Property Based Attestation for a Secure Cloud Monitoring System

Abir Awad, Sara Kadry, Brian Lee, Shuaijun Zhang

Irish Centre for Cloud Computing and Commerce
Software Research Institute, Athlone Institute of Technology
Athlone, Ireland

aawad@research.ait.ie, skadry@research.ait.ie, blee@ait.ie, szhang@research.ait.ie

***Abstract*—In this paper, we consider the problem of trust in cloud monitoring systems. We design and develop a novel scheme for trust certification using property based attestation (PBA). The PBA is based on a trusted platform module (TPM) installed on the monitoring system called CloudPass. This certification scheme can be applied to any other monitoring system. In our proposal, two security properties are studied and tested: The integrity of the monitoring system and the identity of the platform. To test the proposed scheme, a prototype is developed and the certificates are generated at different level security property granularity for the attested system.**

Keywords— cloud, monitoring system, Trusted Platform Module, Property Based Attestation

I. INTRODUCTION

Trust issues arise in the cloud environment because the lack of control which customers face. A customer compute infrastructure is located at an off-site location and is managed by a second- or third-party entity. Recently, a number of monitoring systems [1] have been proposed to boost the trust of the customers in the capability and performance of cloud infrastructures. However, trust of the *monitoring system itself* is also an important issue for the cloud users. Current cloud monitoring solutions have not considered the trust issue of the entity which enforces the monitoring process. Providing a trusted monitoring entity that can provide an honest and intact view of monitored resources for the cloud tenants is a challenge. The monitoring entity is normally assumed in a privileged domain, i.e. is honest, and can't be maliciously subverted by any attacker which means that it never gives fake information. However, in practice, these assumptions could be violated, and in this case the monitoring results can't be fully trusted. Thus, building a trusted monitoring system is still an open issue.

Trusted computing is a paradigm developed and standardized by the Trusted Computing Group (TCG) whose goal is to enforce trustworthy behaviour of computing platforms. The main idea of TCG is to assure a trusted computing platform based on a hardware crypto-processor module designated the Trusted Platform Module (TPM) [2]. An important mechanism of the TPM technology is *platform attestation*. Attestation is a mechanism by which a computing platform proves to a third party that it is trusted. The challenge of the attestation is to define a set of reasonable and measurable metrics that can be used to determine whether a computing platform is trusted. Recently, people have presented new approaches for platform attestation, such as property based attestation which enable more meaningful attestation by abstracting low level binary values to high level security properties or functions [3], [4].

Generally, it is unrealistic to expect that customers have expertise to monitor and determine the state of infrastructures provided by the cloud service provider (CSP). In order to make cloud computing more acceptable, a trusted third party (TTP), who is an expert in the security and trusted computing field, is required. The TTP takes the responsibility for customers to determine whether the infrastructures provided by CSP is trusted.

The authors in [4] provide an analysis of the different property based attestation mechanisms that have been proposed recently with a particular focus on the limitations of each of the mechanisms. They outline a list of important challenges for property attestation including the granularities of the security properties which we also consider in our trust certification scheme.

In this paper, we provide a trusted monitoring framework, based on property based attestation, that can establish a trust chain for the cloud tenants who will be able to ask the TTP for a certificate assuring the security and trust of the monitoring entity.

The paper is organized as follows: Section 2 provides background information about CloudPass (the studied monitoring system) and the property based attestation. Section 3 presents the proposed security system and the checked properties. Section 4 describes the implementation of the system and presents the simulation results. Finally, we summarize our conclusions in section 5.

II. BACKGROUND

A. CloudPass

CloudPASS [5] is an integrated system that monitors and validates SLAs for the cloud. It enhances the trust and dependability of the cloud and enables cloud service providers to communicate their trustworthiness to the

market using a novel technology-mediated cloud-specific nutrition label [6].

