iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3076

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

Handy Intelligent Device to Alert and Ordeit Home Budget for People to Maintain Home Needy without Credit

Dr. S. Hemalatha[1], B. Arulselvi[2], K. Indhumathi[3]
[1]*Professor, Computer Science Department, Panimalar Institute of Technology.*
[2, 3]*IV Year Students of Computer Science Department, Panimalar Institute of Technology.*

Abstract: ***Implement an alert and scheduling for payment system for every month. In this we have an budget for every month like, Grocery, Entertainment, Transportation, Shopping, medical, EB bill and food & vegetables. User has to allot a specific amount as per their expenditure. Android application will monitor the behavior of the user as per the expensed made by the user and alert the user accordingly to cut down the expenses and so as to control the expenses as per the schedule. Same way we connect Eb meter using LiFi and IOT. LiFi Transceiver is connected to both User Eb Meter and Eb Server. The meter readings are calculated through the embedded hardware and sent to the Eb Server via IOT. Same logic is also processed by the android application.***

I. INTRODUCTION

One of the most difficult challenges of implementing a financial plan is budgeting. This is due to the fact that most of us live busy lives and just can't find the time to track every financial transaction. once thought that household budgeting software would make it easier to stay on track. Despite the fact that budgeting software gathers, stores and analyzes financial data, the financial situations barely improve when use these hi-tech solutions. This highlights a critical financial planning concept; most of the time thr financial situations will only improve when decide to change the lifestyles. Budgeting helps and enables to make these sometimes necessary changes. At the core of a household budget is a financial planning statement called the statement of cash flows. This document displays and calculates all of the income (cash inflows) and expenses (cash outflows) of an individual, family. So can create a budget by gathering your financial data, creating a statement of cash flows then forecasting what your income and expenses will be in the future.

II. ARCHITECTURE

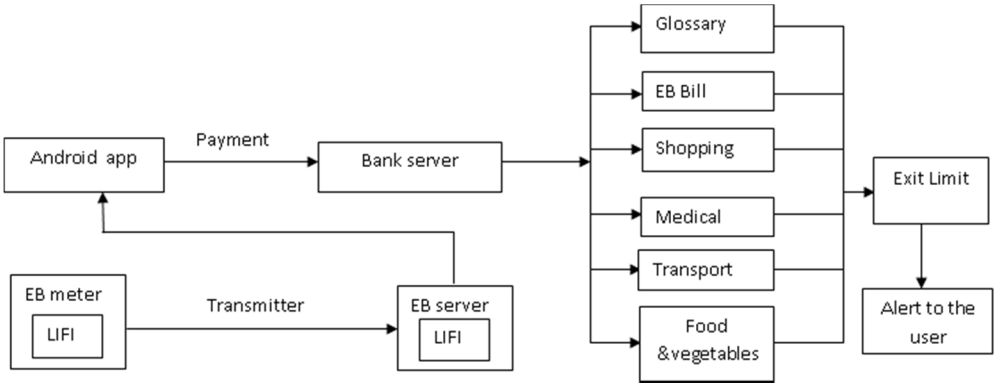


Figure 2.1

This project implementing an alert and scheduling for payment system for every month .In this we have an budget for every month like grocery , entertainment , transportation ,shopping medical ,EB bill and food &vegetables user has to allot a specific amount as per their expenditure .android application will monitor the behavior of the user and alert the user accordingly To cut down the expenses as per the schedule .same way we connect EB meter using LIFI and IOT .LIFI transceiver is connected to both user EB meter and EB server.The meter reading are calculated through the embedded hardware and sent to the EB server via IOT same logic is also processed by the android application. The overall description in figure 2.1

