A Solution for Dynamic Management of User Profiles in IoT Environments

V. Leithardt, *Member, IEEE,* D. Santos, *Student Member, IEEE,* L. Silva, F. Viel, *Student Member, IEEE,* C. Zeferino, *Member, IEEE,* and J. Silva, *Member, IEEE*

***Abstract*—Internet of Things (IoT) is an emerging area in which we expect to have billions of devices connected to the Internet by 2020. IoT applications can offer many benefits to environments, society, and the economy through the interconnection and cooperation of smart objects. However, there are many privacy challenges, such as authentication, authorization, and confidentiality of personal data. With this in mind, we developed a solution for dynamically managing user profiles according to the characteristics of each environment. This solution is a module of a middleware named (Ubiquitous Privacy) and traces the frequency of the user in the environment to update its profile according to the environment's rules. The implemented module was validated using scripts that perform probabilistic simulation and user authentication. From the rules assigned to the simulated environments, it was possible to confirm the high adaptability of the implementation. We also verified that it could be easily adjusted to any IoT environment that wants to treat the authentication and privacy of environments and users.**

***Index Terms*—Internet of Things, Data privacy, Profiles.**

I. Introdução

A Internet das Coisas ou IoT (do inglês, Internet of Things) pode ser vista sob diversas perspectivas e formas, dentre as quais, destacam-se as abordagens orientadas à Internet, às coisas e ao conhecimento. Quanto à forma, basicamente, a IoT pode ser dividida em dar suporte a humanos e a aplicações industriais [1]. Essas duas formas recebem os nomes, respectivamente, de Internet Humana das Coisas (HIoT – Human IoT) e Internet Industrial das Coisas (IIoT – Industrial IoT). Um exemplo de aplicação voltada à IIoT é o trabalho apresentado em [2], no qual é empregado um *gateway* baseado em comunicação Wi-Fi com uso dos protocolos MQTT (Message Queuing Telemetry Transport) e CoAP (Constrained Application Protocol). Portanto, a IoT se define em função da aplicação alvo e ao objetivo que se quer alcançar.

Os três elementos principais que podem ser considerados em um sistema IoT são o hardware, o middleware e a apresentação. O hardware é o responsável por fazer a aquisição de dados por meio de sensores, dar suporte ao tratamento desses dados com unidades de processamento e agir, quando necessário, por meio de atuadores. O middleware é responsável por dar suporte ao desenvolvimento rápido de aplicações que necessitam armazenar, processar e analisar dados, abstraindo o sistema operacional e o hardware. O middleware também é responsável por permitir o acesso de diferentes formas e por diferentes usuários (sistemas computacionais e humanos) ao conhecimento gerado [3], [4]. As características principais das aplicações IoT se resumem, conforme [5], em: (*i*) diversidade, pois as diferentes aplicações apresentam requisitos diversos e provavelmente necessitam de arquiteturas diferentes; (*ii*) tempo real, para realizar as ações necessárias de acordo com os requisitos temporais da aplicação; (*iii*) segurança e privacidade, para proteger as aplicações, as redes e os usuários; e (*iv*) modelo de serviços, sendo o modelo XaaS (Everything-as-a-Service) eficiente, escalável e de fácil uso [6]. Consequentemente, pesquisas descritas em [7], entre outras relacionadas a IoT, apontam a segurança e a privacidade como sendo um grande desafio e problema de pesquisa fundamental para permitir que a IoT seja segura, acessível e adotada em larga escala.

Dentro do contexto supracitado, com o objetivo de proporcionar maior segurança e privacidade aos ambientes que integram sistemas, aplicativos e demais tecnologias IoT, este trabalho apresenta contribuição relacionada à definição de métricas, parâmetros e critérios de hierarquia de perfis para o gerenciamento de privacidade. Para tanto, foi desenvolvido um módulo denominado PRIPRO (Privacy Profiles) do modelo de controle de privacidade para ambientes pervasivos/ubíquos (UbiPri – Ubiquitous Privacy) proposto em [8]. A outra contribuição deste trabalho foi alcançada nos testes realizados, que demonstram a possibilidade de atribuir ou diminuir requisitos ao usuário de acordo com o tempo estabelecido de acordo com a identificação e permanência no ambiente localizado com uso de dispositivos. Para tanto, os ambientes foram definidos em cinco categorias, e os níveis de usuários para acessar e utilizar também em cinco categorias. Com isso, identificamos e atribuímos diferentes níveis de privacidade de acordo com a hierarquia definida individualmente.

O restante deste artigo está organizado em seis seções. A Seção II discute os trabalhos relacionados. A Seção III descreve o middleware de referência do trabalho, enquanto a Seção IV apresenta a modelagem da evolução dos perfis. A Seção V, por sua vez, descreve o protótipo desenvolvido. A Seção VI demonstra os resultados experimentais. E por fim, na Seção VII, são emitidas as considerações finais.

V. Leithardt é professor da Universidade do Vale do Itajaí, 88302-901 Brasil e-mail: valderi@univali.br.

D. Santos é estudante da Universidade do Vale do Itajaí, Itajaí.

L. Silva é egresso da Universidade do Vale do Itajaí, Itajaí.

F. Viel e C. Zeferino são professores da Universidade do Vale do Itajaí.

J.Silva é professor da Universidade de Coimbra, Coimbra, 3000-370 Portugal.

II. Trabalhos Relacionados

Os autores de [9] apresentaram a proposta de um *framework* de controle de acesso orientado a comunidades chamada CO-CapBAC (Community Capability-Based Access Control). No artigo, é proposto que dispositivos inteligentes dentro de uma mesma comunidade possuam as mesmas restrições de acesso. Quando um dos dispositivos da comunidade realizar uma autenticação, os outros precisam apenas se comunicar com o dispositivo de controle de acesso que se localiza dentro da rede interna para buscar as permissões do usuário, aumentando o desempenho da rede para usuários recorrentes. Também foi implementado um protótipo, no qual foi utilizado o microcontrolador ATMEGA328 e a identificação das pessoas é feita com smartphones. A abordagem de [9] se assemelha muito à abordagem adotada neste trabalho. Porém, o presente trabalho apresenta vantagens porque ele abre mais possibilidades de acesso aos dispositivos devido à definição de perfis. Neste trabalho, nós também implementamos um protótipo. Porém, utilizamos o microcontrolador ATMEGA328P, que consome menos energia, e a identificação das pessoas é feita com *tags* RFID (do inglês, Radio Frequency IDentification).

No trabalho [10], foi desenvolvido o sistema CapBAC (Capability Based Access Control), o qual é utilizado como o controlador de acesso ao middleware de automação. Uma desvantagem desse sistema em relação ao presente trabalho, é que ele não é automático. Os administradores do ambiente devem informar manualmente os usuários que terão acesso.

A solução apresentada em [11] é um mecanismo de controle de acesso confiável para IoT denominado TACIoT (Trust-Aware Control Mechanism for IoT) para lidar com a imprecisão associada com as informações do contexto em cenários pervasivos. O CapBAC propõe um novo modelo de confiança baseado na lógica fuzzy, o qual é o pilar do TACIoT. Esse modelo segue a abordagem multidimensional para possibilitar uma computação confiável e precisa para dispositivos IoT [12]. Diferente de modelos anteriores que apenas consideram a reputação e o *feedback*, o CapBAC utiliza os aspectos de segurança e os fatores sociais entre dispositivos IoT, os quais são utilizados por objetos inteligentes para conduzir lógica do controle de acesso.

A Tabela I apresenta a comparação do presente trabalho com os trabalhos analisados. A tabela identifica se as soluções desenvolvidas gerenciam a privacidade de dados, utilizam perfis de usuários para gerenciar a privacidade, consideram privacidade e segurança de ambientes IoT, implementam uma recompensa ou punição de acordo com a permanência do usuário no ambiente, oferecem um sistema genérico que possa ser implementado em ambientes com diferentes características e se propõem um sistema automático para decidir o acesso do usuário com níveis diferenciados de privacidade. Cada uma dessas funcionalidades está presente em uma ou outra solução, mas a nossa é a única que cobre todas as características elencadas. A solução proposta destaca-se ainda em relação às demais por gerenciar a privacidade de ambientes IoT com um sistema genérico e automático, contribuindo com a implementação para a evolução dos perfis de usuários.

Este artigo é uma evolução de um trabalho anterior apresentado em [14], no qual foi proposta uma estratégia para definição de perfis de usuários. O diferencial em relação ao referido trabalho reside na implementação da evolução dos perfis dos usuários em relação à permanência no ambiente e no desenvolvimento de um protótipo de um sistema embarcado, para o controle de acesso de pessoas com base em requisitos e parâmetros definidos. Na evolução de perfis, o perfil pode tanto aumentar ou diminuir na ordem hierárquica, automaticamente, de acordo com as definições e regras. A principal contribuição, além dos itens citados anteriormente, se fundamenta no provimento de uma infraestrutura de apoio ao gerenciamento da privacidade dos dados com base na evolução do perfil do usuário no ambiente. Adicionalmente, o trabalho também se fundamentou no modelo taxonômico de [8], o qual definiu os módulos necessários para o tratamento da privacidade nos ambientes. Os trabalhos em questão são detalhados na seção a seguir que descreve o middleware de referência.

TABELA I
Trabalhos relacionados

	[13]	[9]	[10]	[11]	[14]	Este Trabalho
Privacidade de Dados	•				•	•
Perfis de Usuários					•	•
Privacidade de Ambientes	•	•	•	•	•	•
Evolução de perfis					•	•
Sistema Genérico	•	•		•		•
Sistema Automático		•		•	•	•
Sistema Embarcado		•				•

III. Middleware de Referência

Esse trabalho é fundamentado no middleware UbiPri [8], em continuidade aos estudos realizados em [14]. O middleware UbiPri segue um modelo genérico, o qual contém diversos componentes para controlar ambientes IoT. A Figura 1 apresenta todos os componentes que compõem esse modelo e destaca o módulo alvo deste trabalho, o qual é descrito a seguir. Este middleware é baseado nos seguintes requisitos: (*i*) suporte ao gerenciamento de privacidade baseado em critérios previamente definidos – por exemplo: Usuário, Dispositivo, Aplicação, Comunicações, Ambiente e Privacidade; (*ii*) suporte ao gerenciamento de informações com base na necessidade de coletar informações pessoais para controlar esses sistemas de acordo com as limitações éticas e legais, por que a privacidade das pessoas está envolvida; e (*iii*) funcionalidades do software para localização do usuário, tomada de decisão e adaptação para suportar o gerenciamento de privacidade de dados. Essas características foram pesquisadas, desenvolvidas e estão definidas conforme descrito em [15].

O módulo desenvolvido nesse trabalho é o PRIPRO (Privacy Profiles), o qual deve realizar o controle de transações no gerenciamento do perfil do usuário [8]. Seu principal objetivo é controlar a informação, definida previamente por um motor de busca que possui o propósito de distribuir e direcionar toda a informação sintetizada para os módulos seguintes, a fim de adaptar apropriadamente para a privacidade individual com base no perfil individual.

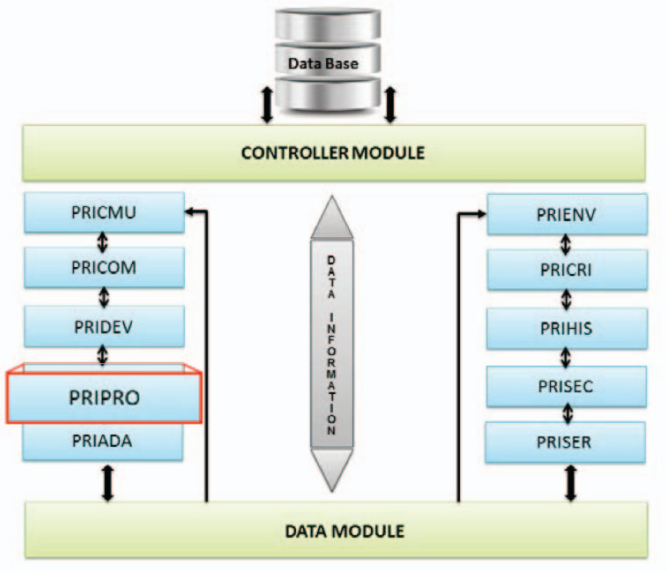


Fig. 1. Arquitetura do middleware UbiPri [8].

O desenvolvimento do módulo PRIPRO utilizou serviços web (*i.e. web services*) com o modelo arquitetural REST (REpresentational State Transfer) e recebe requisições de dispositivos que desejam autenticar usuários no ambiente. Esses dispositivos podem ser leitores biométricos, leitores de RFID (Radio Frequency IDentification), smartphones, entre outros. O serviço web informa ao dispositivo o perfil do usuário, dados do ambiente, recursos e serviços disponíveis utilizando JSON (JavaScript Object Notation). O perfil do usuário é definido a partir dos dados que estão disponíveis para o módulo. Esses dados são informações do usuário enviadas pela requisição e obtidos dos bancos de dados específicos da esfera em que ele se localiza. A Figura 2 exemplifica a utilização dos bancos de dados específicos. Neste exemplo, o serviço web tem acesso ao banco de dados específico de três esferas: (*i*) Universidade; (*ii*) Casa; e (*iii*) Farmácia. No caso de uma requisição ser realizada do ambiente Farmácia, o serviço web deve identificar a esfera de onde originou a requisição e buscar os dados do banco específico dessa esfera. Isso é feito para garantir que os dados de uma esfera não interfiram nas outras esferas.

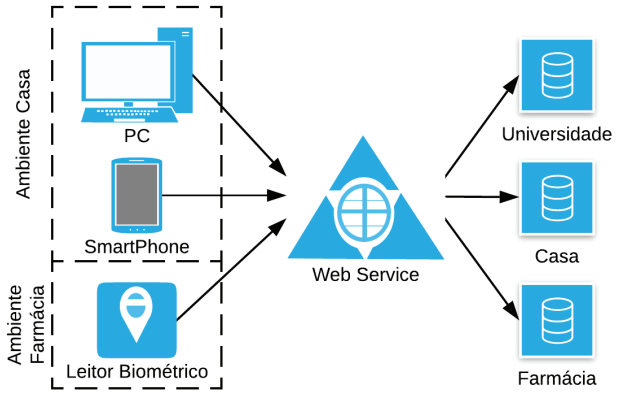


Fig. 2. Arquitetura de utilização do serviço web [14].

Cada esfera possui as suas regras e particularidades, fazendo com que cada uma delas esteja em um contexto totalmente diferente. Para que uma requisição ao sistema seja válida, é necessário indicar certos parâmetros que permitam a busca dos dados do usuário. Visando a simplicidade da requisição, foram definidos como parâmetros: (*i*) o identificador do dispositivo do usuário; (*ii*) o que o usuário pretende fazer (entrar ou sair do ambiente); e (*iii*) o identificador do dispositivo autenticador. Desse modo, os dados necessários nos dispositivos são mínimos, simplificando a implementação.

IV. Modelagem da Evolução dos Perfis

A partir dos resultados preliminares, foram desenvolvidas implementações adicionais relacionadas à evolução do perfil do usuário. Para tanto, foi necessário estabelecer os intervalos de tempo que seriam tratados pela esfera. Esses intervalos são utilizados para calcular a taxa de permanência do usuário na esfera (ou seja, sua frequência). Esses intervalos são definidos neste artigo como intervalos de valência e são utilizados para calcular a frequência do usuário e definir o seu perfil. Por exemplo, os diferentes ambientes (ou esferas) podem ter intervalos próprios para atualizar o perfil do usuário. Uma esfera pode realizar essa atualização diariamente, enquanto outra pode fazer isso semanalmente.

A Figura 3 mostra as tabelas do banco de dados que foram implementadas com o objetivo de configurar a evolução dos perfis dos usuários para as diferentes esferas. No banco de dados específico do ambiente (*e.g.* Universidade), a tabela *Intervalos* armazena todas as opções de intervalo (ou turno) que podem ser utilizadas para definir os perfis dos usuários da esfera (*e.g.* das 08:00 às 12:00, das 09:00 às 13:00 etc.). Na tabela *Intervalos_de_Valência*, são escolhidos, para cada esfera, os intervalos a serem tratados pela esfera. Nessa tabela, também é definido o tempo (em horas) que espera-se que os usuários permaneçam no ambiente em cada intervalo de valência (*e.g.* 4 horas). Uma terceira tabela do banco de dados, denominada *Frequência*, armazena as frequências dos usuários em cada ambiente, otimizando o sistema de modo que, quando o usuário se autenticar nos ambientes, o sistema não precise calcular a sua frequência, reduzindo o seu tempo de resposta.

Em (1), é calculada a frequência do usuário no ambiente (ou seja, sua taxa de permanência). Quando o intervalo de valência da esfera for o menor de todos, será empregada (f_{inf}), mantendo, assim, a mesma hierarquia e definições inferiores para aquele ambiente e intervalo identificados. Considerando um cenário ideal, um usuário gera uma autenticação de entrada e uma de saída para cada vez que ele ingressa ou se retira do ambiente. A equação consiste em somar os intervalos de tempo entre a entrada e a saída (t_0) e (t_1), respectivamente e dividir pelo intervalo de tempo que o ambiente espera que o usuário permaneça nele (Δt), obedecendo a premissa deste trabalho de que o ambiente que define as suas regras.

$$f_{inf} = \frac{\sum_{i=0}^{n-1}(t_1 - t_0)}{\Delta t} \quad (1)$$

onde n é o número de ocorrências (entradas e saídas) do usuário no ambiente. O somatório dos intervalos de cada

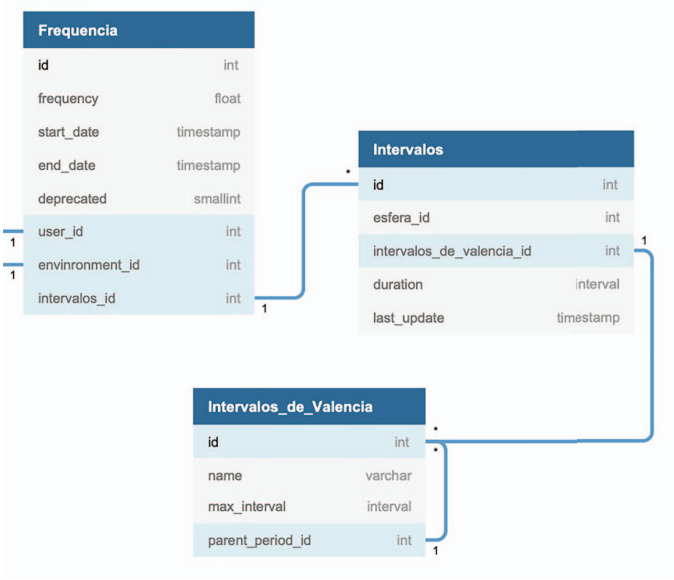


Fig. 3. Modelagem do banco de dados.

ocorrência é feito para que sejam desconsiderados os intervalos de tempo em que o usuário se ausentou do ambiente. Por exemplo, considerando um tempo de permanência esperado de quatro horas, se o usuário permanecer por três intervalos diferentes de uma hora cada intervalo, a sua frequência será de 75%.

Quando for necessário calcular a frequência do usuário no ambiente para intervalos de valência maiores, utiliza-se (2):

$$f_{sup} = \frac{\sum_{i=0}^{m-1} f_{inf}}{m} \tag{2}$$

onde m é a quantidade de intervalos de valência imediatamente inferiores. Essa equação consiste em calcular a média das frequências obtidas para os intervalos de valência imediatamente inferiores ao intervalo de valência considerado. Por exemplo, para obter a frequência de um usuário em um ambiente ao longo de uma semana, aplica-se (2) para calcular a média de suas frequências diárias – as quais foram obtidas usando (1).

O cálculo da frequência dos usuários é realizado toda vez que o intervalo de valência imediatamente inferior da esfera é concluído. Ele consiste em somar o tempo que o usuário permaneceu no ambiente e dividir pela quantidade de horas que o ambiente espera que ele permaneça. Porém, quando constatado que um intervalo de valência superior já possui seu tempo limite expirado, a frequência do usuário é calculada por meio da média dos intervalos de valência imediatamente inferiores desde a última atualização do intervalo desejado. Com a frequência calculada, os usuários evoluem seus perfis de acordo com as regras definidas para cada esfera. Dessa maneira, o ambiente define as suas regras de acesso.

A frequência de atualização dos perfis é definida por meio do intervalo de valência mais inferior da esfera. Na implementação realizada no trabalho anterior [14], foi definida a técnica para implementação de um sistema genérico de definição de perfis, na qual deveria ser realizada uma requisição ao banco de dados específico da esfera. Nesse trabalho, o perfil do usuário é definido a partir do perfil que o usuário obteve no último acesso. Porém, quando o usuário ainda não se autenticou no ambiente, ou seja, não é conhecido pelo sistema, uma requisição ainda deve ser feita para o banco de dados específico da esfera para obter um perfil base. Depois de obtido o perfil base, para todas as autenticações seguintes, são feitas as verificações mostradas no fluxograma ilustrado na Figura 4. As faixas de frequência correspondentes aos perfis são configuráveis conforme as regras do ambiente. Os valores adotados na figura e utilizados no experimento demonstrado logo a seguir são apenas ilustrativos.

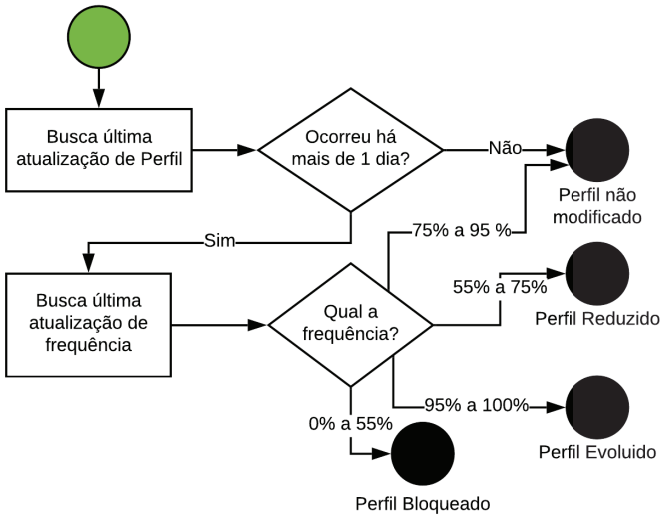


Fig. 4. Fluxograma de evolução do perfil do usuário teste.

Toda vez que o usuário se autenticar no ambiente, é feita a análise descrita no fluxograma. Primeiro, é buscada a última atualização do perfil do usuário (última autenticação no ambiente) e verificado se ocorreu a um tempo maior do que o intervalo de valência mais inferior. Se não ocorrer, o perfil não é modificado. Se ocorrer, o sistema busca a última atualização de frequência do usuário na tabela *Frequência* do banco de dados. A partir do valor da frequência, são aplicadas as regras do ambiente para definir se o perfil do usuário será modificado (reduzido, evoluído ou bloqueado) ou se ele não será modificado. Com o objetivo de realizar testes e validar a implementação, a seção a seguir apresenta o cenário de testes utilizado.

V. Protótipo Desenvolvido

Para os testes e validação, foi desenvolvido um protótipo de sistema embarcado para o controle de acesso das pessoas, sendo este um dispositivo autenticador. O sistema realiza o controle de acesso por meio de *tags* RFID e definições de comunicação conforme descrito em [16]. O protótipo do sistema embarcado desenvolvido é ilustrado na Figura 5 e suas características de hardware estão resumidas na Tabela II. A comunicação para a requisição dos dados é realizada com o uso do protocolo HTTP, sendo que as informações são transferidas em formato JSON.

Na solução desenvolvida, quando um usuário solicita seu acesso, o sistema embarcado envia uma requisição para o

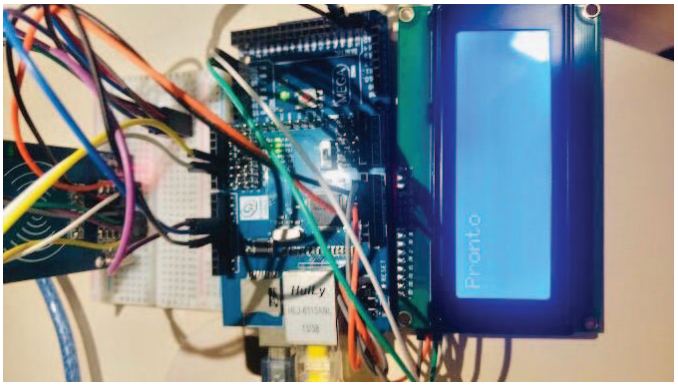


Fig. 5. Protótipo do dispositivo de controle de acesso.

TABELA II
CARACTERÍSTICAS DE HARDWARE

Componente	Funcionalidade
ATMEGA328P	Processamento
W5100	Conectividade Ethernet
MFRC522	Leitura de *tags* RFID
LCD 20x4	Exibição de mensagens
SPI	Conexão entre ATMEGA328P e W5100/MFRC522
I2C	Conexão entre ATMEGA328P e LCD

serviço web informando o ID do dispositivo autenticador e do dispositivo do usuário (*tag* RFID). O serviço web então analisa os dados do usuário e do ambiente e informa o perfil definido de acordo com os critérios e parâmetros correntes.

VI. RESULTADOS EXPERIMENTAIS

A. Cenário de Testes

A implementação realizada se concentrou no cenário de testes de ambientes de uma universidade. O cenário define que o intervalo de valência mais inferior é o dia, o que significa que os usuários podem ter seu perfil modificado uma única vez por dia, impedindo que o mesmo usuário, em um mesmo dia, tenha vários perfis diferentes. Além disso, conforme ilustrado previamente na Figura 4, o perfil do usuário será bloqueado, reduzido, mantido ou evoluído, conforme a sua frequência no ambiente.

O cenário de ambiente testado foi um laboratório de pesquisa, no qual é definido que o intervalo esperado para que o usuário permaneça no ambiente é de 8 horas diárias. Neste cenário, os intervalos de valência utilizados, da ordem do mais abrangente até o menos abrangente, são: *Semestre*, *Mês*, *Semana* e *Dia*.

B. Testes

Foram realizados testes do modelo proposto para identificar, observar, comparar e validar a evolução dos usuários. Para tal, foi realizada uma simulação de uso do ambiente utilizando a linguagem de programação Python. O programa consiste em um *script* que vai modificando a data e hora do sistema e autentica usuários com diferentes características no ambiente.

Na implementação, foram comparados todos os 31 dias do mês de janeiro de 2019 e feitas quatro autenticações para cada usuário, sendo que todos entram às 8:00, permanecem até às 12:00 e entram novamente às 14:00, permanecendo até às 18:00. O horário que o usuário irá sair é definido por uma constante para cada usuário. Porém, para simular de maneira mais realista, essa constante é subtraída por um intervalo aleatório de até 1 hora, que possui 50% de chance de ser aplicado. O Algoritmo 1 apresenta a principal parte do código da simulação.

Algoritmo 1 Código para simulação de usuários

```
for each day in january_days do
    for each user in users_list do
        time_stand ← user.time
        prob_50 ← random(1to100)
        if prob_50 > 50 then
            random_time ← random(0to1)
            time_stand ← time_stand − random_time
        hour_now ← 8hours
        for auth in range(4) do
            set_datetime(datetime_now + hour_now)
            new_authentication(
                passageType=(1 if (j % 2 == 0) else 2),
                authDevice=environmentDeviceIdentifier,
                userDevice=user.device,
                dttime=datetime_now + hour_now
            )
            if auth == 1 then
                hour_now ← 14hours
            else
                hour_now ← hour_now + time_stand
    set_datetime(datetime_now + 23:59 hours)
    refresh_frequencies(datetime_now + 23:59 hours)
    datetime_now ← datetime_now + 1day
```

C. Resultados

Nos testes realizados foi possível evidenciar que a frequência que o usuário teve no dia anterior pode modificar o seu perfil no dia atual, conforme ilustra a Figura 6. Observou-se também que o usuário obteve o perfil básico devido à requisição realizada para esfera específica. Inicialmente, ele mantém o mesmo perfil, pois está frequentando o ambiente dentro dos parâmetros aceitáveis. Porém, nos dias 3 e 5, ele frequentou o ambiente durante um intervalo igual ou maior do que 7,6 horas, fazendo com que, nos dias 4 e 6, seu perfil evoluísse de básico para avançado e de avançado para administrador, respectivamente. Nos dias 9 e 10, o usuário frequentou o ambiente durante um intervalo entre 4,4 e 6 horas diárias, causando uma diminuição de perfil em 2 dias consecutivos (10 e 11). Nos dias 11 e 14, ele permaneceu dentro dos parâmetros aceitáveis, mantendo assim o perfil sem evoluções, até que, no dia 15, ele permaneceu por um intervalo menor do que 4,4 horas, tornando-o bloqueado, pois esse ambiente determina que ele deve permanecer por pelo menos 55% do tempo esperado.

A Figura 7 apresenta os resultados obtidos na evolução de um grupo de usuários. Nele são mostrados os perfis dos

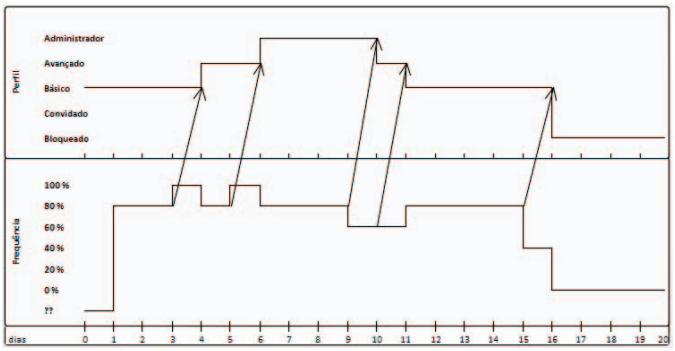


Fig. 6. Evolução do perfil do usuário teste.

usuários ao longo de doze dias. O eixo das ordenadas é o valor da variável qualitativa Perfil, a qual possui cinco possíveis estados: Bloqueado, Convidado, Básico, Avançado ou Administrador, e o eixo das abscissas significa a variação do tempo em dias. Cada linha desse gráfico representa um usuário diferente. Essa simulação foi feita com quinze usuários durante 31 dias, considerando o dia como o intervalo de valência mais inferior. Nesse gráfico, não é possível distinguir usuários com características de frequência muito parecidas, pois suas linhas se sobrepõem, devido as atribuições individuais.

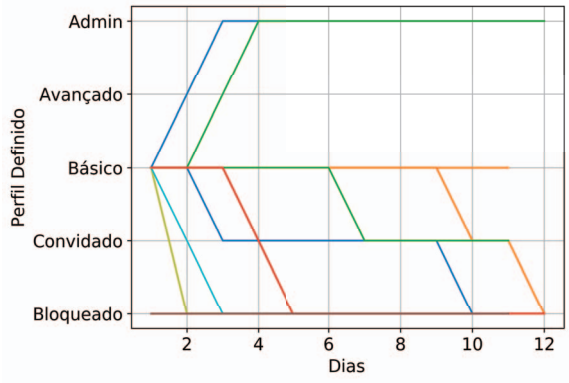


Fig. 7. Evolução de perfis na Simulação.

Porém, foi possível identificar que em 10,5% das autenticações, o usuário obteve o perfil Bloqueado. Em 55,56% das vezes, o usuário recebeu o perfil Convidado. Já em 10% dos casos, o usuário obteve o perfil Básico. Os perfis Avançado e Administrador foram atribuídos em 22,78% e 1,12%, respectivamente. Esse resultado mostra que a ascensão de usuário Básico para Administrador não é fácil de ser obtida, já que o usuário deve possuir uma frequência quase que perfeita. Percebeu-se ainda uma tendência aos usuários terem seu perfil reduzido gradativamente e passarem a ser bloqueados em pouco tempo. Isso se deu por causa da distribuição das constantes dos usuários, as quais foram escolhidas de modo que todas ficassem bem distribuídas.

Com a simulação, foi possível perceber uma significativa melhora no tempo de resposta do sistema ao utilizar o perfil das últimas autenticações ao invés de sempre realizar uma requisição dos dados da esfera específica, como no trabalho anterior, diminuindo a sobrecarga de requisições sobre o servidor.

VII. Conclusões

Este artigo apresentou a implementação de um sistema para controle e gerenciamento para definição de perfis com base na privacidade dos dados em IoT. A partir dos resultados obtidos nos testes foi possível identificar e definir diferentes perfis atribuídos a situações aleatórias. Também foi possível tratar a evolução e a redução da hierarquia com base em fatores que identificam a frequência de usuários nos ambientes testados.

Neste trabalho, também foi possível simular evoluções nas permissões dos usuários dentro dos ambientes de acordo com variáveis genéricas. Exemplos de contribuições de controle como dia da semana, horário de chegada e saída, dias úteis, definição de horário para entrada em ambientes de acordo com perfis, entre outras regras que podem variar. Com isso, foi possível perceber que os intervalos de valência escolhidos influenciam diretamente no tempo que as pessoas demoram para ter evoluções de perfis, trazendo vantagens e desvantagens. Por exemplo, se definimos como intervalo de valência mais baixo o dia, um usuário que começa com perfil Convidado, terá seu perfil evoluído para Administrador em três dias, desde que possua uma frequência perfeita. Consequentemente, se escolhermos como intervalo de valência mais baixo o mês, ele precisaria de três meses com frequência perfeita para evoluir seu perfil para Administrador.

Como trabalho futuro, pretendemos empregar e avaliar novas tecnologias para a definição de perfis, podendo ser utilizadas técnicas de inteligência artificial que implementem características dos ambientes para definir os parâmetros que são necessários para cada ambiente e esfera.

Agradecimentos

Este estudo contou com o apoio da CAPES – Código de Financiamento 001 e da FAPESC – Termo de Outorga No. 2019TR169. Este trabalho contou com apoio do projeto de cooperação internacional para desenvolvimento de pesquisas em gerenciamento de privacidade de dados Brasil / Portugal.

Referências

[1] T. Kubitza, A. Voit, D. Weber, and A. Schmidt, “An IoT infrastructure for ubiquitous notifications in intelligent living environments,” *Proceedings of the 2016 ACM Int. Joint Conf. on Pervasive and Ubiquitous Computing Adjunct - UbiComp ’16*, pp. 1536–1541, 2016, doi:10.1145/2968219.2968545.

[2] I. V. Ferreira, J. A. Bigheti, and E. P. Godoy, “Development of a wireless gateway for industrial internet of things applications,” *IEEE Latin America Transactions*, vol. 17, no. 10, pp. 1637–1644, 2019.

[3] F. Wortmann and K. Flüchter, “Internet of Things,” *Business & Information Systems Engineering*, vol. 57, no. 3, pp. 221–224, 2015.

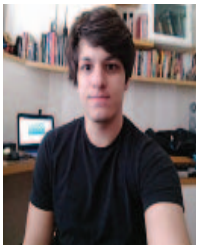
[4] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[5] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, “Middleware for Internet of Things: a survey,” *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 70–95, 2016.

[6] P. Banerjee, R. Friedrich, C. Bash, P. Goldsack, B. Huberman, J. Manley, C. Patel, P. Ranganathan, and A. Veitch, “Everything as a service: Powering the new information economy,” *Computer*, vol. 44, no. 3, pp. 36–43, 2011, doi: 10.1109/MC.2011.67.

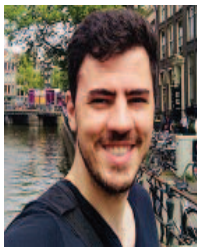
[7] J. Li, Q. Yan, and V. Chang, "Internet of Things: Security and privacy in a connected world," *Future Generation Computer Systems*, vol. 78, pp. 931 – 932, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17319817
[8] V. R. Leithardt, G. A. Borges, A. G. de Morais Rossetto, C. O. Rolim, C. F. R. Geyer, L. H. A. Correia, D. Nunes, and J. Sa, "A privacy taxonomy for the management of ubiquitous environments," *Journal of Communication and Computer*, vol. 10, no. 12, 2013.
[9] D. Hussein, E. Bertin, and V. Frey, "A community-driven access control approach in distributed IoT environments," *IEEE Communications Magazine*, vol. 55, pp. 146–153, 2017.
[10] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the Internet of Things." *Mathematical and Computer Modelling*, vol. 58, no. 5-6, pp. 1189–1205, 2013.
[11] J. Bernal Bernabe, J. L. Hernandez Ramos, and A. F. Skarmeta Gomez, "TACIoT: Multidimensional trust-aware access control system for the Internet of Things," *Soft Comput.*, vol. 20, no. 5, pp. 1763–1779, May 2016. [Online]. Available: http://dx.doi.org/10.1007/s00500-015-1705-6
[12] V. F. Rodrigues, E. Correa, C. A. da Costa, and R. da Rosa Righi, "On exploring proactive cloud elasticity for Internet of Things demands," in *2017 XLIII Latin American Computer Conf. (CLEI)*, Sept 2017, pp. 1–10, doi:10.1109/CLEI.2017.8226417.
[13] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.
[14] D. Santos, J. Cesconetto, J. Martins, L. Silva, I. Ochôa, and V. Leithardt, "Ubipri pripro - controle e gerenciamento de perfis de usuários com base na privacidade de dados," in *15 Escola Regional de Redes de Computadores*, ERRC 2017. SBC, 2017.
[15] V. Leithardt, L. Henrique Andrade Correia, G. Borges, A. Rossetto, C. Rolim, C. Geyer, and J. M. Sá Silva, "Mechanism for privacy management based on data history (ubipri-his)," vol. 10, pp. 11–19, 03 2018, doi: 10.5383/JUSPN.10.01.002.
[16] J. H. Sarker and A. M. Nahhas, "Mobile RFID system in the presence of denial-of-service attacking signals," *IEEE Transactions on Automation Science and Engineering*, vol. 14, no. 2, pp. 955–967, April 2017, doi:10.1109/TASE.2016.2547989.

Valderi Leithardt recebeu seu título de Doutor em Ciência da Computação pela Universidade Federal do Rio Grande do Sul, Brasil, em 2015. É Professor da Universidade do Vale do Itajaí – Univali - Brasil e da Universidade Beira Interior - Portugal. Também é pesquisador do Laboratory of Embedded and Distributed Systems da Univali e COPELABS da ULHT, Lisboa - Portugal. Tópicos de Interesse são Sistemas Distribuídos, Privacidade de Dados e IoT.



Douglas Santos recebeu o título de Bacharel em Engenharia de Computação pela Universidade do Vale do Itajaí – Univali, Brasil, e é estudante do curso de Mestrado em Computação Aplicada da Univali. Atua no Laboratory of Embedded and Distributed Systems da Univali e no Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier – LIRMM, França. Seus tópicos de interesse são Sistemas Embarcados, Linguagens de Programação e Sistemas Tolerantes a Faltas.

Luis Silva recebeu seu título de Mestre em Computação Aplicada pela Universidade do Vale do Itajaí, Brasil, em 2019. É pesquisador colaborador do Laboratory of Embedded and Distributed Systems da Univali e do Expert Systems and Applications Lab da Universidade de Salamanca, Espanha. Seus tópicos de interesse são Sistemas Distribuídos, Computação Ubíqua, Privacidade de Dados e Desenvolvimento para Dispositivos Móveis.



Felipe Viel recebeu seu título de Mestre em Computação Aplicada pela Universidade do Vale do Itajaí, Brasil, em 2019. É Professor Assistente da Escola do Mar, Ciência e Tecnologia da Univali, Brasil, desde 2019, e pesquisador do Laboratory of Embedded and Distributed Systems da Univali. Suas áreas de interesse incluem: Sistemas Embarcados, Sistemas Reconfiguráveis, Aceleradores em Hardware, Processamento Digital de Imagens, Aviônica e Sistemas de Alta Confiabilidade.

Cesar Zeferino recebeu seu título de Doutor em Ciência da Computação pela Universidade Federal do Rio Grande do Sul, Brasil, em 2003, com estágio na Université Paris-Sorbonne, França. É professor titular da Escola do Mar, Ciência e Tecnologia da Univali, Brasil, desde 2002, Gerente de Pesquisa e Pós-Graduação da Univali e líder do Laboratory of Embedded and Distributed Systems da Univali. Seus tópicos de interesse são Aceleradores de Hardware, Internet das Coisas e Networks-on-Chip.

Jorge Silva recebeu seu título de Doutor em Engenharia Informática pela Universidade de Coimbra, em 2001, onde é Professor Associado com Habilitação no Departamento de Engenharia Elétrica e de Computação da Faculdade de Ciências e Tecnologia e Pesquisador Sênior do Laboratório de Comunicação e Telemática do Centro de Engenharia Informática da Universidade de Coimbra. Seus principais interesses de pesquisa são Internet das Coisas, Protocolos de Rede e Redes de Sensores Sem Fio.