Fig. 1 gives the architecture of CloudPass which consists of three logical parts:

- Monitored Subsystem – The monitored subsystem consists of resources and services that are part of the cloud provider system. It may consist of one or more domains corresponding to one or more cloud service providers.
- Monitoring Subsystem – collects, stores and processes raw metrics. The monitoring system is in a different domain than the monitored systems.
- Trust Calculation Subsystem – this component retrieves data (raw or processed) from the monitoring subsystem and transforms this data into an easily understood visual form via the nutrition label.

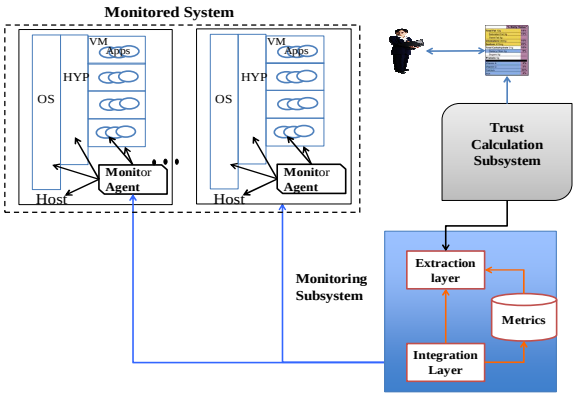

Fig. 1. CloudPass high level architecture

B. Property Based Attestation (PBA)

The Trusted Computing Group (TCG), a not-for-profit industry-standards organization with the aim of enhancing the security of the computing environment, advocates methods to improve cloud transparency using hardware-based attestation mechanisms. The technologies proposed by the TCG are centred on the Trusted Platform Module (TPM), which is typically implemented as a chip mounted on a PC motherboard [2].

However, TCG binary attestation, which is based on the measurements taken by the TPM, has some important drawbacks [3]:

- Disclosure of platform configuration information which can potentially lead to a security and privacy issues.
- Lack of flexibility. Each time a small change occurs, a new reference measurement has to be provided which dramatically increases the number of possible expected values for a component and raise issues after system migration, update or misconfiguration.
- Less scalability due to necessary management of every trusted platform configuration. It requires the verifier to know all possible trusted configurations of all platforms as well as managing updates and patches that change the configuration.
- It is based on hash values which are cumbersome to use as policies as it is difficult to interpret them to be meaningful system states.

To tackle these problems, property-based approaches were proposed which require to only attest whether a platform or an application fulfils the desired security requirements without revealing the specific software or hardware configuration [3], [4]. Instead of attesting hash values of binaries, they attest abstract properties describing the behaviour of a program or system.

Certificate based attestation is the main used PBA mechanism. In this case, a Trusted Third Party (TTP) is necessary. The TTP provides signed certificates for the attested properties. Property based certificate can be generated at different levels of granularities.

III. PBA ON CLOUPASS

The trustworthiness of a monitoring system is a major challenge. To achieve it, we need first to determine what are the security properties of the monitoring system that we need to check to build the trusted monitoring system. In this paper, we apply property based attestation on CloudPass. We first identified two security properties which we want to certify for the monitoring system; *the identity checking and the integrity* properties. Then, we took into account their granularities. Finally, these properties are guaranteed using property certificates.

In the following, we first show the property based attestation pyramid with different levels of granularity of the studied properties. Then, we give the architecture of our system and explain the attestation mechanisms for each property.

A. Property based attestation pyramid

In this section, we define the two security properties of CloudPass and their components based on their granularity. Fig. 2 shows the granularity pyramid for the monitoring system protection. To each level of the pyramid, one or more certificate(s) are associated. As we can see, the pyramid has 4 levels: the class, the services for that class, the components of each service and the mechanisms [6].

Class: The security class is the top of the hierarchy in the pyramid and it is a common intent of the security services that belong to this class. In our case, the class is the monitoring system protection.

Service: A security service addresses a security objective or a security problem within the class. In our case, the service is the monitoring system protection during the *collection and storage of the monitoring* data in the monitoring system.

Service component: Each service is divided into one or more components. In our system, we define two service components for the protection of the monitoring system:

- Monitoring system integrity i.e. the integrity of the system collecting the monitoring data.
- Identity checking i.e. the identity verification of the monitoring system having the TPM.

