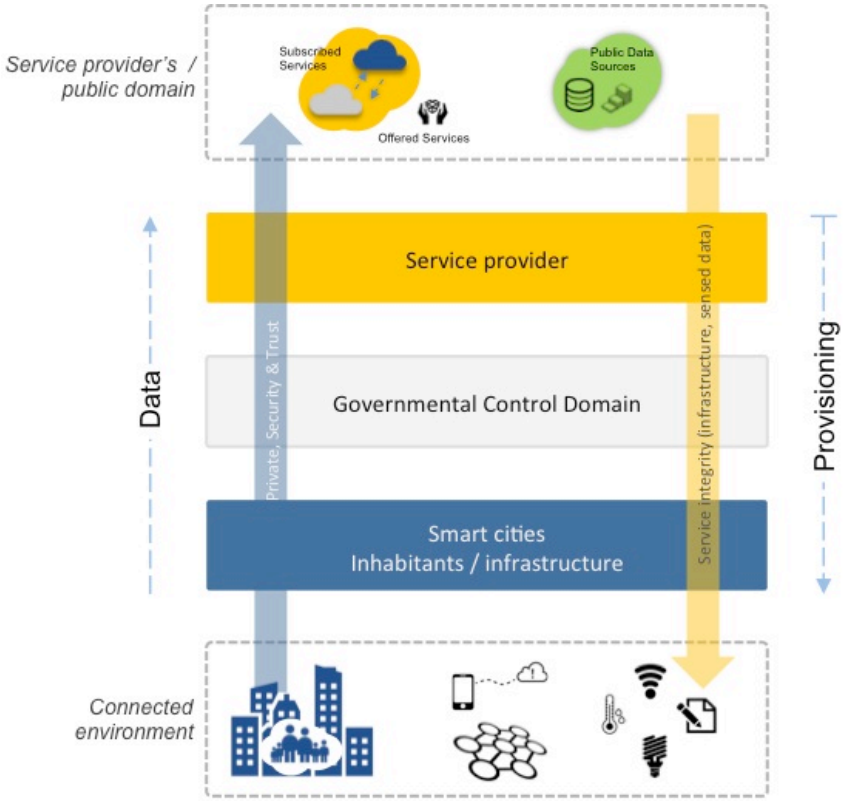

Fig. 3. Conceptual Model

The policy decision point component deals with selection of policies which ensures that necessary measures are taken before user's private and confidential information be accessed or shared. Policies are selected based on sensed information and service descriptor. If a service requests access to private and confidential data, it may be required that to store data in an untrusted domain either data must be anonymized or encrypted before it can leave user controlled domain. The authorisation component complements the capabilities of Services and Applications to enforce appropriate access control policies. It also maintains an access control log to record data access activity. It significantly helps in case of privacy infringement. It is used to store general access control policies which comply with regulatory authority or personalized access control preferences defined by inhabitants. The data confidentiality 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 untrusted domain i.e., public cloud services. It works in conjunction with Services and Applications to conceal sensitive data according to the security policies selected by policy decision point. These policies can specify either all data should be encrypted or only specific parts should be concealed. For accurate and efficient data analysis it is very important that the service providers process and access the 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 anonymisation 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 provider to explore new business possibilities by sharing anonymized sensed data with other service providers.

The ***service provider*** layer is designed to deal with service provisioning and secure and privacy-aware data sharing in 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. The service & application provisioning component represents 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. The data repositories component enables services provider 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 untrusted domain, fine-grained controlled 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. This framework leverages service providers to open an application programming interface to their business logic and accumulate application/specific data,

