Sistema inteligente para controle de acesso e monitoramento de múltiplos ambientes (*class control*)

Vitor V. Pereira, Samaherni M. Dias e Kurios I. P. M. de Queiroz
Laboratório de Automação, Controle e Instrumentação (LACI)
Universidade Federal do Rio Grande do Norte (UFRN), Natal, Brasil
vitorvalepereira@gmail.com, sama@laci.ufrn.br, kurios@laci.ufrn.br

***Resumo*—O conceito de cidades inteligentes vem se expandindo nos últimos anos e está cada vez mais presente em nosso cotidiano, mudando a forma como interagimos com outras pessoas e com a própria cidade. Graças ao progresso da tecnologia da informação, a Internet das Coisas, ou simplesmente IoT, tem contribuído fortemente para o desenvolvimento de soluções inteligentes, aprimorando o monitoramento e controle dos dispositivos. Assim, o problema de gerenciamento de acesso torna-se relevante, motivando o desenvolvimento de soluções para o seu aprimoramento. Este trabalho propõe um sistema de monitoramento e controle de acesso de múltiplos ambientes em um edifício institucional. A arquitetura do sistema proposto será baseada na computação em névoa. Uma trava inteligente foi projetada usando o microcontrolador ESP8266, programado para controlar e monitorar os ambientes com mais eficiência e segurança.**

***Palavras-chave*—Cidades inteligentes, IoT, Tranca inteligente, Computação em névoa**

I. Introdução

O avanço tecnológico na fabricação de semicondutores abriram portas para o desenvolvimento de sistemas embarcados conectados a internet, dando origem a era da internet das coisas (IoT - do inglês *Internet of Things*). Hoje percebe-se que IoT está presente em nossas vidas de várias formas, como no uso de *smartphones*, *tablets*, relógios e até mesmo em óculos, dispositivos estes, que se comunicam com a internet por meio de diversos protocolos de comunicação como Wi-Fi, *bluetooth*, GSM e muitas outras tecnologias.

Com esses avanços surge o conceito de cidades inteligentes, que são cidades que usam informações coletadas e tecnologias de comunicação para que os serviços e monitoramento sejam mais conscientes, interativos e eficientes [1]. Este conceito, que a priori parece futurista, já está fazendo parte da nossa vida cotidiana por meio do uso de diversos dispositivos IoT sendo aplicado em diferentes áreas como automação residencial e industrial, auxílios médicos, assistência médica móvel, assistência a idosos, gerenciamento inteligente de energia e redes inteligentes, automotivo, gerenciamento de tráfego e muitos outros [2].

Entre essas aplicações, o problema de controle de acesso tem se tornado cada vez mais relevante no cenário da internet das coisas e cidades inteligentes, tanto na segurança e gerenciamento de casas e apartamentos como também em ambientes de trabalho onde se faz necessário controlar o acesso a determinados ambientes.

Fechaduras tradicionais são usadas a mais de 4000 anos, sem muita variação de segurança ou sustentabilidade para controle de acesso [3] porém, a urbanização e a diversidade de crimes tem posto à prova sua eficiência [4]. Em grandes complexos de apartamentos, fraternidades ou até mesmo para um proprietário que tenha muitas chaves para cada apartamento, carro ou portão que possui, manter a entrada para pessoas autorizadas é um problema. Além dos custos envolvidos na fabricação, duplicação e distribuição de chaves, há preocupações de segurança em caso de perda de chaves. O uso de um dispositivo de controle de acesso sem chave não só irá resolver todos esses problemas, mas adiciona alguns recursos para sua melhoria [5].

O desenvolvimento de novas tecnologias permitem automatizar inúmeros processos que eram feitos por humanos, podendo assim liberá-los de tarefas simples e repetitivas. As vantagens comumente atribuídas à automação incluem maior produtividade, uso mais eficiente de materiais, maior segurança, diminuição da força de trabalho e redução de tempo desperdiçado. Portanto, este projeto visa automatizar o processo de reservas de múltiplos ambientes em prédios institucionais, bem como monitorar e controlar outros dispositivos associados a cada ambiente com o objetivo de aumentar a segurança e melhorar a eficiência do uso de energia.

De forma mais detalhada, este trabalho propõe o desenvolvimento de um sistema de controle de acesso e monitoramento de múltiplos ambientes, chamado de *class control*, para ser utilizado em salas de aulas equipadas com ar condicionado e retroprojetor. O sistema será responsável por liberar o acesso do usuário (por exemplo um professor) a sala de aula, em horário programado, através de sua identificação por cartão RFID. Além de liberar o acesso do usuário, o sistema também é responsável por monitorar o uso da energia e a climatização do ambiente. A arquitetura do sistema proposto (ver Figura 1) será baseada em computação em névoa, ou seja, um dispositivo de processamento local, um dispositivo de processamento na borda da rede e um dispositivo de processamento em nuvem. Neste projeto cada sala de aula possuirá um dispositivo chamado de tranca inteligente, o qual utiliza um microcontrolador com acesso a rede wi-fi (no

nosso caso o ESP8266) e é o responsável pelo processamento local liberando ou não o acesso e monitorando o ambiente. O processamento na borda da rede será realizado por um microprocessador ARM (*Raspberry Pi*), o qual processa parte dos dados de um conjunto de trancas, assim evitando o envio de um grande volume de dados para a nuvem e adiciona mais robustez ao sistema, pois reduz a dependência do sistema do servidor na nuvem. O processamento em nuvem será realizado por um servidor com um banco de dados e um cliente web para a operação e configuração do sistema *class control*.

II. Referencial bibliográfico

Nos últimos anos, o número de dispositivos conectados a internet vem crescendo a passos largos, porém IoT e cidades inteligentes são conceitos que abrangem diversas áreas do conhecimento, trazendo com isso, complexidade na resolução de problemas relacionados a controle de acesso. Tal desafio tem estimulado o desenvolvimento de diversos tipos de dispositivos inteligentes para este fim.

O trabalho [4] apresenta uma fechadura inteligente cujo o funcionamento consiste na decodificação de sinais ópticos, gerado pelo LED de um *smartphone* e baseados em código morse.

O trabalho [6] propõe uma solução utilizando arquitetura de comunicação baseada em nuvem e que um dispositivo *bluetooth* seria a chave de acesso da tranca, ou seja, caso o portador do dispositivo se aproxime da tranca, ela se abre automaticamente. Esta solução apresenta a vantagem de que qualquer ser humano pode usar este sistema independente de qualquer deficiência física que o mesmo tenha. Outra proposta similar foi desenvolvida em [7] onde a comunicação com a fechadura acontece por meio do protocolo *bluetooth* e a chave de acesso é uma senha de desenho padrão, a mesma que se usa para desbloqueio de *smartphone*.

Os trabalhos [9] e [10] propuseram uma solução para controle de acesso utilizando RFID como chave de acesso, servidor em nuvem e, principalmente o trabalho [10], um alto nível de segurança, pois se trata de um sistema para áreas críticas.

No artigo [15] foi apresentado um sistema utilizando ESP8266 como microcontrolador da tranca inteligente, além de aplicativos para *smartphones* e serviços web se conectando a um servidor via protocolo Wi-Fi. Trabalho similar ao proposto neste artigo.

Os trabalhos relacionados a este tema têm utilizado bastante processamento centralizado em nuvem, juntamente com o uso do *smartphone* e outros dispositivos móveis como chave de acesso para as trancas. O sistema proposto visa diminuir a dependência do servidor em nuvem utilizando computação em névoa, e com isso conferir robustez e tornar o processo de dados mais rápido, retirando carga de processamento da nuvem. Já no desenvolvimento do hardware, o uso do RFID tem como objetivo simplificar a forma de interação com a tranca inteligente, com isso temos a vantagem de diminuir os riscos de falha dos dispositivos móveis, tanto a nível de *hardware* como a nível de *software*, além de tornar o processo de abrir a tranca mais rápido e intuitivo.

Para uma melhor compreensão deste trabalho se faz necessário uma rápida apresentação de dois conceitos, o primeiro a tríade CID, a qual versa sobre integridade, disponibilidade e confidencialidade de dados transmitidos por Wi-Fi. Já o segundo conceito é a computação em névoa, a qual será utilizada neste trabalho.

A. Tríade CID [8]

CID é uma abreviação para confidencialidade, integridade e disponibilidade. Estas são basicamente as diretrizes que são definidas para a segurança da informação em uma organização.

- **Confidencialidade**: Basicamente, são o conjunto de regras que torna a disponibilidade de informações limitada. As medidas são tomadas para garantir que os dados confidenciais não cheguem às mãos de pessoas indesejadas, garantindo que o legítimo proprietário das informações possa acessá-los.
- **Integridade**: Significa que os dados utilizados estão corretos e são confiáveis. Mantendo a precisão, confiabilidade e consistência das informações durante todo o ciclo de vida dos dados. No trânsito de informações, ele não deve ser alterado, ao mesmo tempo que medidas devem ser tomadas para garantir que as informações não sejam violadas por participantes não autorizados.
- **Disponibilidade**: Significa que os dados estão acessíveis apenas a usuários autorizados. A melhor maneira de fazer isso é realizando manutenções rigorosas no hardware, reparos em tempo hábil e mantendo o sistema operacional funcionando adequadamente, livres de problemas de software e garantindo que o mesmo esteja sempre atualizado.

B. Computação em névoa

O uso de computação em nuvem tem crescido bastante nos últimos anos, tem sido solução para diversos problemas da informática e também ferramenta para muitas inovações na tecnologia da informação. Apesar de todos os benefícios da computação em nuvem, ela ainda não é capaz de lidar com a enorme quantidade de dados gerados pela IoT, em 2015 o número de dispositivos conectados eram 15,41 bilhões, em 2018 chegou a 23,14 bilhões e estima-se que esse valor cresça para 75,44 bilhões em 2025 [11].

Na computação em névoa, os dados gerados por diferentes dispositivos IoT podem ser processados na borda da rede em vez de enviá-los para a nuvem, sendo assim, uma arquitetura distribuída capaz de processar e armazenar dados mais próximo do usuário final. Esse tipo de rede proporciona uma resposta mais rápida e com mais qualidade em comparação a computação em nuvem [12]. Desta forma, a computação em névoa pode ser considerada mais adequada para ser integrada ao IoT, fornecendo serviços eficientes e seguros para um grande número de usuários finais. A utilização de computação em névoa pode ser considerada como o futuro da infraestrutura de IoT [13]

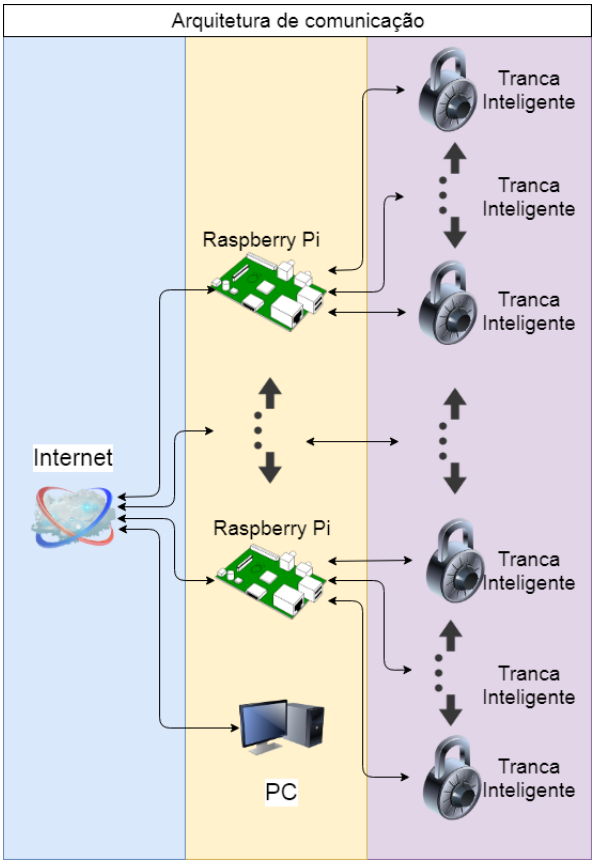

Figura 1. Arquitetura proposta

III. Arquitetura proposta

A arquitetura proposta neste trabalho é composta por 3 níveis de comunicação (ver Figura 1).

O primeiro nível se trata de um servidor em nuvem, sendo a central de informações do sistema, ele terá a função de armazenar as informações das salas que são: usuários cadastrados, registros de acesso ou tentativa de acesso, horários de reserva, registros de alertas e condições do ambiente.

Para fazer a gerência das informações contidas na nuvem, existirá uma interface web que poderá ser acessada por um computador, *tablet* ou *smartphone*. Apenas pessoas com funções de administradores podem acessar essas funções, que serão: registrar/excluir usuário, fazer reserva de acesso, cancelar reserva de acesso conceder acesso, negar acesso e editar informações de reserva.

O segundo nível será composto por nós de comunicação cujo o dispositivo que será usado nesta proposta é o *Raspberry Pi* devido ao seu baixo custo e ser uma plataforma aberta. Cada dispositivo nesta camada tem a função de gerenciar os acessos do conjunto de trancas a ele associadas. Ao início do dia, ou quando ocorrer alguma mudança para um determinado conjunto de trancas, cada nó de comunicação irá receber as informações de reserva/acesso do dia e assim, a partir da comunicação com cada tranca inteligente, negar ou dar permissão de acesso de um usuário a um determinado ambiente, bem como enviar os registros de monitoramento do ambiente para a nuvem.

O terceiro nível de comunicação é a tranca inteligente em si, que utiliza um ESP8266, que se trata de um microcontrolador de baixo custo e *open hardware* capaz de se conectar a redes Wi-Fi. A tranca irá coletar dados do ambiente em que foi instalada e enviar para o *Raspberry Pi* por Wi-Fi, onde serão tomadas as decisões.

IV. Tranca inteligente

A tranca inteligente proposta neste trabalho tem como objetivo não apenas trancar uma porta e manter o acesso apenas para pessoas autorizadas, mas monitorar e controlar algumas partes dos ambiente, aumentando o nível de segurança, utilizando a energia elétrica de maneira mais eficiente e conferindo um grau de inteligência para o sistema.

A. Controle dos dispositivos

A Figura 2 apresenta a arquitetura da tranca inteligente, a qual possui um módulo RFID que tem a função de fazer a leitura dos cartões de acesso por rádio frequência, um microcontrolador ESP8266 que terá a função de gerenciar os dispositivos a ele conectados que são: a fechadura magnética, um sensor de presença, ar condicionado e iluminação.

A fechadura magnética foi escolhida para esse sistema por apresentar uma série de vantagens como: fáceis de instalar, são silenciosas e desbloqueiam instantaneamente quando a energia for cortada permitindo uma liberação rápida. A fechadura é acionada por meio de um relé conectado ao GPIO do

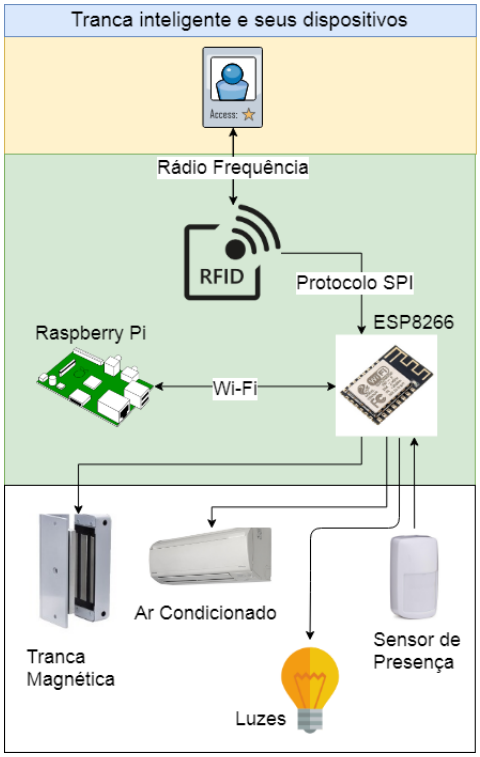

Figura 2. Arquitetura da tranca inteligente

ESP8266. Um sensor de presença é instalado juntamente com a fechadura para detectar a presença de pessoas não autorizadas no ambiente. O acionamento do sistema de condicionamento de ar e da iluminação do ambiente é realizado através de relé individual.

A Figura 3 apresenta o fluxograma do código fonte embarcado no microcontrolador (ESP8266) da tranca inteligente. O fluxograma descreve uma série de instruções que são executadas em um laço infinito. O fluxograma pode ser dividido em quatro grandes grupos de atividades, as quais chamaremos de módulos: Leitor RFID; Iluminação; Detecção de presença; Sistema de condicionamento de ar.

O módulo Leitor RFID fará a leitura dos cartões. Cada cartão possui um código de acesso distinto, após a leitura, o microcontrolador envia para o dispositivo de processamento na borda da rede (*Raspberry Pi*) adequado, a informação do cartão de acesso junto com a identificação da tranca inteligente. Este (*Raspberry Pi*) por sua vez, confronta os dados enviados com a programação recebida da nuvem e retorna para o microcontrolador da tranca os comandos que devem ser executados, como conceder acesso a sala ou negar o acesso e faz o registro das informações no log do sistema.

No módulo de Iluminação (Figura 3) é possível verificar que, caso esteja em horário de reserva, o controle do acionamento das luzes da sala estará disponível para o usuário através dos interruptores da sala. Caso a sala se encontre fora do horário de reserva e os sensores de movimento não indicaram a presença de alguém, o microcontrolador da tranca irá cortar a energia dos interruptores através de uma saída a relé.

O módulo Detecção de presença é utilizado para o supervisionamento da sala. Sempre que a tranca inteligente identificar uma movimentação dentro da sala, fora de horário reservado, enviará ao sistema um alerta. Este sistema de alerta se faz necessário para evitar que alguém fique na sala após o término do período da reserva e também para saber se uma pessoa não autorizada entrou na sala.

Por fim, o módulo Sistema de condicionamento de ar tem o objetivo de utilizar a energia de maneira mais eficiente. Para isso, o sistema adotará um protocolo de acionamento para os condicionadores de ar. O protocolo proposto indica que os condicionadores de ar devem ser ligados sempre que a tranca se encontrar em um horário reservado para o uso da sala e apenas deverão ser desligados se não houver uma reserva marcada para as próximas duas horas (manter os condicionadores de ar ligados, caso o intervalo de reserva seja inferior a duas horas, se faz necessário para evitar o aumento de consumo devido aos picos de correntes gerados na hora de ligar o compressor do ar condicionado [16]). Assim, como o *Raspberry Pi* tem salvo em sua memória todos os horários reservados de cada sala, ele orientará o microcontrolador das trancas em qual momento os condicionadores devem ser acionados ou não. Para isso, cada tranca verifica duas condições distintas: a primeira condição é se a sala está em um horário reservado para uso; a segunda condição é se haverá reserva nas próximas duas horas. Caso uma dessas condições sejam verdadeiras, os condicionadores de ar serão ligados ou se manterão ligados, caso nenhuma das condições seja verdadeira, os os condicionadores de ar serão desligados.

V. Experimento

A arquitetura proposta neste trabalho envolve o desenvolvimento do sistema em três etapas: tranca inteligente, nós de comunicação (*Raspberry Pi*) e servidor em nuvem. A primeira etapa (tranca inteligente) envolve o desenvolvimento de um *hardware* e *software* embarcado para controlar o acesso e monitorar os ambientes de uma sala de aula. Na etapa dos nós de comunicação será desenvolvido um *software* para microcomputadores embarcados que funcionem

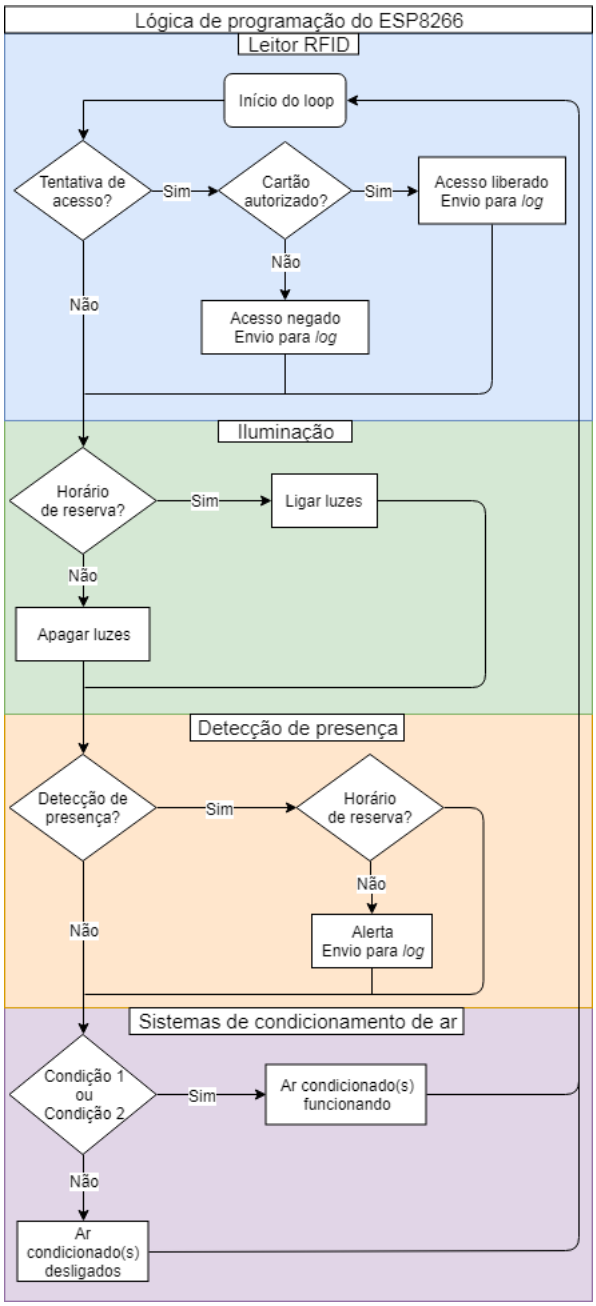

Figura 3. Fluxograma da logica do ESP8266

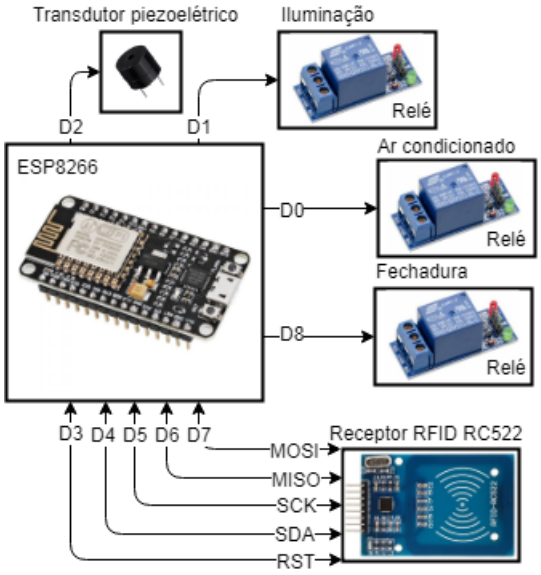

Figura 4. Montagem do protótipo

como intermediários na transmissão de dados do servidor em nuvem para a tranca inteligente. Na terceira e última etapa, será desenvolvida a programação de um servidor em nuvem com um banco de dados, onde serão guardadas todas as informações do sistemas juntamente com uma interface para que administradores possam manipular os dados do banco de dados.

Este trabalho, que encontra-se ainda em desenvolvimento, apresentou a proposta do sistema (*class control*) e apresentará nesta seção os detalhes do protótipo da tranca inteligente. O protótipo foi desenvolvido em uma matriz de contato (protoboard) com sua arquitetura descrita na Figura 4. O protótipo da traca utilizou como microcontrolador um ESP8266, como receptor RFID o MFRC522, três módulos relé e um transdutor *buzzer* piezoelétrico. A leitura dos cartões RFID é realizada pelo receptor e enviado ao microcontrolador por comunicação serial SPI. O acionamento dos condicionadores de ar, da fechadura ou da liberação dos interruptores é realizada através do acionamento de um pino digital de saída do microcontrolador, sendo um pino para cada periférico, o qual controla o acionamento de um dos módulos relés. Cada módulo relé se encontra ligado em série com o circuito de acionamento de um dos periféricos. Por fim, o *buzzer*, que serve para interação com o usuário, será também acionado por um pino digital de saída do microcontrolador. A tranca foi alimentada a partir de uma fonte de 12 V DC e para capturar a comunicação da tranca foi utilizado o serviço da plataforma para internet das coisas *Blynk*, possibilitando obter data e hora em tempo real e as informações trocadas pela tranca inteligente.

VI. Resultados e discussões

Para a execução dos testes, foi arbitrado um conjunto de horários de reservas das sala, o qual foi organizado em formato de tabela (ver Tabela 1). Essas informações foram

Tabela I
Tabela de horários de reserva

Horário inicial	Horário inicial	RFID code	Nome
13:00	13:40	AD 1B 8C 14	Vitor
14:00	14:40	AD 1B 8C 14	Vitor
15:00	15:40	BC 15 F2 26	Pereira
16:00	16:40	AD 1B 8C 14	Vitor
17:00	17:40	BC 15 F2 26	Pereira

armazenadas na memória do ESP8266 e elas sempre são consultadas para a verificar se um determinado usuário tem ou não a reserva da sala naquele horário. A verificação do usuário se dá por meio da comparação das informações recebidas no receptor RFID com as informações da tabela previamente arbitrada. Durante os testes constatou-se o correto funcionamento da tranca, ativando o relé que aciona a fechadura apenas para os usuários que têm acesso durante o período de reserva correspondente. O transdutor *buzzer* piezoelétrico cumpri sua função de sinalizar quando o acesso for negado ou permitido através de tons distintos para cada caso.

Quando o acesso é concedido o microcontrolador aciona os relés para ligar o ar condicionado e a iluminação do ambiente. Já ao final da reserva, o sistema de iluminação é desligado (neste protótipo não foi inserido o sensoriamento do movimento dentro da sala) e a tabela dos horários é verificada mais uma vez para saber se vai haver uma outra reserva nas próximas duas horas, se houver, mantém o relé do ar condicionado ativado, se não faz-se o desligamento do sistema de condicionamento de ar. Cada vez que se faz uma tentativa de acesso a sala, as informações coletadas pela tranca inteligente são enviadas para um terminal da plataforma *Blynk*. O conteúdo das informações enviada possuem a data, hora, código RFID, nome e informação de acesso (acesso negado ou permitido), com todos os campos separados pelo caractere '@', como apresentado na Figura 5, formando assim um *log* de dados.

Tendo em vista que o protótipo se encontra em fase inicial, se faz necessário pontuar quais seriam os próximos passos para a concretização do projeto. Para a melhoria do protótipo atual recomenda-se o desenvolvimento de uma placa de circuito impresso contendo os componentes necessários para o funcionamento completo da tranca inteligente. Com relação ao sistema *class control*, a próxima etapa seria a aquisição de um *Raspberry Pi* e desenvolver o *software* para a intermediação, entre o servidor em nuvem e a tranca inteligente, do gerenciamento para liberação de acesso nos horários reservados. Por fim, é necessário o desenvolvimento das aplicações de gerenciamento e banco de dados no servidor em nuvem. Todo a interação entre o servidor em nuvem e os administradores do sistema será realizado por plataforma web, a qual permitirá aos administradores do sistema cadastrar e remover usuários, cadastrar e remover trancas inteligentes do sistema e fazer todas as atividades de reserva de salas.

Para aprimorar ainda mais a experiência do usuário, o servidor será configurado para permitir, através de aplicativos para

smartphones de terceiros, os usuário de fazer suas solicitações de reservas com mais praticidade.

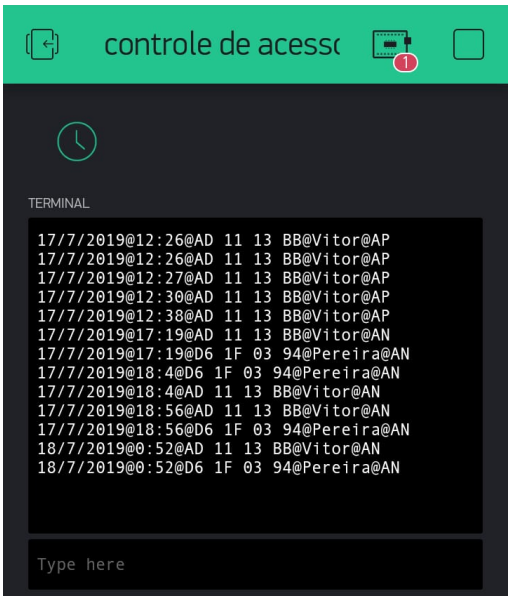

Figura 5. Log de tentativas de acesso

VII. Conclusão

Se apoiando nos conceitos de cidades inteligentes, internet das coisas e computação em névoa, foi proposta uma arquitetura de comunicação para a implementação de um sistema inteligente para controle de acesso e monitoramento de múltiplos ambientes (*class control*). O sistema, como apresentado ao longo do texto, possui diversas funções agregadas ao seu foco principal que é o controle de acesso. As funções agregadas permitem um monitoramento mais inteligente do uso do ambiente reservado e ainda possibilita um consumo mais consciente da energia elétrica deste ambiente.

Embora o sistema ainda se encontre em desenvolvimento, experimentos foram realizados a nível de protótipo comprovando o funcionamento da tranca inteligente (parte integrante do sistema) e o seu potencial para transformação em produto. É importante destacar que o protótipo foi bem sucedido com relação controle de acesso, sendo capaz de trocar informações por meio de comunicação Wi-Fi e gerenciar o funcionamento local dos periféricos.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Referências

[1] Jennifer Belissent, Getting Clever About Smart Cities: New Opportunities Require New Business Models, Forrester Research, 2010.

[2] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, “Convergence of MANET and WSN in IoT urban scenarios,” IEEE Sens. J., vol. 13, no. 10, pp. 3558–3567, Oct. 2013.

[3] ”History”. Locks.ru. Retrieved 2016-03-14, website : www.locks.ru/germ/informat/schlagehistory.htm

[4] C. T. Lee, T. C. Shen, W. D. Lee, and K. W. Weng, ”A novel electronic lock using optical Morse code based on the Internet of Things,”2016 International Conference on Advanced Materials for Science and Engineering (ICAMSE), 2016, pp. 585-588.

[5] X. Lv and L. Xu, ”AES encryption algorithm keyless entry system,”Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, Yichang, pp. 3090-3093, 2012.

[6] M. S. Hadis, E. Palantei, A. A. Ilham and A. Hendra, ”Design of smart lock system for doors with special features using bluetooth technology,”2018 International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, 2018, pp. 396-400.

[7] C. Lee, Y. Chung, T. Shen and K. Weng, ”Development of electronic locks using gesture password of smartphone base on RSA algorithm,”2017 International Conference on Applied System Innovation (ICASI), Sapporo, 2017, pp. 449-452.

[8]]G. Varshney and H. Gupta, ”A security framework for IoT devices against wireless threats,” In Proc. 2017 2nd International Conference on Telecommunication and Networks (TEL-NET), Noida, 2017, pp. 1-6.

[9] M. Kishwar Shafin et al., ”Development of an RFID based access control system in the context of Bangladesh,”2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2015, pp. 1-5.

[10] M. Mathew and R. S. Divya, ”Super secure door lock system for critical zones,”2017 International Conference on Networks & Advances in Computational Technologies (NetACT), Thiruvanthapuram, 2017, pp. 242-245.

[11] Internet of Things (IoT): number of connected devices worldwide from 2012 to 2020 (in billions). https://tinyurl.com/j3t9t2w

[12] S. Yi, C. Li, and Q. Li. A survey of fog computing: concepts, applications and issues. In Proc. of the 2015 Workshop on Mobile Big Data. ACM, June 2015.

[13] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli. Fog computing and its role in the internet of things. In Proc. of the First Edition of the MCC Workshop on Mobile Cloud Computing, August 2012.

[14] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli. Fog computing and its role in the internet of things. In Proc. of the First Edition of the MCC Workshop on Mobile Cloud Computing, August 2012.

[15] M. Pavelić, Z. Lončarić, M. Vuković and M. Kušek, ”Internet of Things Cyber Security: Smart Door Lock System,”2018 International Conference on Smart Systems and Technologies (SST), Osijek, 2018, pp. 227-232.

[16] LUCATEL, Cleiton. Eficientização energética em climatizadores de ar utilizando partida suave na comutação do compressor e desligamentos pré-programados. 64p. 2017. Trabalho de Conclusão de Curso (Graduação em Engenharia Elétrica) – Universidade Federal do Pampa, Campus Alegrete, Alegrete, 2017.