Mechanism: A mechanism is used to implement a service component. In our case, we have two service components, the corresponding mechanisms for each service component are as follow:

- For the monitoring system integrity, remote attestation is used to verify the integrity of the platform.
- For the identity verification, the platform property is generated using the SSL and the AIK certificates of the trusted platform module TPM [8].

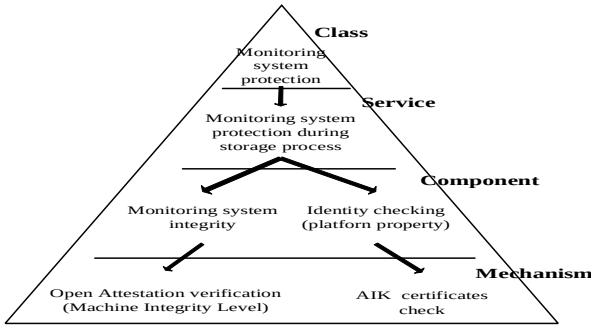

Fig. 2. PBA granularities for CloudPass properties

Properties and components at higher levels provide more privacy for the checked system. This is because properties at the higher levels hide implementation details of both properties and components. Properties at the lower levels of the model provide less privacy but more flexibility for the attestation.

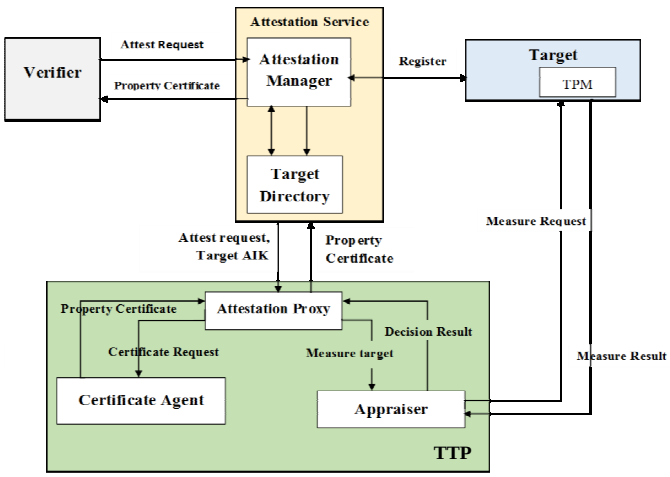

Fig. 3. CloudPass attestation architecture

The purpose of the Cloudpass attestation/certification system is to prove that the attested platform (the CloudPass monitoring system) satisfies the verifier's security requirements. It consists of mapping between the system's configurations (System Measurements) and the system's properties (Integrity, Identity) and publishing these properties in a certificate form. The architecture of the Cloudpass attestation system is shown in Fig. 3. In the CloudPass attestation system architecture, we have the following actors:

- *Verifier:* The party who requests the attestation manager to certify a security property for a specific. The verifier can be an individual or a company.
- *Target* (the monitoring system in our case): The system to be attested/certified i.e. CloudPass in our case.
- *Attestation manager:* The main actor of the attestation service (see Fig. 3). It handles the attestation queries and the attestation sessions. The attestation manager has three functionalities; it stores target's details, receives attestation requests, and sends them to the attestation proxy.
- *TTP:* The trusted third party is responsible of certifying the target. In this part, we have the following three players:
  - Attestation proxy: It is the party that takes the assignment from the attestation manager and is in contact with all the other parties of the TTP.
  - Appraiser: The party which makes the decision about the target. In case of the integrity property, it compares the target measurements with its measurements standard (WhiteList) but in case of identity checking property, it checks the validation of AIK certificate.
  - Certificate agent: is the party issuing the property certificate and returning it to attestation proxy which is giving it in its turn to the attestation manager.

B. *Attestation Phases*

The certificate based attestation of CloudPass consists of two phases: the registration phase and the attestation phase. In the first phase, the target's details are stored by the attestation manager whilst in the second phase, the target is checked to verify either the target's identity or integrity.

