# Privacy-Preserving Television Audience Measurement Using Smart TVs

George Drosatos, Aimilia Tasidou, Pavlos Efraimidis



# Privacy-Preserving Television Audience Measurement using Smart TVs

George Drosatos, Aimilia Tasidou, and Pavlos S. Efraimidis

Dept. of Electrical and Computer Engineering, Democritus University of Thrace, University Campus, 67100 Xanthi, Greece
{gdrosato, atasidou, pefraimi}@ee.duth.gr

**Abstract.** Internet-enabled television systems, often referred to as Smart TVs, are a new development in television and home entertainment technologies. In this work, we propose a new, privacy-preserving, approach for Television Audience Measurement (TAM), utilizing the capabilities of the Smart TV technologies. We propose a novel application to calculate aggregate audience measurements using Smart TV computation capabilities and permanent Internet access. Cryptographic techniques, including homomorphic encryption and zero-knowledge proofs, are used to ensure both that the privacy of the participating individuals is preserved and that the computed results are valid. Additionally, participants can be compensated for sharing their information. Preliminary experimental results on an Android-based Smart TV platform show the viability of the approach.

**Keywords:** Privacy, Television Audience Measurement (TAM), Smart TV, Privacy-preserving Data Aggregation, Economics of Privacy.

## 1 Introduction

Television is nowadays one of the dominant mediums for information and entertainment. Information about television audiences provide valuable insights to broadcasters and the advertising industry on recent trends. Television Audience Measurement (TAM) systems aim at calculating qualitative and quantitative TV audience measurements. For example, Nielsen[1], one of the leading companies in the field of media audience measurement, uses measurements from approximately 18,000 households[2] in the U.S.A. to create the estimates the TV networks use. The viewer data is collected by the special metering equipment installed on the TV sets of the participating households; this data is transferred directly to the company's servers. Apparently, the above measurement process raises important privacy issues for the participants. A person's viewing record can reveal sensitive information about the person's preferences and habits. A privacy-preserving method for creating accountable TAMs is needed, in order to

[1] http://www.agbnielsen.net
[2] February 2010

utilize television ratings information, while protecting the participants' privacy. Additionally, since TAM data bring important financial benefits to the industry (broadcasters, advertising companies, commercial products and more), some kind of fair financial compensation should be offered to the users that provide their viewing records.

Advances in communication and entertainment technologies have recently led to the introduction of Smart TVs, which are Internet enabled devices that support standard computer functionality (i.e., calculations, application execution, etc). This combination of traditional TV functionality with computational and networking capabilities, makes Smart TV technology capable of a whole new set of applications.

In this work, we present PrivTAM, a system for privacy-preserving TAM using Smart TV technology. The core of PrivTAM is a privacy-preserving cryptographic protocol, which accepts as input the viewing records from users' Smart TVs and performs secure multi-party computations [23] to calculate the TAMs. PrivTAM satisfies the following requirements for a reliable, privacy-preserving, TAM:

- Privacy - all records must be secret.
- Completeness - all valid records must be counted correctly.
- Soundness - dishonest records cannot disrupt the measurement process.
- Unreusability - no user can submit their record more than once.
- Eligibility - only those who are allowed to participate can submit their records.
- Verifiability - nobody can falsify the result of the TAM process.

The above requirements are a subset of the typical requirements of e-voting systems [15] and thus, our system borrows techniques from this field [4, 9, 12]. In addition, functionalities for the financial compensation of the participants are supported. The computations of PrivTAM are performed between software agents, which are located at the participants' Smart TVs, and a Trusted Authority (TA). Each Smart TV has an agent which continuously collects the viewing records of its owners.

The Trusted Authority coordinates the computation, verifies the validity of the records, collects the encrypted results and provides the compensation to the participants. This process is performed using encrypted viewing records, hence the record contents are never revealed to the Trusted Authority. Finally, we develop a prototype implementation and perform experiments that confirm the feasibility of the approach.