III. LITRETURE SURVEY

Giulio Giaconi, Deniz Gündüz and H. Vincent Poor[1] A wise meter (SM) sporadically measures end-user electricity consumption and reports it to a utility supplier (UP). Despite the benefits of SMs, their use ends up in serious issues concerning shopper privacy. during this paper, SM privacy is studied by considering the presence of AN energy harvest device (EHD) as a method of masking the user's input load. The user will satisfy half or all of his/her energy wants from the EHD, and hence, less data are often leaked to the UP via the SM. The EHD is often equipped with a chargeable energy storag e device, i.e., a battery, whose fast energy content limits the user's capability in covering his/her energy usage. Privacy is measured by the knowledge leaked concerning the user's real energy consumption once the UP observes the energy requeste d from the grid, that the SM reads and reports to the UP. The minimum data outpouring rate is characterized as a calculable data metaphysical single-letter expression once the EHD battery capability is either infinite or zero. Numerica l results ar conferred for a distinct binary input load let's say the potential privacy gains from the existence of a memory device.

Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli[2] It is usually appealing to assume that existing solutions will be directly applied to rising engineering domains. sadly, careful investigation of the distinctive challenges bestowed by new domains exposes its idiosyncrasies, so usually requiring new approaches and solutions. during this paper, we have a tendency to argue that the Bsmart[grid, exchange its unbelievably eminent and reliable precursor, poses a series of recent security challenges, among others, that need novel approaches to the sphere of cyber security. we are going to decision this new field cyber– physical security. The tight coupling between info and communication technologies and physical systems introduces new security issues, requiring a rethinking of the normally used objectives and strategies. Existing security approaches square measure either unsuitable, not viable, insufficiently ascendable, incompatible, or just inadequate to handle the challenges posed by extremely advanced environments like the good grid. A conjunctive effort by the complete trade, the analysis community, and therefore the policy manufacturers is needed to realize the vision of a secure good grid infrastructure.

Fengjun Li*, Bo Luo and Peng Liu[3] In this paper, we have a tendency to gift a distributed progressive information aggregation approach, during which information aggregation is performed in any respect good metres concerned in routing the info from the supplymetre to the collector unit. With a fastidiously created aggregation tree, the aggregation route covers the complete native neighborhood or any discretional set of selected nodes with minimum overhead. to safeguard user privacy, Homomorphic cryptography is employed to secure the info enroute. Therefore, all the metres participate within the aggregation, while not seeing any intermediate or end result. during this manner, our approach supports economical information aggregation in good grids, whereas absolutely protective user privacy. This approach is very appropriate for good grids with repetitive routine information aggregation tasks.

Ishtiaq Rouf∗, Hossen Mustafa∗, Miao Xu, Wenyuan Xu†, Rob Miller and Marco Gruteser[4] In this paper, we've got a bent to gift a distributed progressive info aggregation approach, throughout that info aggregation is performed in any respect sensible metres involved in routing the data from the provision metre to the collector unit. With a painstakingly created aggregation tree, the aggregation route covers the whole native neighborhood or any discretionary set of designated nodes with minimum overhead. to safeguard user privacy, homomorphic cryptography is utilized to secure the data enroute. Therefore, all the metres participate inside the aggregation, whereas not seeing any intermediate or ending. throughout this way, our approach supports economical info aggregation in sensible grids, whereas fully protecting user privacy. This approach is extremely applicable permanently grids with repetitive routine info aggregation tasks.

Andres Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irwin[5] Household sensible meters that live power consumption in period of time at fine granularities area unit the muse of a future sensible electricity grid. However, the widespread readying of sensible meters has serious privacy implications since they unknowingly leak elaborate info concerning unit activities. during this paper, we have a tendency to show that even while not a previousi information of unit activities or prior coaching, it's potential to extract complicated usage patterns from sensible meter information victimisation ready-to-wear applied mathematics strategies. Our analysis uses 2 months of information from 3 homes, that we have a tendency to instrumented to log mixture unit power consumption each second. With the info from our small-scale readying, we have a tendency to demonstrate the potential for power consumption

patterns to reveal a variety of knowledge, like what number folks area unit within the home, sleeping routines, intake routines, etc. we have a tendency to then sketch out the planning of a privacy-enhancing sensible meter design that enables an electrical utility to attain its web metering goals while not compromising the privacy of its customers.

