

# Medidores Inteligentes de Consumo Baseados numa Estratégia de Sensoriamento de Multidão

Fábio Rodrigues de la Rocha<sup>1</sup>, Michelle Wangham<sup>2</sup>

<sup>1</sup>Universidade Federal de Santa Catarina (UFSC)  
Araranguá - SC

<sup>2</sup>Universidade do Vale do Itajaí  
São José - SC

fabio.rocha@gmail.com, wangham@univali.br

**Abstract.** *The use of energy becomes more transparent through smart meters, which minimize costs and identify losses and energy thefts. These meters are expensive and still need a communication infrastructure to send consumer data to the service provider. This work explores the widespread use of smartphones to analyze a solution based on crowdsensing to acquire consumption data. This paper presents the advantages and challenges of this new consumption measurement model. A proof of concept demonstrates the proposed solution's functions and assesses its applicability.*

**Resumo.** *Medidores inteligentes tornam mais transparente o uso da energia, minimizando gastos e identificando perdas e furtos. Estes medidores têm um custo alto e necessitam ainda de uma infraestrutura de comunicação para enviar os dados do consumidor até a prestadora de serviço. Este trabalho explora o amplo uso de smartphones para analisar uma solução alternativa baseada em sensoriamento de multidão para a obtenção dos dados de consumo. Neste artigo, são apresentadas as vantagens e desafios que esse novo modelo de medição de consumo apresenta, bem como uma prova de conceito que ilustra o funcionamento da solução proposta e que avalia a sua aplicabilidade.*

## 1. Introdução

Os medidores Inteligentes (*smart meters*) foram desenvolvidos para resolver alguns problemas dos tradicionais medidores MMR (*Manual Meter Reading*) [Zivic et al. 2015] e aprimorar o monitoramento e controle do consumo de energia elétrica. Esses medidores inteligentes são classificados em função de sua capacidade de medição, processamento e comunicação de dados. Medidores inteligentes do tipo EMR (*Electronic Meter Reading*) foram desenvolvidos para dificultar a adulteração do medidor, melhorar a precisão e facilitar a operação de leitura do consumo. Esses medidores tipicamente apresentam o consumo cumulativo e, especificamente, para a energia elétrica, medem o consumo não apenas da energia ativa como também da energia reativa. Alguns destes são dotados de um sistema de transmissão de dados para acesso local, via porta óptica, serial (protocolos RS232, PIMA, etc.) ou ainda RF (*Radio Frequency*). Medidores inteligentes mais avançados, tais como AMR (*Automated Meter Reading*) e AMI (*Advanced Metering Infrastructure*) permitem o envio automático para a distribuidora das medições realizadas usando uma infraestrutura de comunicação, além de capturar dados de outros medidores (tais como medidores de consumo de água/gás). Infelizmente, existem dois desafios para

a implantação de medidores inteligentes avançados: (a) o custo de implantação do medidor e (b) o custo da infraestrutura. O custo de implantação é a principal razão para os medidores MMR e EMR sejam os mais comumente encontrados em residências no Brasil e em outros países em desenvolvimento, visto que a substituição completa destes equipamentos por medidores inteligentes avançados é onerosa. Já o custo da infraestrutura refere-se ao conjunto de elementos necessários para permitir a comunicação de dados desde a residência do consumidor até a distribuidora, onde estes serão armazenados e processados.

Este artigo tem por objetivo descrever uma solução de baixo custo para medição do consumo de energia e seu respectivo envio para a concessionária usando sensoriamento de multidão, *smartphones* e medidores EMR. Na proposta, são utilizados *smartphones* em posse de usuários para criar um sistema de sensoriamento de multidão [Guo et al. 2016], voltado ao envio colaborativo de informações dos medidores. No problema específico dos medidores, o sensoriamento de multidão é relevante pelas vantagens financeiras para a distribuidora de energia, pois não demanda a criação de infraestrutura de comunicação entre medidores e o servidor de dados da distribuidora. Porém, ao incluir a participação de usuários colaborativos, surgem questões de privacidade e segurança que também são investigadas neste artigo.

A Seção 2 analisa os trabalhos relacionados. A Seção 3 apresenta a solução proposta, seguida pela implementação na seção 4. A Seção 5 apresenta os testes e avaliações do protótipo desenvolvido e, por fim, a conclusão e sugestões de trabalhos futuros são apresentadas na Seção 6.