1) Registration Phase

The registration phase is divided into two main operations; the installation of the OpenAttestation agent [9] on the target and the registration of the target on the Attestation Service. Fig. 4 shows the sequence diagrams for the registration phase. The algorithm can be explained as follows:

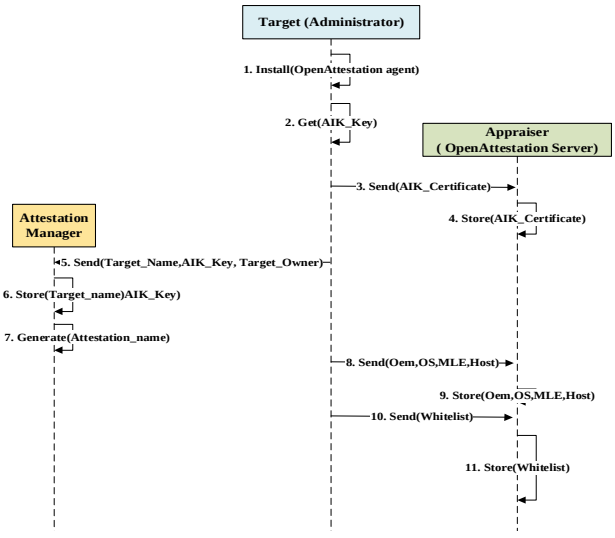

Fig. 4. CloudPass registration phase

- The target (administrator) installs the OpenAttestation agent on the system. After the installation is completed, the target (administrator) gets the AIK public key and the AIK certificate from the TPM which is installed on the target. Then, the target (administrator) sends his AIK certificate to the OpenAttestation server which is on the appraiser system. Finally, the appraiser stores the AIK certificate in his database.
- The target (administrator) starts his registration by sending his details to the attestation manager i.e. the target name, the AIK key, and target owner.
- After the registration is completed, the target (administrator) boots his system and sends its initial measurements to the appraiser. Then, appraiser stores these initial measurements as good values called "Whitelist".

2) Attestation Phase

This phase is to apply the PBA approach on CloudPass architecture to verify its security properties. The attestation phase is divided into two sub phases; attestation request and property verification.

a) Attestation Request

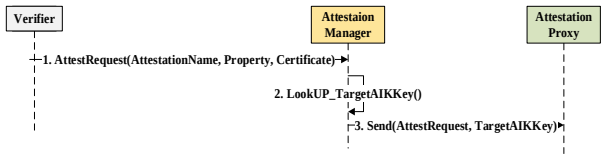

Fig. 5. Attestation request

The attestation algorithm can be explained as follows:

- The verifier transmits a request to the attestation manager for a specific target. The request is to generate a property certificate either for the identity or integrity properties.
- The attestation manager looks into the "Target directory" to find the AIK key corresponding to the target. Then, the attestation manager sends the attestation request with the target AIK key to the attestation proxy

b) Property Verification

In this phase, we have two properties; the identity and the integrity properties.

Identity Property

This property helps the verifier to check the identity of the target before using it. The verifier in this case can be either the monitored system (see Fig. 1) or a CloudPass administrator in case of self-assessment. In order to determine the identity, it is necessary to check the validation of the AIK certificate which proves that the TPM is successfully installed on the target. Fig.6 shows the sequence diagram of the identity verification property.

- The attestation proxy finds the target name which corresponds to the AIK key received from the attestation manager. Then, the attestation proxy asks the appraiser to check the AIK certificate. The appraiser checks then the validation of the AIK certificate and returns the result to attestation proxy.