Georgios Kalogridis∗, Zhong Fan∗ and Sagar Basutkar†[6] Smart metering is an important part of the longer term sensible grid development. However, frequent information collected by home sensible meters reveal a wealth o knowledge concerning residential appliance usage. this offersrise to the sensible metering privacy downside. sensible metering information privacy will be protected by employing a battery to mask energy usage profiles. However, such a system in private modifies usage consumption patterns and it should induce a price counting on battery performance and dynamic utility rating. The aim of this paper is to point out a) however info metaphysical namelessness metrics will be wont to live the privacy protection offered by a water-filling power transformation formula, b) however a decent level of protection and a coffee maintenance price will be obtained with fairly sized batteries, and c) what's the impact on the utility and value. Our initial analysis results counsel that it's potential tospeak granular sensible metering info, defend the consumers' privacy at a coffee price, and promote load equalization within the sensible grid. That renders our privacy protection system reasonable.

Zijian Zhang, Zhan Qin, Liehuang Zhu, Jian Weng[7] Smart meters are wide put in to watch residential electricity usage worldwide. This brings a heavy privacy challenge for the shoppers, as a result of the meter readings area unit potential to show their activities within the house. to handle this privacy issue, battery-based privacy protective schemes have already been studied for many years. In these schemes, a chargeable battery will each stop the meter readings from unseaworthy the customer's energy consumption and play a task of saving the price. However, to the most effective of our information, none of the present schemes can do differential privacy and price saving at the same time. during this article, we have a tendency to 1st propose a battery based differential privacy-preserving (BDP) theme. we have a tendency toadditional gift 2 cost-friendly differential privacy-preserving (CDP) themes by extending BDP scheme. Simulation analyses show that the privacy loss of each CDP schemes area unit smaller than the present work. Meanwhile, each CDP schemes stably save the price below multiple rating policies.

Costas Efthymiou and Georgios Kalogridis[8] The security and privacy of future good grid and good metering networks is very important to their rollout and ultimate acceptance by the public: analysis during this space is in progress and good meter users can ought to be confident that their information is secure. This paper describes a way for firmly anonym zing frequent (for example, each few minutes) electrical metering information sent by a sensible meter. though such frequent metering information could also be needed by a utility or current distribution network for operational reasons, this information might not essentially ought to be due to a selected good meter or shopper. It does, however, ought to be firmly due to a selected location (e.g. a gaggle of homes or apartments) inside the electricity distribution network. the tactic represented during this paper provides a third party written agreement mechanism for attested anonymous meter readings that square measure troublesome to go with a specific good meter or client. This technique doesn't preclude the availability of credited metering information that's needed for different functions like request, account management or market research functions.

Georgios Kalogridis, Costas Efthymiou, Stojan Z. Denic, im A.Lewis and Rafael Cepeda[9] Good grid privacy encompasses the privacy information of knowledge} extracted by analysing good metering data. during this paper, we advise that home electric power routing may be wont to moderate the home's load signature so as to cover appliance usage data. specifically, 1) we have a tendency to introduce an influence management model employing a reversible battery, 2) we have a tendency to propose an influence intermixture rule, ANd 3) we have a tendency to appraise its protection level by proposing 3 completely different privacy metrics: an data conjectural(relative entropy), a agglomeration classification, and a correlation/regression one; these square measure tested on completely different metering datasets. This paper sets the bottom for more analysis on the topic of optimising home energy management with regards to activity load signatures.

David Varodayan∗ and Ashish Khisti[10] A rechargeable battery could also be wont to partly shield the privacy of knowledge contained in an exceedingly household's electrical load profile. we have a tendency to represent the system as a finite state model to form tractable the computation of the speed of knowledge escape. Specifically, we have a tendency to use a trellis formulato estimate the mutual info rate between the battery's input and output hundreds. we have a tendency to show that random battery policies will leak twenty sixth less info than a supposed best-effort formula (that holds the

output load constant whenever possible). we have a tendency to finally describe the extension of the technique to additional realistic models of the battery system.