## 2. Trabalhos relacionados

Em [Zhu and Pecun 2008] são apresentados os principais protocolos utilizados em medidores inteligentes. Segundo os autores, algumas soluções de medidores inteligentes utilizam ZigBee em função do baixo consumo de energia do dispositivo e pela intrínseca capacidade de realizar roteamento de mensagens. Porém, apontam como pontos negativos a crescente interferência gerada com o aumento de nós o que torna as conexões e roteamentos instáveis e com grandes atrasos. Argumentam ainda que os sistemas de RF, mesmo sendo utilizados em vários países para AMR, provêm um serviço limitado e que falhas podem ocorrer ao conectar redes de sensores em face de nós distantes ou quando nós do tipo pai falham. Em [Talwar et al. 2016], os autores apresentam um sistema para auxiliar na leitura de consumo de medidores de água, luz ou gás. O sistema é implementado como um aplicativo móvel que captura a imagem de um medidor e reconhece os dígitos analógicos ou digitais, usando algoritmos de reconhecimento de imagens. Segundo os autores, com o processo automatizado, o tempo e a margem de erros pela leitura manual são reduzidos. O sistema não necessita de modificação nem instalação de novos elementos de hardware nos medidores existentes. O artigo aborda apenas a questão de reconhecimento das imagens e não apresenta mais informações como privacidade e segurança dos dados. Na abordagem, ainda é necessária a visita individual a cada medidor por um funcionário da distribuidora de energia. Em [Li and Chong 2019], os autores apresentam o projeto e desenvolvimento de um medidor eletrônico para medição de água. O dispositivo captura a leitura do consumo de água e transmite por *bluetooth* para dispositivos próximos. O usuário precisa inicialmente parear o *smartphone* com o medidor para posteriormente obter o valor da leitura usando um aplicativo móvel. Não são utilizados sistemas de segurança para autenticar o medidor e as medidas capturadas. Em [Cao et al. 2008], é apresentado um modelo composto por medidores eletrônicos ligados em

nós sensores. Os nós sensores (que operam por baterias) capturam os valores de consumo dos medidores e enviam via protocolo *ZigBee* para uma estação coletora que segundo os autores é capaz de capturar dados de até 100 nós sensores. Por sua vez, a estação coletora envia via GSM os dados para a distribuidora de energia. Em função de obstáculos, o sinal dos nós sensores pode ser incapaz de chegar à estação coletora. Nestes cenários existe a figura do repetidor que retransmite os sinais dos nós sensores até a estação base. Nada é mencionado sobre questões de segurança para autenticação do nó sensor o que abre possibilidade de fraude. O sistema necessita de uma grande infraestrutura como repetidores, estação base, além dos nós sensores. Em [Suresh et al. 2017] é apresentado o projeto de um sistema embarcado *bluetooth* mantido por baterias para ser acoplado a um medidor de água. Um *smartphone* com um aplicativo móvel faz o pareamento com o sistema embarcado, conecta e obtém dados deste. Os dados podem ser visualizados ou transmitidos para a distribuidora de energia. O usuário precisa fazer o pareamento e conectar no dispositivo específico o que é inviável para leituras em diversos medidores.

### 3. Solução Proposta

O sistema de medição de consumo proposto é baseado num sistema de sensoriamento eletrônico que utiliza BLE (*Bluetooth Low Energy*) (em função da compatibilidade com os *smartphones* atuais) para comunicação dos dados capturados com usuários de *smartphones* próximos. A comunicação de dados com a distribuidora de energia é realizada utilizando o conceito de sensoriamento de multidão. Os usuários dos *smartphones* próximos recebem os dados dos medidores e utilizam sua própria conexão de dados para propagar as leituras obtidas para a distribuidora de energia. Por sua vez, a distribuidora é informada do consumo da residência e não precisa enviar um funcionário para realizar a medição in loco. Os dispositivos *smartphones* envolvidos podem ser do proprietário da residência, bem como de uma rede de usuários colaborativos, formada para auxiliar o sistema de sensoriamento de consumo.

O sensoriamento de multidão é vantajoso para a distribuidora de energia, mas para ser funcional é necessário motivar os usuários para sua adoção. Os usuários do sistema colaboram com a comunidade, reduzindo custos operacionais da distribuidora que poderiam ser revertidos numa tarifa reduzida. De forma semelhante, a distribuidora pode implementar um sistema de recompensa, visando retribuir (por exemplo, através de descontos) os usuários colaborativos. Finalmente, os usuários também possuem como vantagem a capacidade de acompanhar mais facilmente o seu próprio consumo de energia, manter o histórico de consumo e identificar possíveis desperdícios dentro de sua residência. Como aspectos negativos, há a necessidade de instalação de um aplicativo móvel (que pode comprometer o espaço de armazenamento de alguns *smartphones*), o uso da conexão de dados do usuário e finalmente o aumento do consumo de bateria do *smartphone*.