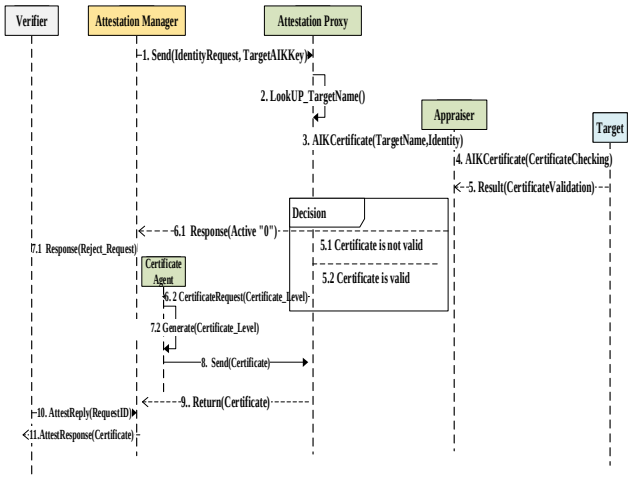

Fig. 6. Identity property

- If the result is "not valid"; the attestation proxy returns "not trusted" to the attestation manager. Then, attestation manager sends a "reject" response to the verifier.
- If the result is "valid"; the attestation proxy asks the certificate agent to generate a property certificate. Once the certificate is ready, the attestation proxy sends it to attestation manager. Finally, the attestation manager retransmits it to the verifier.

Integrity Property

This property determines the integrity of the target which is important to prove that the target is not attacked by an intruder.

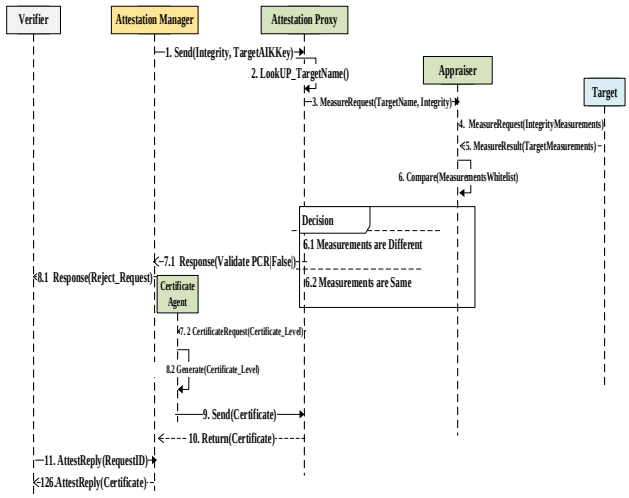

Fig. 7. Integrity property

The verifier in this case can be either a CloudPass administrator in the case of self-assessment or an external user such as a person, company or cloud provider.

As shown in Fig. 7, to check the integrity property, the appraiser uses the Platform Configuration Registers (PCR) values which reflect the measurements of the current state. Then, the appraiser returns the decision result to the attestation proxy. The decision result is obtained by comparing the current measurements with the “WhiteList”.

- If the result is "different"; the attestation proxy returns "not trusted" to the attestation manager and sends "reject" response to verifier.
- If the result is the "same"; the attestation proxy asks the certificate agent to generate the integrity certificate which will be returned later to the attestation manager to the attestation proxy. Finally, the attestation manager transmits the certificate to the verifier.

IV. IMPLEMENTATION

We developed a prototype for our property certification system. In our implementation, we used OpenAttestation which is a framework developed by Intel [9] as a measurement tool for the target. It enables the OpenStack Nova Scheduler to retrieve and verify the integrity of the cloud (CloudPass in our case) nodes. ASP.NET is used to develop the websites, MySQL for the databases and C# for generating the certificates. Fig. 8 gives a more technical view of the certification system architecture.