Some of the advantages of our approach in comparison to traditional TAM systems are:

- Preserving the privacy of participants' viewing records.
- More reliable measurements can be achieved, since a practically unrestricted number of participants can produce the PrivTAM results.
- Supports fine grained measurements which can be automatically calculated in small time intervals as well as specific one-time queries.

- Reducing the cost for conducting a TAM. No specialized equipment is required and only the participants in a calculation need to be compensated.
- Supporting measurements using records from any Internet-enabled broadcasting medium (e.g., Broadcast TV, Cable TV, IPTV and Satellite TV).

Our solution requires Smart TV's to have permanent Internet access, a requirement which is satisfied by default. Moreover, the computational and networking requirements of PrivTAM can be easily fulfilled by modern embedded Android-based platforms.

**Related Work.** To our knowledge this is the first attempt at creating a privacy-preserving TAM system, particularly one that supports an arbitrarily large amount of participants. In general, TAMs are products of aggregation operations and therefore our work is related to common privacy-preserving aggregation systems. For example, in [17], privacy-preserving data aggregation in people-centric urban sensing systems is discussed. A market for personal data, supporting anonymous data aggregation operations is presented in [3]. The economic aspects of personal privacy are discussed in [22, 1]. The fact that individuals need to be in control and be compensated when their personal information is used for commercial purposes, is discussed in [11, 18]. The sensitivity of the viewing records is stressed by both the Video Privacy Protection Act [20] and the Cable TV Privacy Act [19].

Overall, we consider that PrivTAM lies between privacy-preserving aggregation systems and e-voting systems, offering verifiable, privacy-preserving, aggregation functionalities. Additionally, PrivTAM takes into account the economic aspects of privacy and supports compensation functionalities for the measurement subjects.

## 2 The PrivTAM System

An overview of the PrivTAM system architecture, built on top of Smart TV technology, is shown in Figure 1. The main parts of the architecture are the participating Smart TVs, the Television Audience Measurement Service (TAM Service) and the Trusted Authority (TA). Every Smart TV contains a software agent that collects and stores its viewing records and maintains a set of demographic elements, such as gender, age and educational level of the viewers. The agent manages the viewers' personal data, provides controlled access to the data, and has the ability to participate in distributed protocols and computations.

The TAM Service collects the measurements and is responsible for coordinating the distributed key generation [13] for the public-key cryptosystem between itself and a group of $L$ TV agents. These $L$ agents are chosen with a verifiable random selection [7] and participate in both the public-key creation phase and the decryption of the results phase. The TA is responsible for coordinating the PrivTAM computation process. Time is divided into consecutive intervals, and for each interval, an aggregate result is periodically calculated using input from the participating Smart TV's. The TAM Broker is used to facilitate the

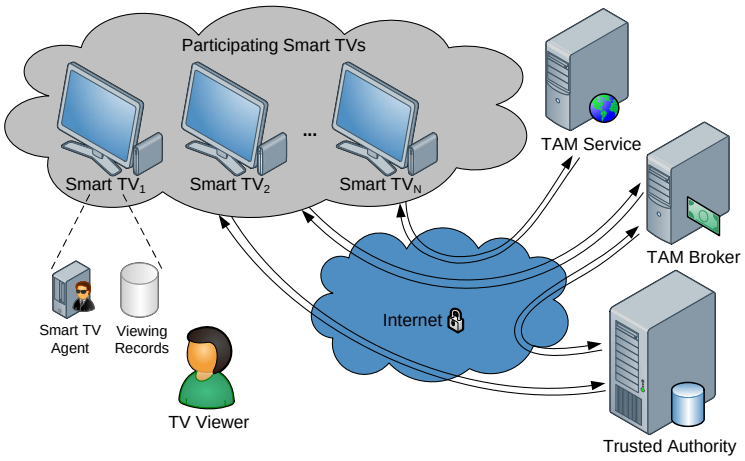


**Fig. 1.** The general architecture of our system.

(optional) payment functionality described in Section 3.2. Each Smart TV agent encrypts its viewership vector with the public-key of the measurement and sends it to the TA for verification. Following a successful verification, the TA adds this vector to the current encrypted result of the measurement. The final encrypted TAM is transmitted to the participants in the distributed key generation for decryption and announcement of the result.