#### 3.1. Componentes do sistema

A Figura 1 apresenta os atores envolvidos no sistema. O número ① é o medidor BLE, ② os usuários colaborativos e ③ o servidor de aplicação na distribuidora de energia.

O medidor BLE é um sistema eletrônico embarcado, identificado por um *mac-address* e responsável por capturar e enviar por BLE informações para os *smartphones* próximos, tais como, status do medidor, energia ativa, reativa, energia que a residência fornece para a rede, identificação do medidor, bem como parâmetros de qualidade da energia (flutuações de tensão, tempo de interrupção do fornecimento, harmônicas, etc.).

A quantidade de informações está relacionada à quantidade de sensores internos instalados no sistema embarcado. Usuários nas proximidades, em posse de um *smartphone* com um aplicativo móvel instalado, atuam como intermediadores. De forma colaborativa, os usuários capturam e propagam as mensagens para a distribuidora de energia, usando suas próprias conexões de dados. Como exemplo, a Figura 2 apresenta uma visão parcial de uma cidade com medidores BLE na frente de cada residência e dois usuários colaborativos. a) Um caminhão de recolhimento de detritos - no qual o motorista, ao andar pela cidade (utilizando o aplicativo móvel), captura as mensagens dos diversos medidores pelo caminho e as propaga para a distribuidora de energia. b) Uma ciclista, ao pedalar para seu trabalho, realiza a mesma tarefa. Os usuários colaborativos podem ou não ser funcionários da distribuidora de energia, ou atuar em nome desta

Além de contar com usuários colaborativos, pode-se vislumbrar um modelo onde o próprio proprietário da residência informa o valor do seu consumo apenas aproximando o seu *smartphone* do medidor da sua casa. Em qualquer uma das situações, as leituras são automáticas, sem a necessidade da intervenção dos usuários e sem incorrer em falhas humanas durante a leitura do medidor.

O servidor ③ (na Figura 1) é responsável por receber e tratar as mensagens dos usuários e manter os dados da distribuidora atualizados. O aplicativo dos usuários acessa o servidor de aplicação, utilizando uma interface de apresentação ① com uma API (*Application Program Interface*) padronizada. Por meio desta interface, o aplicativo pode consultar o consumo de um usuário validado ② ou atualizar dados de consumo ③. Para atualizar informações de consumo o acesso é realizado através do gerenciador de consumo ④, que por sua vez acessa o banco de dados de consumo. Já a consulta de consumo ⑤, acessa o banco de dados de usuários cadastrados e também do consumo.

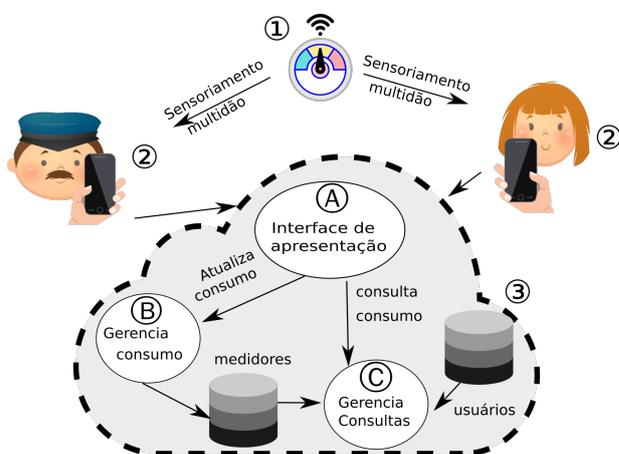


Figura 1. Atores no sistema



Figura 2. Usuários colaborativos

### 3.2. Segurança

O sistema de atualização de dados de consumo é baseado na participação de usuários colaborativos que capturam mensagens e as propagam para a distribuidora de energia. Essa abordagem abre uma brecha de segurança para ataques de usuários maliciosos. Um usuário pode capturar uma mensagem, alterá-la e propagá-la para a distribuidora de energia como sendo uma mensagem original. De forma semelhante, um usuário malicioso pode armazenar uma mensagem e propagá-la num momento futuro para induzir ao erro a distribuidora de energia. Finalmente, um usuário malicioso pode identificar-se como um

medidor inteligente e propagar uma mensagem por *broadcast* na expectativa de que esta seja capturada por um usuário inocente que a propagará para a distribuidora de energia.

Na solução proposta, as questões de segurança são solucionadas por meio do uso de assinaturas digitais das mensagens para prover integridade, autenticidade e não-repúdio. Assinatura digital é implementada usando criptografia assimétrica. Duas opções são apresentadas. A primeira utiliza apenas a assinatura digital das mensagens não mantendo a confidencialidade da informação e é especialmente útil na etapa de implementação e testes do sistema para detectar e apresentar os valores de diversos medidores capturados pelo aplicativo móvel. A segunda abordagem garante a confidencialidade ao adicionar um passo de cifragem ao processo de assinatura da mensagem.

### 3.2.1. Sem confidencialidade das mensagens

Quando um medidor novo é inserido no sistema são criadas chaves públicas e privadas (ex: RSA, ECC). A chave pública é mantida no banco de dados e a chave privada é transferida para o medidor inteligente (Figura 3). Para assinar uma mensagem, o medidor aplica uma função *hash* (ex: SHA-256) na mensagem original, resultando um valor de resumo. O valor de resumo é criptografado utilizando a chave privada e o resultado é adicionado na mensagem original para formar a mensagem que será enviada.

Quando uma mensagem é recebida pelo servidor na distribuidora de energia, o valor do resumo criptografado é separado da mensagem e descriptografado, utilizando a chave pública. A função *hash* é aplicada na mensagem (sem a parte do resumo criptografado) e os valores dos *hashes* são comparados. Caso sejam iguais, a mensagem não foi modificada e a origem da mensagem verificada.

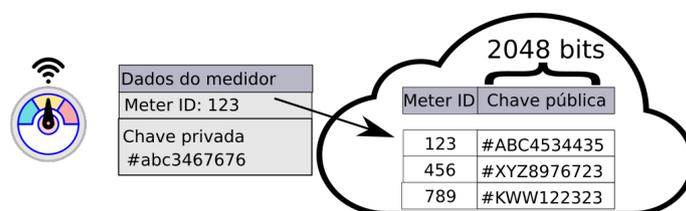


Figura 3. Chave pública e privada mantidas no servidor e nos medidores

### 3.2.2. Com confidencialidade das mensagens

Para manter a confidencialidade das mensagens, o medidor deve possuir, além de sua chave privada, uma cópia da chave pública da distribuidora de energia. Repetem-se os passos para assinar digitalmente a mensagem e, em seguida, usa-se a chave pública da distribuidora para criptografar a mensagem que será enviada. Ao receber a mensagem na distribuidora de energia, a chave privada desta é utilizada para descriptografar a mensagem e, posteriormente, repetir os mesmos passos para verificação da assinatura digital.

## 4. Implementação

Como prova de conceito foi desenvolvido um protótipo de medidor inteligente BLE para medir o consumo de energia elétrica residencial e transmitir os dados de forma segura. Ao invés de desenvolver um sistema embarcado que realize ambas as funções, foi desenvolvido um protótipo que utiliza um medidor convencional EMR para realizar a primeira

função em face da facilidade de desenvolvimento que agrega ao protótipo baixo custo da solução e confiabilidade de um dispositivo homologado.

#### 4.1. Protótipo do medidor BLE

O medidor monofásico padrão utilizado pela CELESC (em julho de 2020) é o LUMEN 3, fabricado pela empresa Nansen, que é um medidor capaz de medir o consumo de energia ativa em sentido direto ou inverso e possui uma porta de dados que segue o padrão de comunicação PIMA [COPEL 2018]. O sistema embarcado é composto por um microcontrolador com uma unidade interna BLE. O microcontrolador ESP32 [Maier et al. 2017] é um dispositivo de baixo custo fabricado pela Espressif e pode ser programado, utilizando o ambiente de desenvolvimento de software livre **Arduino**. Na Figura 4, há as atividades realizadas pelo microcontrolador: (a) captura e interpretação dos dados do medidor de energia por meio do protocolo PIMA; (b) criação de mensagem com a informação de energia consumida/produzida e, bem como sua assinatura digital; (c) transmissão da mensagem usando o protocolo de disseminação de dados sobre o BLE.

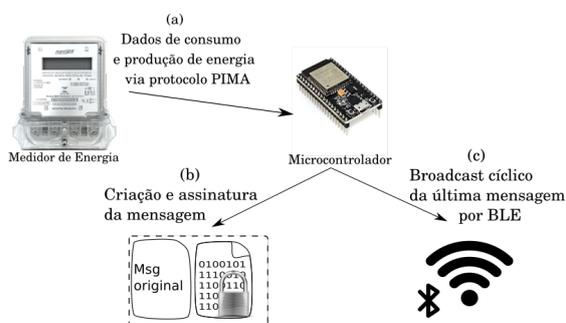


Figura 4. Medidor BLE



Figura 5. Bancada de testes

Para os testes foi desenvolvido um protótipo de bancada que utiliza o mesmo modelo de medidor de energia para compor um medidor BLE (Figura 5). O protótipo é composto pelo medidor de energia, o sistema embarcado (microcontrolador) montado numa *protoboard* e uma fonte de alimentação para o microcontrolador. O protótipo dispõe de uma tomada de 3 pinos onde se conecta a carga que será medida (ex: eletrodoméstico).

##### 4.1.1. Assinatura digital

Para esta prova de conceito, a questão da assinatura digital das mensagens foi simplificada, utilizando um sistema de compartilhamento de segredo. No servidor de aplicação, existe um banco de dados com tuplas compostas pela identificação do medidor e chave (texto fixo gerado aleatoriamente) para cada um dos medidores. Cada medidor possui uma cópia da sua chave e para assinar uma mensagem deve concatenar o conteúdo da informação útil que deseja enviar com a sua chave (técnica chamada *salt*), gerar o *hash*, utilizando a função de dispersão criptográfica (SHA-256) sobre o texto resultante e enviar o resultado, usando o protocolo de disseminação de dados. Ao ser recebida no servidor de aplicação por meio de um usuário colaborativo, a informação útil será separada, concatenada com a chave do medidor associado é gerada a soma SHA-256 correspondente. Essa soma é comparada com a soma SHA-256 que foi recebida na mensagem. Se forem iguais, a mensagem não foi corrompida/adulterada e sua origem verificada.

#### 4.1.2. Protocolo de disseminação de dados

Neste protocolo, os aplicativos móveis dos usuários capturam os pacotes de *advertise* que são transmitidos por *broadcast* e dentro destes pacotes está representada a informação útil do medidor BLE. Os pacotes de *advertise* são pequenos em comparação à quantidade de dados que o medidor envia (*status*, *timestamp*, dados, etc.), o que levou ao desenvolvimento de um protocolo que divide a mensagem original com os dados completos em fragmentos enumerados, os quais são enviados um por vez por *broadcast* dentro do pacote de *advertise*. Os fragmentos são enviados a cada 200ms e o ciclo reinicia após o último fragmento da mensagem ter sido enviado. Os fragmentos são recebidos por um ou mais aplicativos móveis, armazenados e remontados sem que estes fragmentos precisem ser recebidos (corretamente) em ordem crescente. Quando o aplicativo dos usuários estiver com todos os fragmentos pertencentes a uma mensagem, esta é repassada para a próxima camada de software do aplicativo móvel e propagada para a distribuidora de energia, utilizando a conexão de dados do *smartphone*.

No protocolo não existe a necessidade de pareamento e estabelecimento formal de conexão entre o medidor BLE e o *smartphone*. Desta forma, os dados de um medidor BLE podem ser simultaneamente recebidos por diversos aplicativos móveis. Com base no número dos fragmentos, os aplicativos dos usuários sabem se receberam um fragmento de uma mensagem  $X_1$  ou da mensagem  $X_2$ . Ao receber um fragmento que pertence a uma mensagem posterior, os fragmentos armazenados da mensagem anterior são descartados, visto que jamais serão reenviados. O medidor transmite ciclicamente os fragmentos da mensagem corrente, até que uma nova mensagem do medidor esteja disponível.