Jesus Gomez-Vilardebo and Deniz Gunduz[11] Smart meter (SM) privacy is studied assumptive that the SM readings, that report the number of energy every user gets from the grid to the utility supplier (UP) at whenever instant, can not be tempered. The privacy is measured by the number of data concerning the users' energy profile leaked to the utility supplier through the SM readings. Privacy are often achieved due to the existence of another energy supply (AES), whose energy generation profile is thought to the UP solely statistically. assumptive that one AES with a given power generation capability serves multiple users, the optimum exploitation of the energy generated by the AES so as to maximise total user privacy is characterized.

Jesus Gomez-Vilardebo and Deniz Gunduz[12] Good meter (SM) measurements offer close to real time data on the electricity consumption of a user to the utility supplier (UP). This information may be wont to extract personal data on the energy consumption patterns of the user. assumptive that the user has access to an alternate energy supply (AES) additionally to the ability grid, SM privacy drawback is studied from associate data suppositional perspective. The energy demand of the user (input load) at when instant may be glad either from the ability grid (output load) or from the AES. it's assumed that the output load may be absolutely tracked by the UP, and therefore the privacy is measured through the data leak rate. For given average and peak power constraints on the AES, privacy-power perform is outlined, and its equivalence to the rate-distortion perform with a distinction distortion live is shown. that specialize in continuous input masses, the privacy-power perform is characterized once there's solely peak power limitation on the AES, whereas the engineer edge is provided for the final case. The sure is shown to be doable for the exponential input distribution.

Sami Zhioua[13] Anonymity protocols area unit a special sort of security protocols that target protective the identities of human action entities during a network communication. during this analysis we tend to explore the notion of obscurity from associate degree information-theoretic purpose of read. we tend to see a protocol as a loud channel that links a collection of anonymous events (inputs) to a collection of observables (outputs). The degree of obscurity of the protocol will then be expressed in terms of what quantity info is being leaked by the channel. In scientific theory, {the info|the knowledge |the data} leaked by a loud channel is given by the notion of mutual information. we tend to propose an alternate live of knowledge escape supported the vector configuration of the strident channel's matrix. we tend to show that a variant of this new live coincides with mutual info which provides a motivating geometric interpretation to mutual info.

Frederic Dupuis, Wei Yu and Frans M. J. Willems[14] This paper presents numerical algorithms for the computation of the capability for channels with non-causal transmitter facet info (the Gel'fand-Pinsker problem) and therefore the rate-distortion perform for supply secret writing with decoder facet info (the Wyner-Ziv problem). The algorithms area unit supported the reformulation of the mutual info expressions in terms of Claude E. Shannon methods.

Simon Li, Ashish Khisti and Aditya Mahajan[15] In smart-metered systems, fine-grained time-series power usage information (load profile) is communicated from a user to the utility supplier. The correlation of the load profile with a user's personal activities leaves open the chance of reasoning attacks. employing a reversible battery, the user will partly obscure its load profile and supply some protection to the personal info mistreatment numerous ways for charging and discharging the battery (battery management policies). mistreatment mutual info because the privacy metric, we have a tendency to study optimum battery management policies for separate alphabets. we have a tendency to show that the matter is developed as a mathematician call method, establish the territory and action area, and mistreatment this framework characterize the optimum policy for the binary alphabet case.