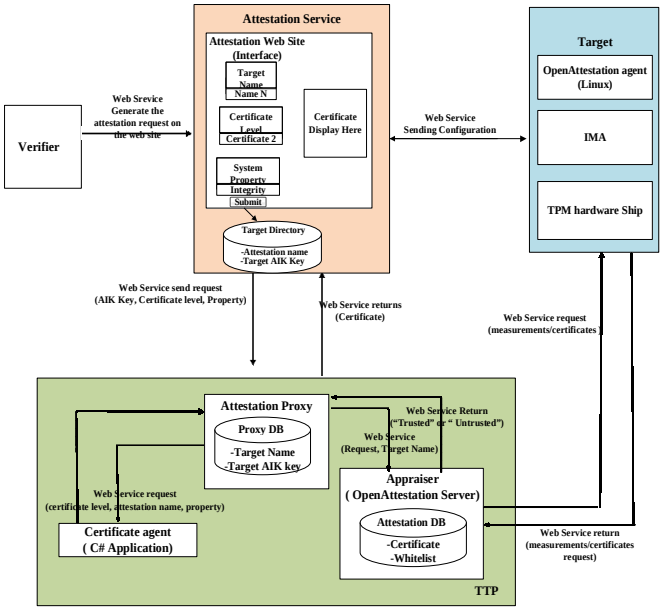

Fig. 8. Technical view of CloudPass attestation architecture

In this section, we show some snapshots of implementation that shows how property based attestation applies on CloudPass through different scenarios.

The main screen of our system is shown in Fig. 9.

The main screen shows Cloudpass functionalities:

- Registration: Target administrator registers its host using this function
- Verification request: Verifier attest request uses this function
- Verification reply: Verifier uses this function to retrieve the certificate request

Fig. 9. Cloupass certificatin system main screen

A. *Scenario 1: Target registers with attestation service*

In this scenario, the target administrator registers his system to the attestation manager by filling all requirements such as target name, owner name, AIK key and target’s type as we can see in Fig.10.

In our prototype, we just considered the certification of a physical machine. The attestation of the virtual machines will be considered is a future work.

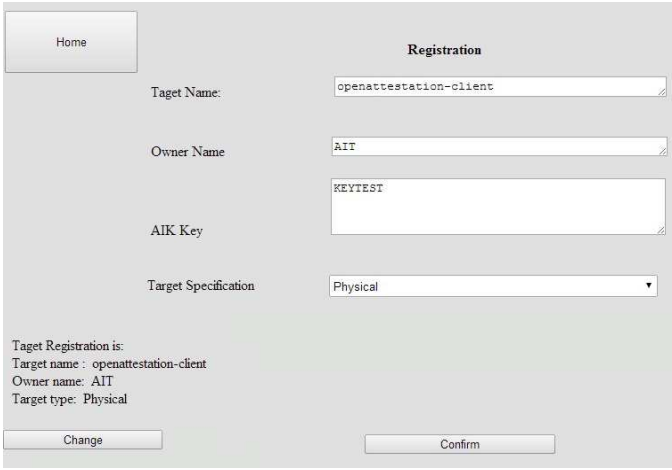

Fig.10. Cloupass certificatin system registration screen.

B. *Scenario 2: Property Verification*

The verifier first selects the host name and then selects which certificate level for which property (Fig. 11).

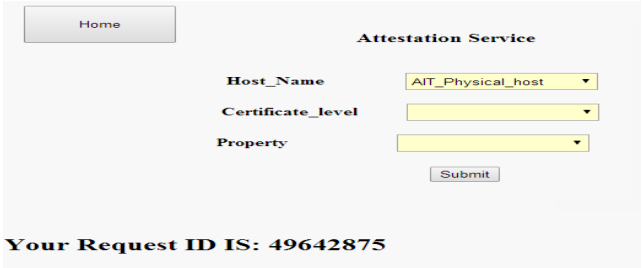

Fig. 11. Property verification main screen.

In our implementation, the verifier can request a certificate at level 1 or 2 for one of the following two properties: Identity and integrity.

1) Identity Verification

In this section, we assume that the verifier requests an Identity Checking Property Certificate at Level 1 (Fig.11).

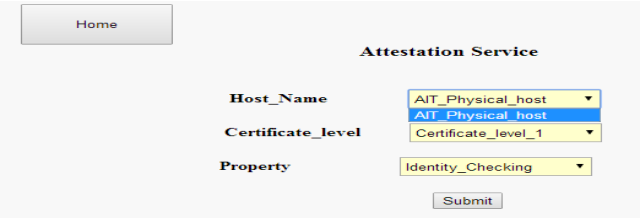

Fig. 12. Identity checking attestation request for a certificate level1

Using his request identifier, the verifier is able to retrieve the certificate validated by our certification system as we can see in Fig. 13.

