Dissertação: Autenticação não-invasiva para transações financeiras *hands-free* em locais conectados confiáveis

Victor Takashi Hayashi[1] **e Wilson Vicente Ruggiero**[1]

[1]Escola Politécnica – Universidade de São Paulo (USP)

{victor.hayashi, wruggiero}@usp.br

Abstract. *Virtual assistants deployed on smartphone and smart speaker devices enable hands-free financial transactions by voice commands. Even though these voice transactions are frictionless for end-users in trusted connected locations, they are susceptible to typical attacks to authentication protocols (e.g., replay). Using traditional knowledge-based or possession-based authentication with additional invasive interactions prejudice usability. State-of-the-art schemes for trusted devices with Physical Unclonable Functions (PUF) have complex enrollment processes. We propose a scheme based on a challenge response protocol with a trusted IoT autonomous device for hands-free scenarios (i.e., with no additional user interaction) integrated with a trusted connected location behavior for continuous authentication. The challenge-response protocol was validated with formal security tests with Burrows-Abadi-Needham logic and Scyther tool. A proof of concept with websockets presented an average response time of 383ms for mutual authentication using a 6-message protocol with a simple enrollment process. We performed hands-free activity recognition of a specific user based on a smart home testbed data from two months, obtaining an accuracy of 97% and a recall of 81%. Given the data minimization privacy principle, it is possible to reduce the total number of smart home events time series from 7 to 5. When compared to existing invasive solutions, our non-invasive mechanism contributes to enhance financial institutions virtual assistants usability while maintaining security and privacy.*

Resumo. *Assistentes pessoais em dispositivos móveis e smart speakers permitem transações financeiras sem o uso das mãos por comandos de voz. Mesmo que essas transações de voz sejam úteis para os usuários finais em ambientes conectados confiáveis, elas são suscetíveis a ataques típicos a protocolos de autenticação (e.g., ataque de replay). O uso da autenticação tradicional baseada em conhecimento ou posse de dispositivo confiável com interações invasivas adicionais prejudica a usabilidade. Soluções propostas na literatura com dispositivos confiáveis usam Funções Físicas Não-Clonáveis (PUF) com processos de cadastramento complexo. É proposto um mecanismo de autenticação não-invasivo com protocolo desafio-resposta com um dispositivo autônomo IoT confiável integrado com o comportamento de um local conectado confiável para autenticação continuada. O protocolo desafio-resposta foi validado por meio de provas formais de segurança com lógica Burrows-Abadi-Needham e ferramenta Scyther. Uma prova de conceito com websockets apresentou um tempo médio de resposta de 383ms para autenticação mútua usando um protocolo de 6 mensagens com um processo de cadastro simples. Realizamos o reconhecimento de*

atividades sem o uso das mãos de um usuário específico com base em dados de uma casa inteligente de dois meses, obtendo uma acurácia de 97% e uma revocação de 81%. Dado o princípio de privacidade de minimização de dados, é possível reduzir o número total de séries temporais de eventos de casa inteligente de 7 para 5. Quando comparado às soluções invasivas existentes, o mecanismo não invasivo proposto contribui para aprimorar a usabilidade dos assistentes virtuais das instituições financeiras, ao mesmo tempo que mantém a segurança e a privacidade do usuário.

1. Dados Gerais

- **Título em português da dissertação**: Autenticação não-invasiva para transações financeiras *hands-free* em locais conectados confiáveis
- **Título em inglês da dissertação**: Non-invasive authentication for hands-free financial transactions in trusted connected locations
- **Nome do Autor**: Victor Takashi Hayashi
- **Afiliação do Autor**: Escola Politécnica da Universidade de São Paulo
- **Nome do Orientador**: Wilson Vicente Ruggiero
- **Afiliação do Orientador**: Escola Politécnica da Universidade de São Paulo

2. Motivações

Assistentes inteligentes estão permitindo interações com mãos-livres por comandos de voz em locais conectados confiáveis. A base instalada do Google Assistant em *smartphones* e alto-falantes inteligentes ultrapassa 1 bilhão de dispositivos [1], enquanto o Amazon Alexa é implantado em mais de 100 milhões de dispositivos de alto-falante inteligentes [2]. 20% dos adultos dos EUA relataram ter um alto-falante inteligente em 2018 [3].

As interações de voz fornecem serviços abrangentes por integração com dispositivos da Internet das Coisas (IoT) presentes em locais conectados. A Ericsson estima 18 bilhões desses dispositivos conectados até 2022 [4]. Esses objetos cotidianos com capacidades de detecção, processamento e atuação se comunicam entre si para oferecer serviços convenientes aos usuários em tempo hábil [Köckemann et al. 2020].

No entanto, a segurança em ambientes de Internet das Coisas (IoT) ainda é uma questão em aberto [Nandy et al. 2019, Hassija et al. 2019, Kavianpour et al. 2019]. No cenário mãos-livres considerado, alguns ataques relevantes são personificação, replay, síntese de fala e conversão de fala. Em um ataque de personificação, o oponente é outro ser humano que tenta imitar a voz de um usuário legítimo; em um ataque de repetição, um áudio de comando de voz legítimo gravado anteriormente é reproduzido em um dispositivo com um alto-falante integrado próximo ao dispositivo de alto-falante inteligente comprometido por um invasor; a síntese de voz pode ser usada por oponentes para gerar comandos de voz artificialmente; e na conversão de voz, o oponente pode modelar a voz de um usuário legítimo usando técnicas de aprendizado estatístico [Sahidullah et al. 2019].

[1] https://www.cnet.com
[2] https://www.theverge.com
[3] https://voicebot.ai/
[4] https://www.ericsson.com

As transações sem as mãos por voz nesses ambientes de IoT podem variar de transferências de dinheiro P2P (pessoa a pessoa), contas de serviços públicos [5] e entrega de comida [6] pagamentos. Por exemplo, o Axis Bank Alexa Skill [7] possibilita que os usuários acessem seus saldo, obtenha a fatura do cartão de crédito, consulte o histórico de transações e até bloqueie cartões com o assistente pessoal; O American Express Alexa Skill [8] permite que os usuários acessem as informações da conta e façam pagamentos por voz; Capital One Alexa Skill [9] permite que os usuários verifiquem seu saldo, acompanhem gastos e paguem contas.

As soluções de autenticação existentes para essas transações são baseadas em mecanismos invasivos, como notificação de *smartphone* [10] . Os usuários optam por interagir com alto-falantes inteligentes usando comandos de voz porque percebem que exige menos esforço quando comparado à alternativa de *smartphone* [Ponticello 2020], portanto, uma autenticação invasiva que requer interação adicional com outro dispositivo pode ser impraticável para ampla adoção.

Alexa fornece o Alexa PIN, um PIN de 4 dígitos necessário para interação do usuário com a American Express Skill [11]. No caso do Axis Bank Skill, seus Termos e Condições afirmam que o Banco não é responsável por possíveis perdas incorridas pelo uso indevido do PIN Alexa [12]. Os Termos e Condições do Capital One Alexa Skill deixam claro que o comando de voz não é usado para autenticação e que a Amazon pode ter acesso por meio de conversas realizadas [13]. O código SMS e os códigos falados de 4 dígitos são mecanismos comumente usados com sistemas de reconhecimento de voz [de Barcelos Silva et al. 2020].

Como exigir a confirmação por uma interface diferente da interface de fala deixa os usuários frustrados ao interagir com assistentes pessoais [de Barcelos Silva et al. 2020], é razoável considerar que uma autenticação não invasiva poderia melhorar a usabilidade, mantendo a segurança para transações financeiras sem as mãos.

Trabalhos relacionados encontrados na literatura que apresentam esquemas não invasivos [Das et al. 2020] usam funções físicas não clonáveis diretamente em protocolos de autenticação, resultando em procedimentos de registro complexos (ou seja, registro offline de pares desafio-resposta). Outras soluções contam com biometria de voz e também apresentam um processo de cadastro complexo [Pradhan et al. 2019, Meng et al. 2018]. Consideramos alguns esquemas de última geração baseados em wearables como soluções invasivas [Feng et al. 2017, Gao et al. 2019]. Outros trabalhos relacionados são soluções de fator único [Das et al. 2020, Nespoli et al. 2019].

[5]https://www.livemint.com/
[6]https://www.startse.com
[7]https://www.axisbank.com/
[8]https://www.americanexpress.com/
[9]https://www.capitalone.com/
[10]https://www.daon.com/
[11]https://www.americanexpress .com/
[12]https://www.axisbank.com/
[13]https://www.capitalone.com

3. Objetivo

Propor um mecanismo de autenticação que não exija interação invasiva adicional do usuário para transações financeiras sem as mãos por voz em um local conectado confiável e prove que tal solução tem desempenho e níveis de segurança comparáveis com as soluções de autenticação invasiva existentes (por exemplo, token em dispositivo móvel, Alexa PIN). O processo de cadastramento associado deve ser simples.

4. Resultados Obtidos

Os principais resultados obtidos são:

- **Mecanismo** de autenticação não invasivo para transações financeiras *hands-free* por voz em locais conectados confiáveis, com dispositivo de hardware autônomo e processo de cadastro simples, apresentando tempo de resposta e nível de segurança comparáveis às soluções invasivas existentes;
- **Protocolo** de desafio-resposta para autenticação mútua entre um servidor e um dispositivo IoT, com um verdadeiro gerador de números aleatórios baseado em funções físicas não clonáveis (PUF) para maior aleatoriedade de nonces;
- Um **método** para aprendizado de comportamento baseado em dados coletados por dispositivos IoT e técnicas de aprendizado de máquina para avaliar o nível de confiança de um local conectado confiável.

Os resultados obtidos tornaram possível validar as seguintes hipóteses:

Hipótese 1: é viável realizar uma autenticação continuada baseada em aprendizado de comportamento com dados coletados por dispositivos de Internet das Coisas instalados em um local conectado confiável (e.g., uma casa conectada).

Hipótese 2: Requisitos de desempenho e privacidade para autenticação não-invasiva são atendidos por meio de uma arquitetura de processamento na ponta, privacidade por *design* e ambiente inteligente.

5. Produção Científica Associada

- **Periódicos (3)**
  - (Fator de Impacto 3.576, Qualis A1) [Hayashi and Ruggiero 2022]
  - (Fator de Impacto 3.576, Qualis A1) [Hayashi and Ruggiero 2020]
  - [Hayashi et al. 2020c]
- **Conferências (4)**
  - (Qualis A4) [Hayashi et al. 2021]
  - (Qualis B2) [Hayashi et al. 2020a]
  - [Hayashi et al. 2020b]
  - [Arakaki et al. 2020]
- **Workshops (2)**
  - XI Workshop de Gestão de Identidades Digitais (WGID).Geração de Dados Sintéticos para Autenticação Continuada em Local Conectado Confiável. 2021.
  - VI Workshop de Regulação, Avaliação da Conformidade, Certificação e Educação em Cibersegurança (WRAC+). Avaliação Formal de Protocolos de Autenticação usando Lógica BAN e Ferramenta Scyther. 2021.

6. Endereço Web no qual está disponível a dissertação

https://www.teses.usp.br/teses/disponiveis/3/3141/tde-21062022-140511/pt-br.php

7. Contribuição e Originalidade do Trabalho para a Área

Uma comparação da solução proposta e trabalhos relacionados encontrados na literatura é apresentada na Tabela 1.

A primeira coluna é a referência da solução proposta encontrada na literatura. As colunas "Dispositivo Confiável", "Biometria"e "Comportamento"descrevem quais mecanismos básicos de autenticação são usados em cada solução. A coluna "Invasivo"apresenta se o trabalho relacionado possui uma autenticação invasiva ou não invasiva. De forma semelhante, a coluna "Cadastro"apresenta se o processo de cadastro associado é considerado simples ou complexo. Esses aspectos são características das soluções, não são considerados para avaliar quão bem cada solução está resolvendo o problema.

A comparação é realizada com base nos aspectos "Usuários", "Acurácia"e "Tempo de Resposta (ms)". A "Acurácia"apresenta o resultado de precisão obtido com a solução proposta, e o "Tempo de Resposta (ms)"apresenta o tempo total de resposta do usuário desde a solicitação de autenticação até o resultado da autenticação.

Solução	**Dispositivo Confiável**	**Biometria**	**Comportamento**	**Invasivo**	**Cadastro**	**Usuários**	**Acurácia**	**Tempo de Resposta (ms)**
VoicePop [Wang et al. 2019]	Não	Sim	Não	Não	Complexo	18	90%	-
2MA [Blue et al. 2018]	Não	Sim	Não	Não	Complexo	-	84%	-
VSButton [Lei et al. 2018]	Não	Não	Sim	Não	Complexo	-	-	-
WifiU [Shahzad and Singh 2017]	Não	Sim	Sim	Não	Complexo	50	92%	-
Shi et al. [Shi et al. 2017]	Não	Não	Sim	Não	Complexo	11	92%	-
UCFL [Das et al. 2020]	Sim	Não	Não	Não	Simples	-	-	150
EarEcho [Gao et al. 2019]	Não	Sim	Não	Sim	Complexo	20	95%	1000
PALOT [Nespoli et al. 2019]	Não	Não	Sim	Não	Complexo	24	70%	-
REVOLT [Pradhan et al. 2019]	Não	Sim	Sim	Não	Complexo	10	97%	1100
Wivo [Meng et al. 2018]	Não	Não	Sim	Não	Complexo	5	96%	320
VAuth [Feng et al. 2017]	Sim	Sim	Não	Sim	Simples	18	97%	300
Solução Proposta	Sim	Não	Sim	Não	Simples	4	97%	383

Tabela 1. Comparação da Solução Proposta com os Trabalhos Relacionados.

Conforme mostrado na Tabela 1, a solução proposta tem uma precisão de 97%, comparável a REVOLT [Pradhan et al. 2019] e VAuth [Feng et al. 2017]. No entanto, o REVOLT possui um processo de cadastramento complexo, pois é baseado em fatores de autenticação biométrica e comportamental, que requerem tempo de treinamento ou registro biométrico específico, e o VAuth é uma solução invasiva.

O tempo de resposta de 383 ms apresentado pela Prova de Conceito com a versão SHA-256 é comparável ao VAuth e Wivo [Meng et al. 2018]. Ainda assim, o Wivo conta apenas com o fator de autenticação de comportamento, portanto, possui um processo de cadastramento complexo devido à sua fase de treinamento. UCFL [Das et al. 2020] apresenta o melhor tempo de resposta, embora também conte com um fator de autenticação de dispositivo confiável exclusivo.

Embora a abordagem tenha sido avaliada com menos usuários do que o trabalho relacionado, validamos em um cenário do mundo real (ou seja, "na natureza") sem controle sobre a rotina dos habitantes no período de coleta de dados de consumo de energia de

2 meses. Além disso, realizamos reconhecimento de atividades e pessoas em um cenário multiusuário com 4 pessoas. O número total de usuários pode parecer pequeno, mas argumentamos que esse número é uma propriedade compartilhada por muitos ambientes domésticos ou até mesmo de escritório. Vale ressaltar que o trabalho relacionado baseado em sensores estacionários em um local conectado não suporta cenários multiusuário [Shahzad and Singh 2017, Shi et al. 2017, Nespoli et al. 2019].

Embora o cadastro proposto possa não ser considerado simples devido ao número de chaves compartilhadas, consideramos simples com base no cadastro complexo com mecanismos de PUF encontrados na literatura.

O VSButton [Lei et al. 2018] reconhece as atividades, mas não quem as está realizando. O Wivo realiza a vivacidade de voz de certas pessoas, mas não reconhece a atividade associada, e foi validado com dois usuários no cenário de múltiplos usuários [Meng et al. 2018]. O PALOT contou com um conjunto de dados de um apartamento onde os participantes foram solicitados a realizar certas atividades diárias enquanto interagiam com os sensores implantados, por isso apresentou um certo grau de controle sobre as atividades dos habitantes [Nespoli et al. 2019]. WifiU realizou experimentos para coletar dados de marcha em um laboratório típico com área de 50 metros quadrados, que é um ambiente controlado [Shahzad and Singh 2017].

Considerando que o cenário multiusuário é um desafio para o desenvolvimento de algoritmos de casa inteligente [Nef et al. 2015, Liu et al. 2017], e que é difícil implementar um controle de acesso granular para alto-falantes inteligentes em ambientes multiusuário, defendemos que nossa abordagem contribua para fechar esta lacuna de pesquisa, apresentando uma maneira de realizar o reconhecimento de atividade mãos-livres de uma pessoa específica. A abordagem se baseia em dados de consumo de energia no nível do dispositivo de dois ambientes diferentes para obter resultados aceitáveis de precisão e recuperação.

Dentre as possíveis expansões em trabalhos futuros, destacam-se como o processo de aprendizado de hábito pode ser refinado a partir da instalação da solução em um conjunto maior de residências ou outros locais confiáveis (e.g., escritório), e como a solução pode se adaptar no cenário de mudança de comportamento, uma vez que o presente trabalho considerou um hábito padrão fixo.

Referências

[Arakaki et al. 2020] Arakaki, R., Hayashi, V. T., and Ruggiero, W. V. (2020). Available and Fault Tolerant IoT System: Applying Quality Engineering Method. In *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, pages 1–6.

[Blue et al. 2018] Blue, L., Abdullah, H., Vargas, L., and Traynor, P. (2018). 2MA. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, New York, NY, USA. ACM.

[Das et al. 2020] Das, A. K., Kalam, S., Sahar, N., and Sinha, D. (2020). UCFL: User Categorization using Fuzzy Logic towards PUF based Two-Phase Authentication of Fog assisted IoT devices. *Computers and Security*, 97.

[de Barcelos Silva et al. 2020] de Barcelos Silva, A., Gomes, M. M., da Costa, C. A., da Rosa Righi, R., Barbosa, J. L. V., Pessin, G., De Doncker, G., and Federizzi, G. (2020). Intelligent personal assistants: A systematic literature review.

[Feng et al. 2017] Feng, H., Fawaz, K., and Shin, K. G. (2017). Continuous authentication for voice assistants. In *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*, volume Part F131210, pages 343–355. Association for Computing Machinery.

[Gao et al. 2019] Gao, Y., Wang, W., Phoha, V. V., Sun, W., and Jin, Z. (2019). EarEcho. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(3).

[Hassija et al. 2019] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., and Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access*, 7:82721–82743.

[Hayashi et al. 2020a] Hayashi, V., Garcia, V., Manzan de Andrade, R., and Arakaki, R. (2020a). OKIoT Open Knowledge IoT Project: Smart Home Case Studies of Short-term Course and Software Residency Capstone Project. In *Proceedings of the 5th International Conference on Internet of Things, Big Data and Security*, pages 235–242. SCITEPRESS - Science and Technology Publications.

[Hayashi and Ruggiero 2020] Hayashi, V. and Ruggiero, W. (2020). Non-Invasive Challenge Response Authentication for Voice Transactions with Smart Home Behavior. *Sensors*, 20(22).

[Hayashi et al. 2020b] Hayashi, V. T., Arakaki, R., Fujii, T. Y., Khalil, K. A., and Hayashi, F. H. (2020b). B2B B2C Architecture for Smart Meters using IoT and Machine Learning: a Brazilian Case Study. In *2020 International Conference on Smart Grids and Energy Systems (SGES)*. IEEE.

[Hayashi et al. 2020c] Hayashi, V. T., Arakaki, R., and Ruggiero, W. V. (2020c). OKIoT: Trade off analysis of smart speaker architecture on open knowledge IoT project. *Internet of Things*, 12.

[Hayashi et al. 2021] Hayashi, V. T., Ribeiro, C. M. N., Quintino Filho, A., Pita, M. A. B., Trazzi, B. M., Estrella, J. C., and Ruggiero, W. V. (2021). Improving IoT Module Testability with Test-Driven Development and Machine Learning. In *2021 8th International Conference on Future Internet of Things and Cloud (FiCloud)*, pages 406–412.

[Hayashi and Ruggiero 2022] Hayashi, V. T. and Ruggiero, W. V. (2022). Hands-Free Authentication for Virtual Assistants with Trusted IoT Device and Machine Learning. *Sensors*, 22(4):1325.

[Kavianpour et al. 2019] Kavianpour, S., Shanmugam, B., Azam, S., Zamani, M., Narayana Samy, G., and De Boer, F. (2019). A Systematic Literature Review of Authentication in Internet of Things for Heterogeneous Devices. *Journal of Computer Networks and Communications*, 2019.

[Köckemann et al. 2020] Köckemann, U., Alirezaie, M., Renoux, J., Tsiftes, N., Ahmed, M. U., Morberg, D., Lindén, M., and Loutfi, A. (2020). Open-source data collection and data sets for activity recognition in smart homes. *Sensors (Switzerland)*, 20(3).

[Lei et al. 2018] Lei, X., Tu, G. H., Liu, A. X., Li, C. Y., and Xie, T. (2018). The insecurity of home digital voice assistants - Vulnerabilities, attacks and countermeasures. In *2018 IEEE Conference on Communications and Network Security, CNS 2018*. Institute of Electrical and Electronics Engineers Inc.

[Liu et al. 2017] Liu, Y., Ouyang, D., Liu, Y., and Chen, R. (2017). A novel approach based on time cluster for activity recognition of daily living in smart homes. *Symmetry*, 9(10).

[Meng et al. 2018] Meng, Y., Zhang, W., Zhu, H., and Shen, X. S. (2018). Securing Consumer IoT in the Smart Home: Architecture, Challenges, and Countermeasures. *IEEE Wireless Communications*, 25(6):53–59.

[Nandy et al. 2019] Nandy, T., Idris, M. Y. I. B., Md Noor, R., Mat Kiah, L., Lun, L. S., Annuar Juma'at, N. B., Ahmedy, I., Abdul Ghani, N., and Bhattacharyya, S. (2019). Review on Security of Internet of Things Authentication Mechanism. *IEEE Access*, 7.

[Nef et al. 2015] Nef, T., Urwyler, P., Büchler, M., Tarnanas, I., Stucki, R., Cazzoli, D., Müri, R., and Mosimann, U. (2015). Evaluation of three state-of-the-art classifiers for recognition of activities of daily living from smart home ambient data. *Sensors (Switzerland)*, 15(5):11725–11740.

[Nespoli et al. 2019] Nespoli, P., Zago, M., Celdrán, A. H., Pérez, M. G., Mármol, F. G., and Clemente, F. J. (2019). PALOT: Profiling and authenticating users leveraging internet of things. *Sensors (Switzerland)*, 19(12).

[Ponticello 2020] Ponticello, A. (2020). *Towards Secure and Usable Authentication for Voice-Controlled Smart Home Assistants*. PhD thesis, Wien.

[Pradhan et al. 2019] Pradhan, S., Sun, W., Baig, G., and Qiu, L. (2019). Combating Replay Attacks Against Voice Assistants. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(3):1–26.

[Sahidullah et al. 2019] Sahidullah, M., Delgado, H., Todisco, M., Kinnunen, T., Evans, N., Yamagishi, J., and Lee, K.-A. (2019). Introduction to Voice Presentation Attack Detection and Recent Advances.

[Shahzad and Singh 2017] Shahzad, M. and Singh, M. P. (2017). Natural Web Interfaces Continuous Authentication and Authorization for the Internet of Things. Technical report.

[Shi et al. 2017] Shi, C., Liu, J., Liu, H., and Chen, Y. (2017). Smart User Authentication through Actuation of Daily Activities Leveraging WiFi-enabled IoT. pages 1–10. Association for Computing Machinery (ACM).

[Wang et al. 2019] Wang, Q., Lin, X., Zhou, M., Chen, Y., Wang, C., Li, Q., and Luo, X. (2019). VoicePop: A Pop Noise based Anti-spoofing System for Voice Authentication on Smartphones. Technical report.