### 5. Testes e avaliações

Foram realizados dois testes funcionais: a) verificar a captura de dados do medidor, b) recepção dos dados pelo *smartphone* e posterior envio da mensagem para um servidor de aplicação. No teste a), o microcontrolador foi programado para capturar os pacotes de dados enviados via protocolo PIMA e mostrar as informações no terminal serial de um computador. Os valores obtidos corresponderam aos mostrados no *display* LCD do medidor de energia. Já para o teste b), foi desenvolvida uma bancada de testes com 7 microcontroladores ESP32, e cada qual simula um medidor BLE com um número de série entre 1 e 7. Os medidores simulados transmitem como medidas de consumo/produção valores incrementais, iniciando com um valor pré-estabelecido. O protótipo do medidor BLE transmite as medidas reais obtidas (medidor com número de série 55075378). O aplicativo móvel captura os fragmentos e monta os pacotes recebidos pelo protocolo de difusão. Os resultados são apresentados na Figura 6 que apresenta a captura de tela do aplicativo com os endereços *mac-address*, o tipo da mensagem (99 - mensagem de medida de energia), o número de série do medidor, a energia consumida e a energia gerada. O aplicativo também apresenta o tempo desde o recebimento da última mensagem. A assinatura digital e o *timestamp* são recebidos a cada mensagem, mas foram omitidos da tela para facilitar a visualização dos dados. As mensagens capturadas dos medidores foram submetidas pelo aplicativo móvel e corretamente recebidas no servidor de aplicação.

### 6. Conclusão e trabalhos futuros

Este trabalho apresentou um sistema para medição de energia elétrica, baseado numa estratégia de sensoriamento de multidão por *smartphones* e dispositivos BLE. Como prova de conceito, foi desenvolvido um protótipo que utiliza um medidor de energia comercial

Dados recebidos dos medidores BLE						
#	Bluetooth	Signal Strength	RSSI	TX Power	RX Power	Latency
1	3C:71:BF:FE:F9:96	99	3	69	70	3s
2	3C:71:BF:FF:AA:D6	99	1	50	51	1s
3	24:6F:28:96:F0:BE	99	2	37	38	0s
4	30:AE:A4:0B:09:0E	99	6	66	67	3s
5	30:AE:A4:03:47:BE	99	7	75	76	7s
6	A4:CF:12:02:CB:A2	99	4	46	47	0s
7	CC:50:E3:99:19:BA	99	5	56	57	1s
8	30:AE:A4:0C:D6:52	99	55075378	7	0	0s

Figura 6. Detecção dos medidores próximos com suas medições de consumo

homologado e um microcontrolador que captura dados de consumo/produção de energia residencial e os transmite via BLE, utilizando um protocolo próprio de disseminação de dados sem a necessidade de conexão ou pareamento. Foram investigadas questões quanto à segurança das informações transmitidas para identificar e lidar com ataques maliciosos e realizados testes funcionais para avaliar o funcionamento do protótipo. Como trabalhos futuros, pretende-se analisar o custo computacional da criptografia utilizada na assinatura digital das mensagens e estudar o ambiente de execução seguro, desenvolvido para a nova versão do microcontrolador.

## Referências

- Cao, L., Tian, J., and Liu, Y. (2008). Remote real time automatic meter reading system based on wireless sensor networks. In *2008 3rd International Conf. on Innovative Computing Information and Control*. IEEE.
- COPEL (2018). *Etc 3.11 – Especificação Técnica Parasaída Serial Assíncrona Unidirecional*. COPEL. Departamento De Medição Da Distribuição.
- Guo, B., Chen, C., Zhang, D., Yu, Z., and Chin, A. (2016). Mobile crowd sensing and computing: when participatory sensing meets participatory social media. *IEEE Communications Magazine*.
- Li, X. J. and Chong, P. H. J. (2019). Design and Implementation of a Self-Powered Smart Water Meter. *Sensors*.
- Maier, A., Sharp, A., and Vagapov, Y. (2017). Comparative analysis and practical implementation of the ESP32 microcontroller module for the internet of things. In *2017 Internet Technologies and Applications (ITA)*. IEEE.
- Suresh, M., Muthukumar, U., and Chandapillai, J. (2017). A novel smart water-meter based on IoT and smartphone app for city distribution management. In *2017 IEEE Region 10 Symposium*. IEEE.
- Talwar, M., Nimbalkar, P., Bodge, S., Gavit, B., and Mankhair, S. (2016). Android based Meter Reader using OCR Technique. *International Journal of Emerging Technologies and Innovative Research*.
- Zhu, J. and Pecan, R. (2008). A Novel Automatic Utility Data Collection System using IEEE 802.15.4-Compliant Wireless Mesh Networks. In *In Proc. of the IAJC-IJME International Conference*.
- Zivic, N. S., Ur-Rehman, O., and Ruland, C. (2015). Evolution of smart metering systems. In *2015 23rd Telecommunications Forum Telfor (TELFOR)*. IEEE.