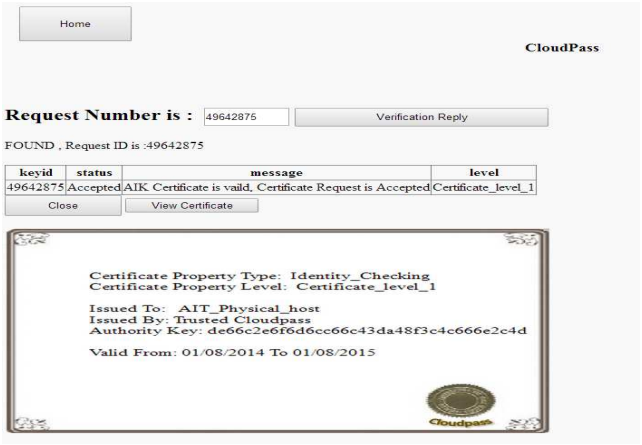

Fig. 13. Identity checking certificate level 1

2) Integrity Verification

In this verification case, the verifier requests the integrity property certificate from our certification system. The attestation request works as previously shown for the identity property. However, in this case, instead of validation of the AIK Certificate of target, the appraiser gets the PCR's values of the TPM, which are hash values for each application on target, then compares them with "whitelist" and returns the measurements decision result to attestation proxy before the certification phase (see Fig. 14).

Fig. 14. Integrity process certification screen

V. Conclusion

A trust certification scheme using property based attestation is designed and implemented to achieve trust in the cloud monitoring system. The proposed scheme permits the assessment of the system security properties. Two security properties are considered in the current phase; the integrity and the identity of the monitoring system. To the best of our knowledge, this paper is the first to propose the use of property based attestation for cloud monitoring. Taking into account other security properties such as the authentication and the extension of the proposed scheme for the cloud virtual machines will be the subject of future work.

Acknowledgment

The research work described in this paper was supported by the Irish Centre for Cloud Computing and Commerce, IC4 (www.ic4.ie) an Irish national Technology Centre funded by Enterprise Ireland and the Irish Industrial Development Authority.

References

[1] K. Fatemaa, V. C. Emeakarohaa, P. D. Healya, J. P. Morrisona, T. Lynn, "A Survey of Cloud Monitoring Tools: Taxonomy, Capabilities and Objectives," Journal of Parallel and Distributed Computing, 2014.

[2] E. Gallery, C. J. Mitchell, "Trusted Computing: Security and Applications," Crypto logia, vol. 33, no. 3, pp. 217-245, 2009.

[3] A. R. Sadeghi, C. Stuble, "Property-based attestation for computing platforms: Caring about properties, not mechanisms," In Proceedings of the 2004 workshop on New security paradigms, ACM, pp. 67-77, 2004.

[4] A. Nagarajan, V. Varadharajan, M. Hitchens, E. Gallery, "Property Based Attestation and Trusted Computing: Analysis and Challenges," In Network and System Security, NSS'09, Third International Conference on IEEE, pp. 278-285, 2009.

[5] http://www.ic4.ie/research/projects/

[6] L. van der Werff et al, "Building Trust in the Cloud Environment: Towards a Consumer Cloud Trust Label," In ICDS 2014, The Eighth International Conference on Digital Society, pp. 157-163. 2014.

[7] A. Nagarajan, V. Varadharajan, M. Hitchens, "Analysis of Property Based Attestation in Trusted Platforms," IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp. 833-840, 2010.

[8] N. Borhan, R. Mahmod, "Platform Property Certificate for Property-based Attestation Mode," International Journal of Computer Applications, vol. 65, no.13, pp. 0975 – 8887, 2013.

[9] Intel, OpenAttestation SDK (OAT) A SDK for Remote Attestation, https://github.com/ OpenAttestation /OpenAttestation.