## 3 The PrivTAM Protocol

In this section, we present the cryptographic protocol used in PrivTAM. The communication between the entities in our protocol is performed over secure sockets (SSL/TLS) with both server and client authentication enabled. Our protocol is secure in the Malicious Model, assuming that the TA and the TAM Service are Honest-But-Curious (HBC) (see Section 4). During the calculation the actual users' personal data are not disclosed in any stage of the process, but only the final results are revealed at the end.

### 3.1 Problem Definition

We define the PrivTAM problem for verifiable, privacy-preserving TAM. A PrivTAM problem instance consists of:

- **N Smart TVs** - $TV_1, TV_2, \ldots, TV_N$ and the viewing records of their owners.
  - **Input:** The viewership vector of each owner.
  - **Output:** The TAM for the participating viewership vectors.

We assume that one viewership vector is submitted per Smart TV. We do not consider user identification issues within family members, as this is an existing issue in TAM systems and is out of the scope of this work.

### 3.2 Outline of the Computation

The computation consists of three main phases. In Figure 2, the participating entities of each phase are illustrated. The full descriptions of the three phases are given in the following paragraphs.

- In Phase 1 a distributed key generation for a Threshold Paillier Cryptosystem is performed.
- In Phase 2 the privacy-preserving TAM calculation takes place.
- In Phase 3 the final encrypted TAM is forwarded for decryption and the result is announced.

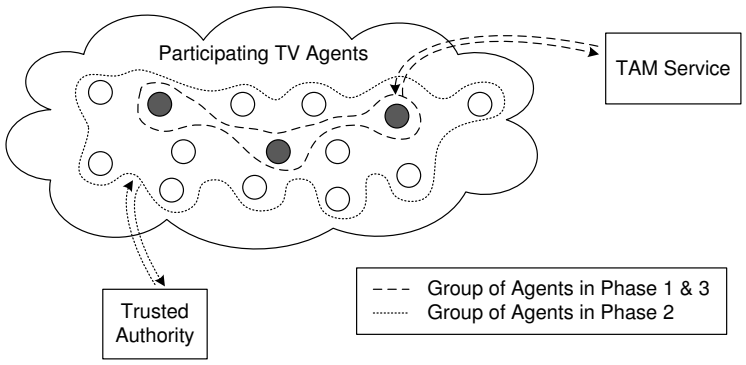


**Fig. 2.** Illustration of protocol participants.

**Phase 1.** During Phase 1 the TAM Service selects an $L$-sized subset of the $N$-sized set of all the participating TV agents with a verifiably random procedure. An example of a publicly verifiable random selection process is described in [7]. This technique prevents the TAM Service from making a biased or impeachable group selection. Then, the TAM Service and the $L$ selected TV agents execute a cryptographic protocol for the distributed key generation of the Threshold Paillier Cryptosystem [6]. We use the following Threshold Decryption Model, which is an adaptation of the corresponding definition in [4] to our needs, so that the distributed key generation can be performed without a trusted dealer [13].