IV. PROPOSED WORK

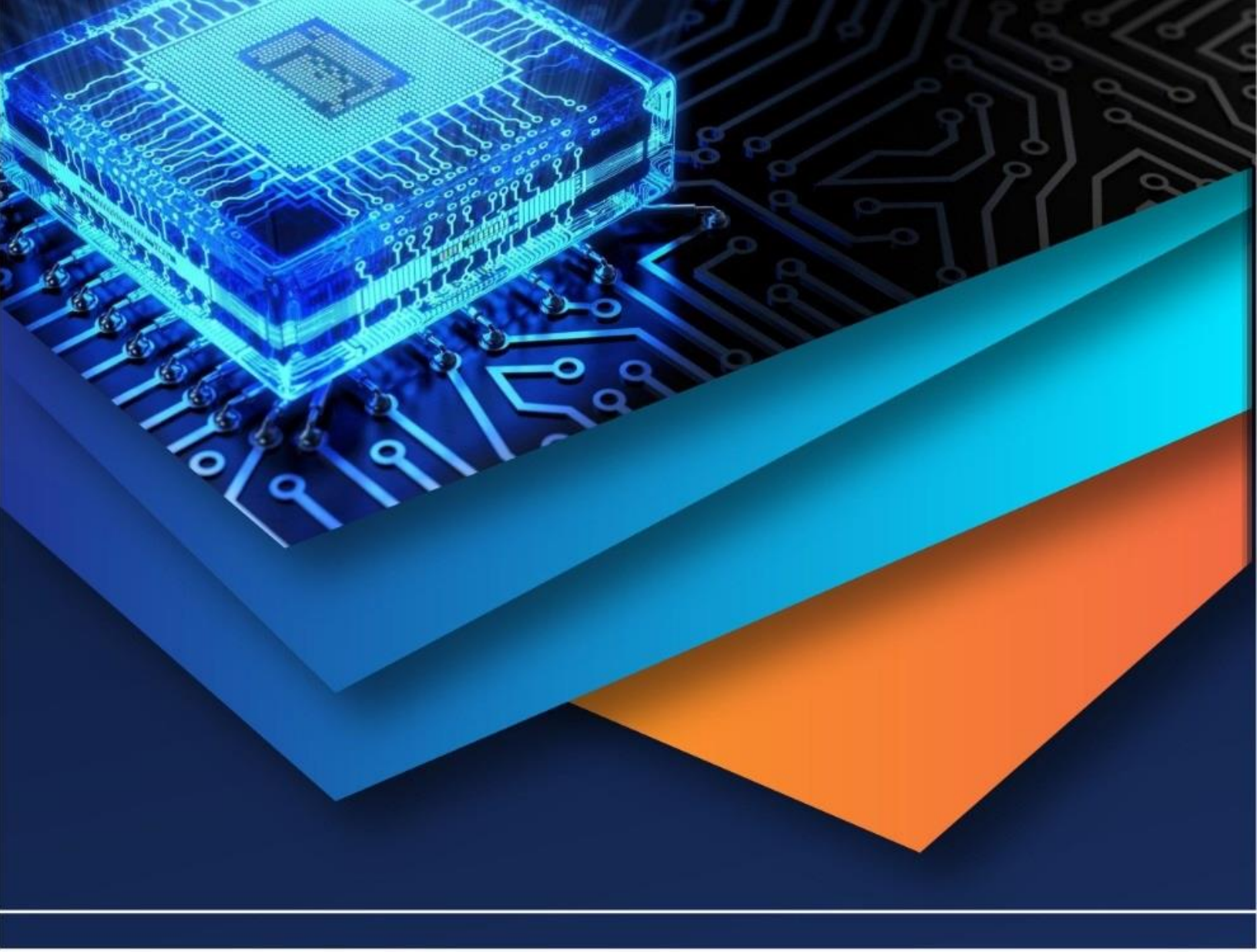
In the proposed system we implement an alert and scheduling for payment system for every month. In this we have an budget for every month like, Grocery, Entertainment, Transportation, Shopping, medical, EB bill and food & vegetables. User has to allot a specific amount as per their expenditure. Android application will monitor the behavior of the user as per the expensed made by the user and alert the user accordingly to cut down the expenses and so as to control the expenses as per the schedule. Same way we connect Eb meter using LiFi and IOT. LiFi Transceiver is connected to both User Eb Meter and Eb Server. The meter readings are calculated through the embedded hardware and sent to the Eb Server via IOT. Same logic is also processed by the android application.

