Abordagem IoT DB-Audit: uma contribuição a adequação do middleware EXEHDA à Lei Geral de Proteção de Dados

Rogério Albandes[1,2], Rodrigo Lambrecht[2], Leandro Pieper[2], Franklin Barcellos[3], Ana Marilza Pernas[1], Adenauer Yamin[1,2]

[1]Programa de Pós-Graduação em Computação (PPGC/UFPel)

[2]Mestrado em Engenharia Eletrônica e Computação (MEEC/UCPel)

[3]Universidade Católica de Pelotas (UCPel)

Abstract. *The use of the Internet of Things, especially in the healthcare sector, raises concerns related to the handling of personal data. The LGPD regulates the protection of this data in Brazil, encouraging IoT middleware to consider aspects related to their privacy and security. This article discusses the design of an approach, called IoT DB-Audit, that uses database auditing and alerts arising from the processing of association rules to promote compliance with the LGPD. An initial evaluation by users had positive feedback, indicating that the inclusion of auditing can improve the security and privacy of information stored in databases managed by IoT middleware.*

Resumo. *O emprego da Internet das Coisas, especialmente na área da saúde, gera preocupações relacionadas ao manuseio de dados pessoais. A LGPD regulamenta a proteção desses dados no Brasil, incentivando middlewares IoT a considerarem aspectos relacionados à privacidade e segurança dos mesmos. Este artigo discute a concepção de uma abordagem, denominada IoT DB-Audit, que utiliza auditoria em bancos de dados e alertas decorrentes do processamento de regras de associação para promover conformidade com a LGPD. Uma avaliação inicial por usuários teve um retorno positivo, indicando que a inclusão de auditoria pode melhorar a segurança e a privacidade das informações armazenadas em bancos de dados gerenciados por middlewares IoT.*

1. Introdução

A Internet das Coisas (IoT) se caracteriza por um elevado potencial de impactar uma ampla gama de setores da sociedade moderna. Particularmente, na área da saúde, é crucial atentar para o grande volume de dados pessoais sensíveis usualmente manipulados. A privacidade dos dados gerados nesses processos é uma preocupação social central, uma vez que na IoT o acompanhamento é distribuído, possibilitando assim um monitoramento constante e uma análise em *soft real-time* de muitos aspectos da vida cotidiana dos pacientes [Hon et al. 2016].

Essa preocupação é agravada pelo emprego da computação em nuvem e suas metodologias de armazenamento e processamento dos dados coletados, levando a IoT a ser uma prioridade para os órgãos reguladores de proteção de dados [Weber 2010].

A LGPD foi criada para proteger os direitos fundamentais de liberdade, privacidade e desenvolvimento da personalidade das pessoas naturais. Seu objetivo principal

é estabelecer um ambiente de segurança jurídica, padronizando regulamentos e práticas para garantir a proteção dos dados pessoais de todos os cidadãos brasileiros, seguindo padrões internacionais [de Oliveira et al. 2019].

A abordagem discutida neste artigo, denominada , tem como objetivo central abordar o problema de pesquisa relacionado a auditaria de bancos de dados em *middlewares* para IoT baseados em serviços. A introdução da auditoria pode aumentar a segurança, garantindo maior consistência nos dados provenientes de sensores e outras fontes de entrada de dados. Como resultado, busca-se promover a conformidade desses *middlewares* com a LGPD.

A concepção da abordagem Abordagem IoT DB-Audit: uma contribuição a adequação do middleware EXEHDA à Lei Geral de Proteção de Dados contempla a integração de: (i) uma plataforma de criação de triggers no Repositório de Informações Contextuais (RIC) do *middleware* EXEHDA para construir a tabela de auditoria; (ii) um ambiente de análise de dados para processar a auditoria coletada, visando enviar alerta e gerar relatórios sobre eventos suspeitos identificados pela auditoria; e (iii) uma interface de visualização textual e gráfica usada para incluir as tabelas a serem auditadas e visualizar os eventos gerados pelas regras de associação processadas pelo algoritmo Apriori.

A expectativa com a IoT DB-Audit é que o *middleware* avance em conformidade e maturidade em relação às diretrizes da LGPD. Vários possíveis *gaps* de segurança ao longo da arquitetura do *middleware* EXEHDA foram identificados, resultando em problemas de integridade e, consequentemente, de confiabilidade dos dados armazenados. A auditoria e os alertas gerados pela abordagem visam garantir a integridade e a confiabilidade dos dados, impulsionando o EXEDHA a progredir para se tornar compliance com a LGPD.