**Definition 1 (Threshold Decryption Model).** *In a threshold cryptosystem, instead of merely decrypting the encrypted message, we use $n$ parties $P_i$ with their secret keys, so that at least $t$ parties, where $t \leq n$, are required to decrypt the message. The decryption process includes the following players: a combiner (can be one of the $n$ parties), a set of $n$ parties $P_i$, and users. We consider the following scenario:*

- *In an initialization phase, the parties use a distributed key generation algorithm to create the public key $PK$ of their private keys $SK_i$. Next the parties publish their verification keys $VK_i$.*

- *To encrypt a message, any user can run the encryption algorithm using the public key $PK$.*
- *To decrypt a ciphertext $c$, we forward $c$ to the combiner and $n$ parties. Using their secret keys $SK_i$ and their verification keys $VK_i$, each party runs the decryption algorithm and outputs a partial decryption $c_i$ with a proof of validity of the partial decryption $proof_i$. Finally, the combiner uses the combining algorithm to recover the cleartext, provided that at least $t$ partial decryptions are valid.*

In PrivTAM, we use the Paillier public key generated in Phase 1 for the encryption of the viewership vectors and utilize the Pailler Cryptosystem's homomorphic property in Phase 2. In addition, we specify that $t$ is equal to $n$ in our Threshold Decryption Model, meaning that all the parties are required to decrypt a message. Setting $t = n$ is important to ensure that the final result cannot be decrypted without the active participation of the TAM Service. Phase 1 should be repeated occasionally, to renew the keys and the set of $L$ agents.

**Phase 2.** During this phase, the TA coordinates the voting process, and collects and verifies the encrypted viewership vectors of the participants. Upon successful verification, the TA adds the submitted viewership vector to the current TAM result, and sends the compensation to the participant.

In detail, Phase 2 begins with the TV agents that hold viewing records for the particular time period, creating their viewership vectors (Figure 3). Each such vector is submitted to the TA for the verification. The verification process is based on a zero-knowledge proof that an encrypted message lies in a given set of messages [4]. This way, when encrypting a message, it is possible to append a proof that the message lies in a public set $S = \{m_1, \cdots, m_p\}$ of $p$ messages without revealing any further information. This proof is described in detail in Section 4.

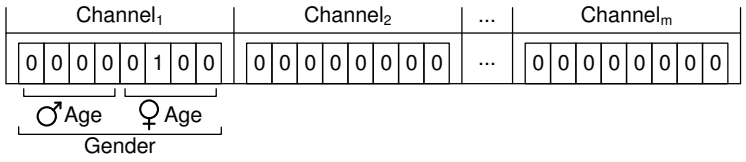


**Fig. 3.** Example of a viewership vector.

In Figure 3, the viewership vector for $m$ TV channels is illustrated. The vector section for each channel consists of a number of ciphertexts, which result from the number of demographic elements used in the vector. In our example, these elements are the age group and the gender of the viewer. The gender categories are male and female and the age groups are "$Age_1 \leq 24$", "$25 \leq Age_2 \leq 40$", "$41 \leq Age_3 \leq 55$" and "$Age_4 > 55$". Consequently, a combination of 8 ciphertexts is created to represent these elements. In order to indicate the channel the

viewer was watching, the representation of their demographic elements are added to the viewership vector section for the corresponding channel. For example, in our case the gender is female, the age is between 25 and 40 years old and she was watching $Channel_1$. All the values in the viewership vector lie in the public set $S = \{0, 1\}$ and they are encrypted using the public key that is generated in Phase 1. Every participant should prove that their vector is valid so that the TA can avoid any malicious behavior from them. More specifically, the participants should prove that:

1. Every ciphertext in the viewership vector should lie in the set $S = \{0, 1\}$.
2. The multiplication of the ciphertexts in every channel should lie in the set $S = \{0, 1\}$.
3. Finally, the multiplication of all ciphertexts in the viewership vector should equal to "1". This means that the participant was watching TV.

The multiplication of the ciphertexts in the above proofs utilizes the homomorphic property of the Paillier Cryptosystem [14]. Using homomorphic encryption one can perform a specific algebraic operation on the plaintext by performing a (possibly different) algebraic operation on the ciphertext. The additive homomorphic property of the Paillier cryptosystem, if the public key is modulus $m$, is shown in the following equation:

$$\mathcal{E}(x_1) \cdot \mathcal{E}(x_2) = \mathcal{E}(x_1 + x_2 \bmod m)$$

Once the viewership vector is confirmed by the TA, the vector is multiplied, using the homomorphic property, with the current TAM result. We assume that the TA only logs the participants in a measurement in order to ensure unreusability of the vectors. However, even if the vectors were stored, the TA would not be able to reveal their contents, unless all the participants of the threshold decryption are malicious and collude towards this purpose. The final result of Phase 2 is the encrypted TAM of the particular query, which ensures k-anonymity (see Section 4).

***Payments in PrivTAM.*** The PrivTAM system can support functionalities for the compensation of participants, either in the form of financial payments or in the form of vouchers or points. The requirement for a participant to be compensated is that they provide a valid viewership vector to the computation. After the successful verification of a participant's viewership vector, the TA sends the compensation to the participant.

In case of financial compensation, the payment scheme within PrivTAM needs to be efficient enough to facilitate large numbers of small amount payments, without entailing substantial transaction costs. Therefore, we draw techniques along the lines of micropayments, as proposed in [16]. The main actors in micropayment schemes are Brokers, Vendors and Users. A User becomes authorized to make micropayments by the Broker. A Vendor receives micropayments from authorized users and redeems them through the Broker. Relationships of Users and Vendors with the Broker are long term. In PrivTAM, the Smart TV

owners can act as Vendors and the TA can act as a user making micropayments. The TAM Broker is introduced in the architecture to facilitate the payments (Figure 1). A micropayment scheme suitable for PrivTAM is Payword, presented in [16]. Payword is a credit-based scheme, based on chains of hash values (called Paywords) and the Broker does not need to be online in order for a transaction between a User and a Vendor to take place. Due to lack of space, the Payword protocol is not presented here.

Alternatively, non-monetary compensation, including points that can be redeemed with participating companies, can be offered to participants. The amount of compensation for each PrivTAM calculation is fixed for simplicity, but methods for providing different pricing could be introduced into the system. It is important to stress that the collected points of each participant are not recorded in a profile by a centralized service, but are kept at the participant's side.

**Phase 3.** In Phase 3, the final encrypted result of Phase 2 is forwarded to the $L$ selected TV agents of Phase 1 and the TAM Service. The $L$ agents perform partial decryptions and send the results to the TAM Service which acts as the final participant and combiner of the threshold decryption. This way, only the TAM Service can see the final result of the calculation, which is acceptable if the TAM Service is considered honest and reports accurately the decrypted result. In order for the PrivTAM calculation to be protected from inaccurate reporting of the results from the TAM Service, a verification mechanism can be introduced to validate the announced results. This verification could be accomplished by using multiple combiners in the threshold decryption, to confirm the announced results from the TAM Service.

## 4 The Protocol's Security

In this section, we show that the PrivTAM protocol achieves the requirements described in the introduction, i.e., privacy, completeness, soundness, unreusability, eligibility, and verifiability. The security model holds for Malicious viewers, with the assumption that the TA and the TAM Service are Honest-But-Curious (HBC). Malicious users can submit any value as input to the computation or even abandon the protocol at any step. See the definition of the Malicious Model given in [10] or the more detailed description in [8]. An Honest-But-Curious party (adversary) [2] follows the prescribed protocol properly, but may keep intermediate computation results, e.g. messages exchanged, and try to deduce additional information from them other than the protocol result.

The security of the Threshold Paillier cryptosystem and its homomorphic property ensures that the viewing records are never disclosed and cannot be associated with any particular participant. To prove the privacy attribute of the protocol, we show that it satisfies the criterion of k-anonymity [5]. In the context of this work, k-anonymity means that no less than k individual users can be associated with a particular personal viewing record.

The following zero-knowledge proof illustrates the steps of the verification process in Phase 2. The security of this zero-knowledge proof is shown in [4].

**Proof that an encrypted message lies in a given set of messages [4].** Let $N$ be a $k$-bit RSA modulus, $\mathcal{S} = \{m_1, \cdots, m_p\}$ a public set of $p$ messages, and $c = g^{m_i} r^N \mod N^2$ an encryption of $m_i$ where $i$ is secret. In the protocol, the prover $P$ convinces the verifier $V$ that $c$ encrypts a message in $\mathcal{S}$.

1. $P$ picks at random $\rho$ in $\mathbb{Z}_N^*$. He randomly picks $p-1$ values $\{e_j\}_{j \neq i}$ in $\mathbb{Z}_N$ and $p-1$ values $\{\upsilon_j\}_{j \neq i}$ in $\mathbb{Z}_N^*$. Then, he computes $u_i = \rho^N \mod N^2$ and $\{u_j = \upsilon^N (g^{m_j}/c)^{e_j} \mod N^2\}_{j \neq i}$. Finally, he sends $\{u_j\}_{j \in \{1,\cdots,p\}}$ to $V$.
2. $V$ chooses a random challenge $e$ in $[0, A[$ and sends it to $P$.
3. $P$ computes $e_i = e - \sum_{j \neq i} e_j \mod N$ and $\upsilon_i = \rho r^{e_i} g^{(e - \sum_{j \neq i} e_j) \div N} \mod N$ and sends $\{\upsilon_j, e_j\}_{j \in \{1,\cdots,p\}}$ to $V$.
4. $V$ checks that $e = \sum_j e_j \mod N$ and that $\upsilon_j^N = u_j (c/g^{m_j})^{e_j} \mod N^2$ for each $j \in \{1, \cdots, p\}$.

We note that $r$ is the random number which was used for the encryption of message $m_i$ and $a \div b$ is the quotient in the division of $a$ by $b$. According to Theorem 2 of [4], it holds that $t$ iterations of the above protocol is a perfect zero-knowledge proof (against an honest verifier) that the decryption of $c$ is a member of $\mathcal{S}$, for any non-zero parameters $A$ and $t$ such that $1/A^t$ is negligible.

The main security features of the protocol are:

- The TA cannot obtain information about the contents of the viewership vector, since the ciphertexts are encrypted with the Paillier encryption.
- In case the TA stores the viewership vector, the contents cannot be revealed unless all the participants in the threshold decryption are malicious and collude towards this purpose.
- The participants cannot submit invalid viewership vectors and disrupt the calculation, due to the verification process.
- At the end of the protocol, only the aggregate TAM result is revealed. As a result, no individual can be associated with the viewership vector that they submitted. Consequently, the proposed protocol preserves k-anonymity for $k = N$, where $N$ is the number of all the participants who take part in the measurement.
- In order to be protected from inaccurate result reporting from the TAM Service, multiple combiners can be introduced in Phase 3, to confirm the announced results.

## 5 Experimental Results

To evaluate our solution, we developed a prototype that implements the Priv-TAM calculation. The prototype can be separated into two main parts, the first being the application on the Smart TVs and the second the application on the TA. The Smart TV application is implemented using the Google TV platform[3] and the Java for Android 3.1 SDK. The application on the TA is also

[3] http://www.google.com/tv/

implemented in Java. Both applications use the cryptographic primitives of the Paillier Threshold Encryption Toolbox [21]. In this library, a centralized mechanism (with a trusted dealer) for threshold key generation [6] is implemented, instead of a distributed Paillier key generation [13]. In our view, this is enough for this prototype implementation.

The TV agents use production-ready cryptographic libraries and employ 1024 bits RSA X.509 certificates. The communication between agents is performed over secure sockets (SSL/TLS) with both client and server authentication. At this stage, the full functionalities of the TV agents described in our proposed system are not implemented, rather, we only implement the privacy-preserving cryptographic TAM computation.

We performed an experiment of the PrivTAM calculation, where 6 TV agents, the TA and the TAM Service participated and four channels exist. Each agent generated random values for the submitted viewing record, as well as for the gender and the age of the viewer. Initially, the TAM Service randomly chooses two of the participating TV agents ($L = 2$), $TVAgent_2$ and $TVAgent_5$, for the first phase of the protocol. Therefore, the final encrypted measurement will be decrypted from $TVAgent_2$, $TVAgent_5$ and the TAM Service ($n,\ t = 3$ parties).

Next, each TV agent encrypts the viewership vector and transmits it to the TA for verification. This process in our experiments takes less than 8 seconds. Once the viewership vector is verified, the TA multiplies it with the current encrypted TAM result. In Table 1 the values used to create the viewership vector of each agent are shown, along with the resulting current encrypted measurement after the submitted viewership vector is calculated by the TA.

**Table 1.** Example of a PrivTAM.

| **TV Agents Values** | | | | **Current Encrypted TAM** | | | |
|---|---|---|---|---|---|---|---|
| Agent | Channel | Gender | Age | $Channel_1$ | $Channel_2$ | $Channel_3$ | $Channel_4$ |
| $TVAgent_1$ | $Channel_3$ | Male | 23 | 0000 0000 | 0000 0000 | 1000 0000 | 0000 0000 |
| $TVAgent_6$ | $Channel_1$ | Female | 45 | 0000 0010 | 0000 0000 | 1000 0000 | 0000 0000 |
| $TVAgent_2$ | $Channel_1$ | Male | 32 | 0100 0010 | 0000 0000 | 1000 0000 | 0000 0000 |
| $TVAgent_4$ | $Channel_4$ | Female | 29 | 0100 0010 | 0000 0000 | 1000 0000 | 0000 0100 |
| $TVAgent_3$ | $Channel_3$ | Female | 53 | 0100 0010 | 0000 0000 | 1000 0010 | 0000 0100 |
| $TVAgent_5$ | $Channel_3$ | Female | 22 | 0100 0010 | 0000 0000 | 1000 1010 | 0000 0100 |

At the end of the computation, the TA sends the encrypted results to $TVAgent_2$, $TVAgent_5$ and the TAM Service. The TAM Service collects the partial decryption results from $TVAgent_2$ and $TVAgent_5$, and combines the partial decryption results. The decrypted TAM result, is shown in the last row of Table 1, where $Channel_3$ has the highest audience (50%) and the 66.66% of viewers were women. A snapshot of the application during the execution of the experiment is shown in Figure 4.

**Fig. 4.** A snapshot of the $TVAgent_5$.

## 6 Conclusions

The introduction of Internet connectivity and computation capabilities to contemporary television systems, opens the possibility of conducting TAMs using larger samples of viewers. In this work we design an efficient protocol for privacy-preserving TAMS and test the applicability of the proposed solution. The accuracy and trustworthiness of the produced results act as strong incentives for TAM Services to adopt the PrivTAM system. From the viewers' perspective, PrivTAM offers the privacy assurance necessary for them to participate in a TAM system, while fair compensation can be offered for their participation, returning some of the economic benefits of TAMs back to the viewer. Additionally, PrivTAM can support alternative kinds of measurements, providing interesting information about audiences to the TV industry. These results are achieved without using any specialized equipment and can take into account data from multiple broadcasted sources.

**Acknowledgments.** This work was performed in the framework of and partially funded by the GSRT/CO-OPERATION/SPHINX Project (09SYN-72-419) (http://sphinx.vtrip.net).

## References

1. Acquisti, A.: Privacy and security of personal information: Technological solutions and economic incentives. In: Camp, J., Lewis, R. (eds.) The Economics of Information Security. pp. 165–178. Kluwer (2004)

2. Acquisti, A., Gritzalis, S., Lambrinoudakis, C., De Capitani di Vimercati, S.: Digital privacy. Auerbach Publications, Taylor & Francis Group (2008)
3. Adar, E., Huberman, B.: A market for secrets. First Monday 6(8) (2001)
4. Baudron, O., Fouque, P.A., Pointcheval, D., Stern, J., Poupard, G.: Practical multi-candidate election system. In: PODC 2001. pp. 274–283. ACM, New York (2001)
5. Ciriani, V., Capitani di Vimercati, S., Foresti, S., Samarati, P.: $\kappa$-anonymity. In: Secure Data Management in Decentralized Systems, Advances in Information Security, vol. 33, pp. 323–353. Springer, Heidelberg (2007)
6. Damgård, I., Jurik, M.: A generalisation, a simplification and some applications of paillier's probabilistic public-key system. In: PKC 2001. pp. 119–136. Springer, London (2001)
7. Eastlake 3rd, D.: Publicly Verifiable Nominations Committee (NomCom) Random Selection. RFC 3797 (Informational) (Jun 2004)
8. Goldreich, O.: The Foundations of Cryptography, vol. 2. Cambridge University Press (2004)
9. Karlof, C., Sastry, N., Wagner, D.: Cryptographic voting protocols: a systems perspective. In: 14th USENIX Security Symposium. pp. 33–50 (2005)
10. Kissner, L., Song, D.: Privacy-preserving set operations. In: CRYPTO 2005, LNCS, vol. 3621, pp. 241–257. Springer, Heidelberg (2005)
11. Kleinberg, J., Papadimitriou, C., Raghavan, P.: On the value of private information. In: TARK 2001. pp. 249–257. Morgan Kaufmann Publishers Inc. (2001)
12. Kremer, S., Ryan, M., Smyth, B.: Election verifiability in electronic voting protocols. In: ESORICS 2010. pp. 389–404. Springer, Heidelberg (2010)
13. Nishide, T., Sakurai, K.: Distributed paillier cryptosystem without trusted dealer. In: WISA 2010. pp. 44–60. Springer, Heidelberg (2010)
14. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: EUROCRYPT 1999. LNCS, vol. 1592, pp. 223–238. Springer (1999)
15. Pieprzyk, J., Hardjono, T., Seberry, J.: Fundamentals of computer security, chap. 15. Monographs in theoretical computer science, Springer (2003)
16. Rivest, R.L., Shamir, A.: PayWord and MicroMint: two simple micropayment schemes. In: CryptoBytes. vol. 2, pp. 69–87 (1996)
17. Shi, J., Zhang, R., Liu, Y., Zhang, Y.: PriSense: Privacy-preserving data aggregation in people-centric urban sensing systems. In: IEEE INFOCOM 2010. pp. 1–9. IEEE (March 2010)
18. Tasidou, A., Efraimidis, P.S., Katos, V.: Economics of personal data management: Fair personal information trades. In: Next Generation Society. Technological and Legal Issues, LNICST, vol. 26, pp. 151–160. Springer, Heidelberg (2010)
19. US Government: The cable tv privacy act of 1984. In: 47 USC, Chapter 5, Subchapter V-A, Part IV, Sec. 551. U.S. Gov. Printing Office, Washington, DC (1984)
20. US Government: Video privacy protection act. In: 18 USC, Part I, Chapter 121, Sec. 2710, Pub.L. 100-618. U.S. Gov. Printing Office, Washington, DC (1988)
21. UTD Data Security and Privacy Lab: Paillier threshold encryption toolbox (November 2011), http://www.utdallas.edu/∼mxk093120/cgi-bin/paillier/
22. Varian, H.: Economic aspects of personal privacy. In: Privacy and self-regulation in the information age. NTIA, Washington, DC (1997)
23. Yao, A.C.C.: Protocols for secure computations (extended abstract). In: FOCS 1982. pp. 160–164. IEEE, Los Alamitos (1982)