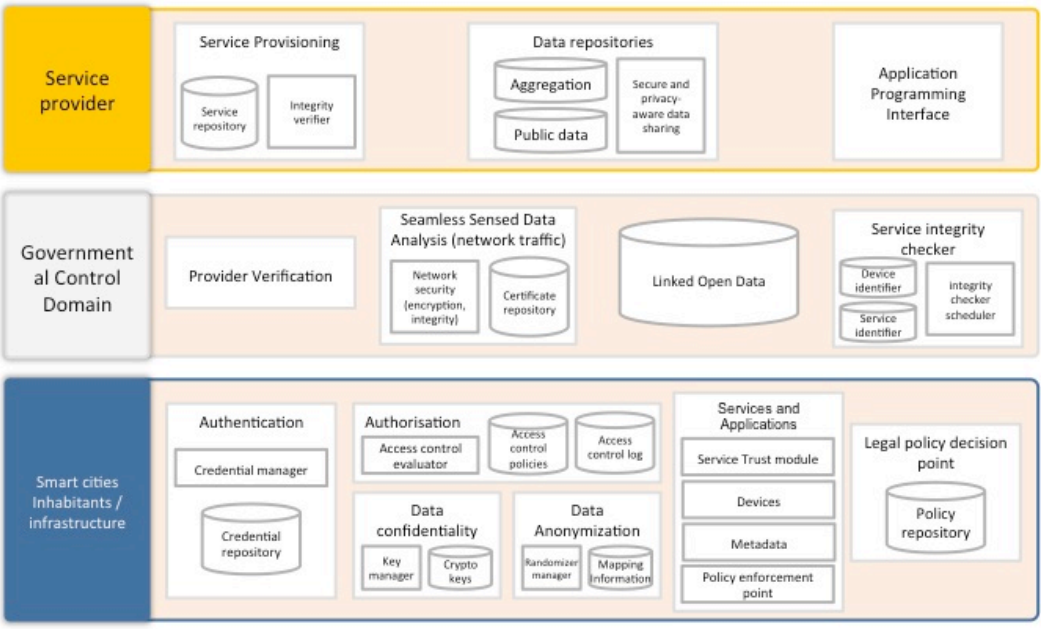

Fig. 4. Security and privacy framework for Smart cities

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.

V. Security Protocol Verification

Due to space limitation, we only cover authentication component of the above architecture. The authentication component is based on FIPS-196 entity authentication protocol for authenticating. For verifying this component we used Scyther verification tool [15] that uses a formal language for automated security protocol verification. The various steps involved in authentication protocol are described in the following Scyther compliant formal language:

```
// 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);
```

In literature, that man-in-the-middle, replay attack, message tampering, and information leakage (identity) are some of the potential attacks those can be launched on authentication protocol. Therefore, in our claims, from sender's point of view, we specified following claims 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 with attribute *Nisynch* provides the verification that the messages are received from legitimate sender in specified sequence. Since, in our protocol, we encrypted challenge using 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 the second 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. In our used protocol, challenge numbers are digitally signed which holds the properties of tamper resistance and

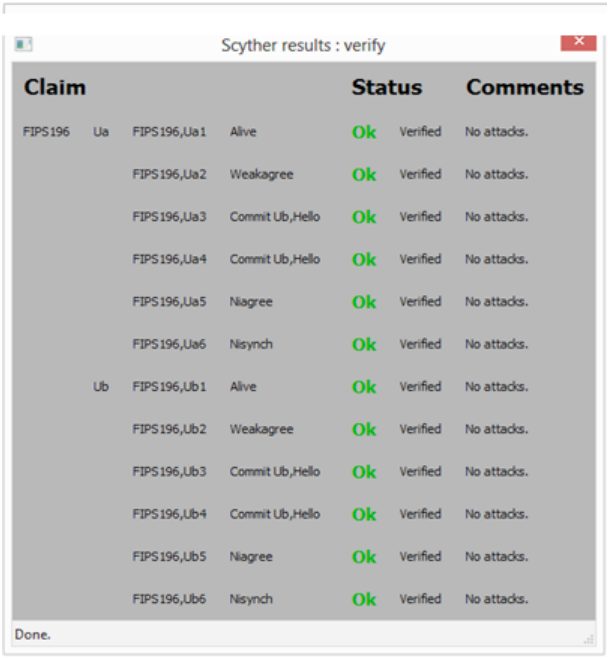

Fig. 5. Scyther results

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. 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.

The verified results of above mentioned properties are shown in Figure 5. The results show that the used authentication protocol satisfied all properties and resisted against man-in-the-middle, replay attack, and message tampering. However, this authentication protocol does not preserve privacy of the user and consequently, during authentication an attacker can extract the identity of the users. To solve this issue, it is recommended that instead of using identity based certificate, an anonymous certificate may be used but the sequence and procedure of the protocol will remain same.

VI. Conclusion

In this paper we highlighted data security and privacy issues in the context of cloud based smart cities solutions. Our approach considers security aspects from different stakeholders' point of view and proposes end-to-end security for smart cities applications which use open data and promote citizen participation. We proposed a comprehensive framework to deal with data security, privacy and trust issues. Such a framework can be useful to provide secure context-aware information services for citizens in a smart city environment [16]. Using Scyther security verification tool, the authentication component of the proposed framework is tested against possible attacks with promising results. Other components of the proposed framework including secure communication protocol are being implemented and tested using scenario-based approach as part of future work.

References

[1] Z. Khan, A. Anjum, S. L. Kiani, Cloud based big data analytics for smart future cities. Proc. ITAAC 2013 - 6th IEEE/ACM International Conference on Utility and Cloud Computing, pp. 381-386, 9th-12th December, 2013. Dresden, Germany.

[2] Z. Khan, D. Ludlow, R. McClatchey, A. Anjum, An architecture for integrated intelligence in urban management using cloud computing, Journal of Cloud Computing: Advances, Systems and Applications, 1:1, pg. 1-14, ISSN 2192-113X, 2012.

[3] J. Bohli, P. Langendorfer, A. F. Skarmeta, , Security and Privacy Challenge in Data Aggregation for the IoT in Smart Cities, In Ovidiu Vermesan, Peter Friess (Eds) Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, pp. 225-244, 2013, River Publishers.

[4] N. Gruschka, D. Gessner (Eds), 2012, IoT-A, Internet of Things Architecture, Project Deliverable D4.2 - Concepts and Solutions for Privacy and Security in the Resolution Infrastructure, Feb, 2012.

[5] A. Martínez-Ballesté, P. Pérez and A. Solanas, The Pursuit of Citizens Privacy: A Privacy-Aware Smart City is Possible, *IEEE Communications Magazine*, Vol. 51, no. 6, pp. 136-141, Jun 2013, ISSN: 0163-6804.

[6] K. Popović, Ž. Hocenski, "Cloud Computing Security Issues and Challenges", Proc. 33rd International Convention MIPRO May 24-28, 2010, pp 344-349, Opatija, Croatia.

[7] A. Martínez-Ballesté, P. Pérez and A. Solanas, W3-privacy: the three dimensions of user privacy in LBS, 12th ACM Int'l. Symp. Mobile Ad Hoc Networking and Computing, May 2011, Paris, France.

[8] A. S. Elmaghraby, M. M. Losavio, Cyber security challenges in Smart Cities: Safety, security and privacy, Journal of Advanced Research, Volume 5, Issue 4, July 2014, pp. 491-497, ISSN 2090-1232, http://dx.doi.org/10.1016/j.jare.2014.02.006.

[9] Executive Report: Smart Cities. "Transformational 'smart cities': cyber security and resilience". Symantec 2013. URL Access: http://eu-smartcities.eu/sites/all/files/blog/files/Transformational%20Smart%20Cities%20-%20Symantec%20Executive%20Report.pdf

[10] Y. Im Cho, (2012), Designing smart cities: Security issues, In Computer Information Systems and Industrial Management, LNCS Vol. 7564, pp. 30-40, Springer Berlin Heidelberg.

[11] A. Bartoli, J. Hernández-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, Security and privacy in your smart city, In Proc. of the Barcelona Smart Cities Congress, December 2011.

[12] M. Sen, A. Dutt, S. Agarwal, A. Nath, Issues of Privacy and Security in the Role of Software in Smart Cities, International Conference on Communication Systems and Network Technologies (CSNT), p.p. 518-523 6-8 April 2013, Gwalior.

[13] L. Wang, C. Jing, P. Zhou, Security Structure Study of City Management Platform Based on Cloud Computing under the Conception of Smart City, Fourth Int. Conference on Multimedia Information Networking and Security (MINES), p.p. 91-94, 2-4 November 2012, Nanjng.

[14] I. Alexander, A taxonomy of stakeholders: Human Roles in System Development, International Journal of Technology and Human Interaction, Vol 1, 1, 2005, p.p.23-59, 2005.

[15] Scyther tool, URL Access: http://www.cs.ox.ac.uk/people/cas.cremers/scyther/ Last Accessed: 31 July 2014.

[16] Z. Khan, S. Kiani, K. Soomro, A Famework for Cloud-based Context-aware Information Services for Citizens in Smart Cities, Journal of Cloud Computing: Advances, Systems and Applications, 2014. In press.