V. CONCLUSION

Implement an alert and scheduling for payment system for every month. In this we have an budget for every month like, Grocery, Entertainment, Transportation, Shopping, medical, EB bill and food & vegetables. The meter readings are calculated through the embedded hardware and sent to the Eb Server via IOT. Same logic is also processed by the android application.

REFERENCES

[1] G. Giaconi, D. Gund ¨ uz, and H. V. Poor, "Smart meter privacy with an ¨energy harvesting device and instantaneous power constraints," in Proc.IEEE Int. Conf. on Commun., London, UK, Jun. 2015, pp. 7216–7221
[2] Y. Mo, T.-H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, andB. Sinopoli, "Cyber-physical security of a smart grid infrastructure,"Proc. IEEE, vol. 100, no. 1, pp. 195–209, Jan. 2012
[3] F. Li, B. Luo, and P. Liu, "Secure and privacy-preserving informationaggregation for smart grids," Int. J. of Security and Networks, vol. 6,no. 1, pp. 28–39, Apr. 2011
[4] I. Rouf, H. Mustafa, M. Xu, W. Xu, R. Miller, and M. Gruteser,"Neighborhood watch: Security and privacy analysis of automatic meterreading systems," in Proc. ACM Conf. on Comput. and Commun.Security, Raleigh, NC, USA, Oct. 2012, pp. 462–473
[5] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin,"Private memoirs of a smart meter," in Proc. ACM Workshop onEmbedded Sensing Systems for Energy-Efficiency in Building, Zurich,Switzerland, Nov. 2010, pp. 61–66
[6] G. Kalogridis, Z. Fan, and S. Basutkar, "Affordable privacy for homesmart meters," in Proc. IEEE Int. Symp. on Parallel and DistributedProcess. with Applicat. Workshops, Busan, Korea, May 2011, pp. 77–8
[7] F. D. Garcia and B. Jacobs, "Privacy-friendly energy-metering viahomomorphic encryption," in Proc. Int. Conf. on Security and TrustManage., Athens, Greece, Sep. 2010, pp. 226–238.
[8] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymizationof smart metering data," in Proc. IEEE Int. Conf. on Smart GridCommun., Gaithersburg, MD, USA, Oct. 2010, pp. 238–243.
[9] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, and R. Cepeda, "Pri-vacy for smart meters: Towards undetectable appliance load signatures,"in Proc. IEEE Int. Conf. on Smart Grid Commun., Gaithersburg, MD,USA, Oct. 2010, pp. 232–237.
[10] D. Varodayan and A. Khisti, "Smart meter privacy using a rechargeablebattery: Minimizing the rate of information leakage," in Proc. IEEE Int.Conf. on Acoust., Speech and Signal Process., Prague, Czech Republic,May 2011, pp. 1932–1935
[11] D. Gund ¨uz and J. G ¨omez-Vilardeb´ o, "Smart meter privacy in the ´presence of an alternative energy source," in Proc. IEEE Int. Conf. onCommun., Budapest, Hungary, Jun. 2013, pp. 2027–2031.
[12] J. Gomez-Vilardeb´ o and D. G´ und ¨uz, "Privacy of smart meter systems ¨with an alternative energy source," in Proc. IEEE Int. Symp. on Inform.Theory, Istanbul, Turkey, Jul. 2013, pp. 2572–2576.
[13] K. Chatzikokolakis, C. Palamidessi, and P. Panangaden, "Anonymityprotocols as noisy channels," Information and Computation, vol. 206,no. 2, pp. 378 – 401, 2008.
[14] R. Blahut, "Computation of channel capacity and rate-distortion func-tions," IEEE Trans. Inf. Theory, vol. 18, no. 4, pp. 460–473, Jul. 1972
[15] S. Li, A. Khisti, and A. Mahajan, "Privacy-optimal strategies forsmart metering systems with a rechargeable battery," arXiv:1510.07170[cs.IT], Aug. 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY