International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-027 PAGE NO: 142-145

PARQ BASED RANGE QUERYPREDICATE IN GRID COMPUTING

C.MENAGA
PG IN COMPUTER SCIENCE AND ENGINEERNG
NPR COLLEGE OF ENGINEERING AND TECH
NATHAM,DINDIGUL DT),INDIA

H.PRABHA

ASSISTANT PROFESSOR IN COMPUTER SCIENCE AND ENGINEERNG
NPR COLLEGE OF ENGINEERING AND TECH
NATHAM,DINDIGUL (DT),INDIA

Abstract— **Smart grid, envisioned as an indispensable power infrastructure, is featured by real-time and two-way communications. How to securely retrieve and audit the communicated metering data for validation testing is, however, still challenging for smart grid. In this paper, we propose a novel privacy-preserving range query (PaRQ) scheme over encrypted metering data to address the privacy issues in financial auditing for smart grid. Our PaRQ allows a residential user to store metering data on a cloud server in an encrypted form. When financial auditing is needed, an authorized requester can send its range query tokens to the cloud server to retrieve the metering data. Specifically, the PaRQ constructs a hidden vector encryption based range query predicate to encrypt the searchable attributes and session keys of the encrypted data. Meanwhile, the requester's range query can be transferred into two query tokens, which are used to find the matched query results. Security analysis demonstrates that in the PaRQ, only the authorized requesters can obtain the query results, while the data confidentiality and query privacy are also preserved. The simulation results show that our PaRQ can significantly reduce communication and computation costs.**

Keywords: Privacy, Smart Grid, Statistics, Aggregation, Stream, Fault-Tolerance

I. INTRODUCTION

The concept of smart grid refers to the modernization of the existing electrical grid, including bidirectional communication between meters and utilities, more accurate meter readings. Expected electricity savings depend on matching generation and demand, achieved partly through dynamic taris with higher rates during peak consumption periods.

Further savings are expected through the use of smart meter data for more accurate forecasting,

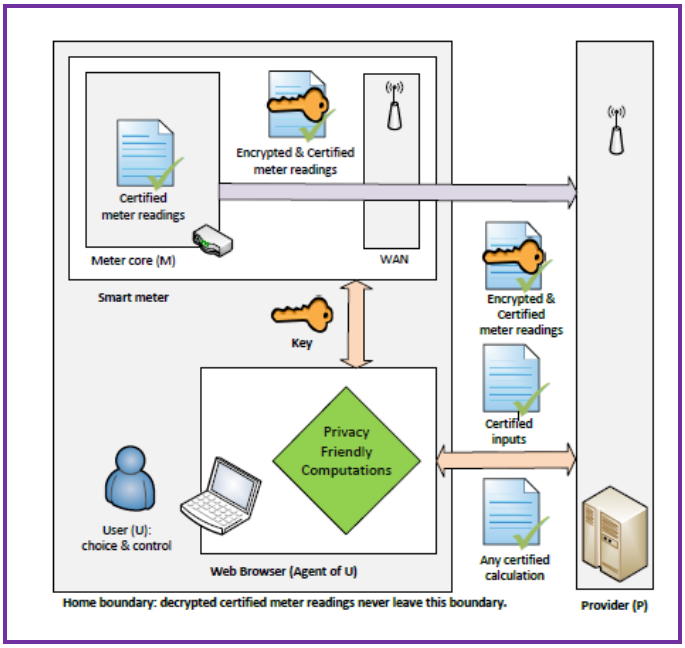
Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-027 PAGE NO: 142-145

more accurate settlement of costs between suppliers and producers as well as customised energy efficiency advice. Both the United States and the European Union currently promote the deployment of smart grids. Currently, most smart grid deployment projects lean towards an architecture with severe privacy problems meters send all negrained measurements to the utilities or a centralised database. Yet, it is recognised that meter readings leak personal information.

For example, load monitoring allows the identication of special electrical appliances. As a result, detailed consumption data would facilitate the creation of user lifestyle process, including but not limited to house occupancy, meal times, working hours, or prayer or fasting patterns. To alleviate such concerns, privacy impact assessments (PIA) are included in ongoing standardization processes. The National Institute of Standards and Technology (NIST) lists ne-grained readings as being used for load monitoring, forecasting, demand-response, efficiency analysis and billing. Time-of-use billing is a major reason for collecting and storing all _ne-grained readings, and thus we use it to illustrate our techniques.

Consumer privacy concerns have already jeopardised the mandatory deployment of smart meters in the Netherlands , leading to a deployment deadlock. This deadlock stems from the assumption that smart metering is necessarily privacy invasive and that a balance needs to be struck between privacy and the social utility of ne-grained billing. Our work refutes this assumption: we demonstrate an architecture that guarantees privacy and high integrity for a very broad set of smart-metering and billing applications.



II.Preliminaries

Signature Schemes: A signature scheme consists of
the algorithms (Keygen; Sign;Verify). Keygen(1k) outputs a key pair (sk; pk). Sign(sk;m) outputs a signature s on message m. Verify(pk; s;m) outputs accept if s is a valid signature on m and reject otherwise.
This definition can be extended to support multi-block messages ~m = fm1 Existential unforgeability requires that no probabilistic polynomial time adversary should be able to output a message-signature pair (s;m) unless he has previously obtained a signature on m.

Commitment schemes: A non-interactive commitment scheme consists of the algorithms ComSetup, Commit and Open. ComSetup(1k) generates the parameters of the commitment scheme parc. Commit(parc; x) outputs a

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-027 PAGE NO: 142-145

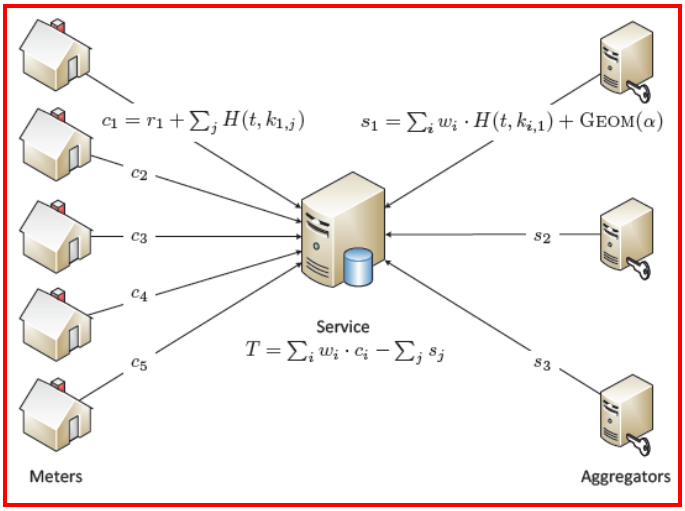
commitment cx to x and auxiliary information openx. A commitment is opened by revealing (x; openx) and checking whether Open(parc; cx; x; openx) outputs accept. The hiding property ensures that a commitment cx to x does not reveal any information about x, whereas the binding property ensures that cx cannot be opened to another value x0. Our fast protocols use homomorphic commitment schemes extensively. A commitment scheme is said to be additively homomorphic if, given two commitments cx1 and cx2 with openings (x1; openx1) and (x2; openx2) respectively, there exists an operation such that, if c = cx1 cx2 , then Open(parc; c; x1 + x2; openx1 + openx2) outputs accept. Additionally, we require a commitment scheme that also provides an operation between a commitment cx1 and a value x2 such that, if c = cx1 _x2, then Open(parc; c; x1 _x2; openx1 _x2) outputs accept.

For the purposes of proving security, we employ a trapdoor commitment scheme, in which algorithm ComSetup(1k) generates parc and a trapdoor td. Given a commitment c with opening (x1; openx1) and a value x2, the trapdoor td allows finding openx2 such that algorithm Open(parc; c; x2; openx2) outputs accept.

Proofs of Knowledge: A zero-knowledge proof of Knowledge is a two-party protocol between a prover.

III.APPLICATIONS TO SMART METERING

Smart-meters collect information about household electricity usage or generation at a granularity ranging from 15 to 30 minutes. Aggregates of these results are used by different actors in the energy industry: energy distributors, providers and generators require timely statistics to support their business processes; distributors require statistics about the peak loads that particular lines may be subject to; while providers need to know the exact consumption of their customer base for every settlement period. All entities require statistics to support the development of their future services or financial forecasting at different geographic or demographic levels. We present and verify a novel protocol that allows readings from smart meters to be aggregated in weighted sums and used by different entities to serve their needs, without compromising the privacy of customers by disclosing fine-grained consumption data.



Furthermore, missing readings due to failing meters or unreliable networks do not impede the aggregation of the readings collected.

Conclusions

We provide a protocol in the fault-tolerant, private distributed aggregation model that allows a data consumer to calculate unbounded statistics (weighted sums) over homomorphically encrypted sensitive data items from data producers. Our protocol is fault-tolerant, as the data consumer can

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-027 PAGE NO: 142-145

choose to calculate over an arbitrary subset of all available data items, Smart-meter privacy is a serious concern and failure to protect it has jeopardised the smart-meter deployments. Naively, it appears that a balance must be struck between the intrusion necessary for time-of-use billing and the claimed social benefits of smart-grids.

i.e., failing data producers do not prevent the statistics calculation. It is also privacy-preserving, because a (possibly distributed) key-managing authority ensures differential privacy before responding to the data consumer's decryption request for the homomorphically encrypted statistics result.

ACKNOWLEDGMENT

I am greatly indebted to my parents and department faculties for their great encouragement and co-operation in all aspects to develop this paper.

I wish to thank everyone who helped us directly or indirectly for the successful completion of this paper.

REFERENCES

1) Mihhail Aizatulin, Andrew D. Gordon, and Jan J□urjens. Extracting and verifying cryptographic models from c protocol code by symbolic execution. 2011.

2) Ross Anderson and Shailendra Fuloria. On the security economics of electricity metering. In The Ninth Workshop on the Economics of Information Security, 2010.

3) Josep Balasch, Alfredo Rial, Carmela Troncoso, Bart Preneel, Ingrid Verbauwhede, and Christophe Geuens.
Pretp: Privacy-preserving electronic toll pricing. In 19th Usenix Security Symposium, August 2010.

4) Privacy-Preserving Smart Metering, Alfredo Rial, George Danezis, Microsoft Research Cambridge, UK.

5) Fault-Tolerant Privacy-Preserving Statistics, Marek Jawurek and Florian Kerschbaum, SAP Research.

6) Verified Computational Differential Privacy with Applications to Smart Metering, Gilles Barthe_, George Danezisz, Benjamin Gr´egoirey, C´esar Kunz_, Santiago Zanella-B´eguelinz

Published by SK Research Group of Companies (SKRGC).