2. Desafios da LGPD em *middlewares* IoT

A Lei Geral de Proteção de Dados Pessoais (LGPD) [da República 2018], Lei nº 13.709/2018, é a legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16º do Marco Civil da Internet.

Embora diversas tecnologias de *middleware* para IoT sejam utilizadas para atender aos requisitos de segurança mais relevantes exigidos pelas diversas aplicações existentes, com o advento de marcos regulatórios como a LGPD e similares, o nível de exigência em termos de segurança e privacidade de dados impulsiona as pesquisas para um novo período. O momento da obrigatoriedade pela proteção de dados pessoais.

Garantir o controle de acesso aos dados coletados da IoT em servidores ou na nuvem é um desafio para a privacidade. Argumenta-se que os modelos tradicionais de controle de acesso não são adequados para a escala e o escopo da IoT. Além disso, o compartilhamento de dados entre *middlewares* para a IoT também apresenta desafios. Assim, o armazenamento e compartilhamento de dados de IoT requerem técnicas apropriadas para garantir o consentimento e a privacidade do usuário [Pereira et al. 2022].

Segurança e Auditoria de Banco de Dados

A auditoria em bancos de dados visa manter a integridade e confiabilidade dos dados, controlar o acesso e as mudanças nos dados e na estrutura, além de monitorar os acessos

e os papéis de cada usuário [Anwar et al. 2021]. Também visa aprimorar e assegurar a credibilidade das informações armazenadas, verificando se as atividades na base de dados estão conforme as diretrizes estabelecidas pela política da empresa ou pela legislação.

A auditoria considera as seguintes premissas: (i) registro de logon/off; (ii) registro de uso; e (iii) registro de atributos de segurança (privilégios, usuário/login e alterações de senha). Este processo começa com a criação de gatilhos que alimentam tabelas responsáveis por coletar dados para a auditoria. Os relatórios resultantes incluem atividades suspeitas de acesso, usuários inativos, acesso fora do horário de operação, dados de sinais vitais fora do intervalo esperado e/ou padrões normais.

Regras de Associação

As regras de Associação visam identificar elementos que frequentemente ocorrem juntos em uma mesma transação, revelando relacionamentos ou padrões entre conjuntos de dados [Hipp et al. 2000]. Uma transação refere-se aos itens consultados durante uma operação específica.

Diversos algoritmos se destacam na mineração de padrões frequentes. Apriori, Reduced Association Rule Mining (RARM), Equivalence Class Transformation (ECLAT), Frequent Pattern Growth (FP-Growth), dentre outros. Cada um desses algoritmos tem seus pontos fortes e fracos, e a escolha do algoritmo depende de fatores como o tamanho e as características do conjunto de dados, os recursos computacionais e os requisitos da tarefa de mineração. Nesta fase do trabalho será utilizado o Algoritmo Apriori.

O algoritmo Apriori é um método de mineração de dados que identifica conjuntos de itens frequentes em um banco de dados. Ele utiliza um processo iterativo de duas etapas: junção e remoção. Na junção, gera conjuntos de itens candidatos a partir dos itens frequentes da iteração anterior. Em seguida, verifica o suporte desses conjuntos no conjunto de dados. Conjuntos que ultrapassem o limite de capacidade de suporte são considerados frequentes [Abbass et al. 2020].

3. Trabalhos Relacionados

A LGPD é muito recente, inspirada na General Data Protection Regulation (GDPR) da Comunidade Européia. Um esforço de pesquisa foi realizado para identificar trabalhos relacionadas à adequação de abordagens relacionadas a IoT que utilizam dados pessoais à GDPR, dentre as quais foram selecionados cinco trabalhos. Para sua seleção o trabalho deveria contemplar os seguintes aspectos: (i) segurança em banco de dados na IoT; (ii) compliance a GDPR; e (iii) prioridade na preservação da privacidade de dados pessoais.

No trabalho de [Kammüller et al. 2019], são investigadas as implicações da GDPR no design de um sistema de saúde IoT. Foi proposto um modelo de rotulagem de dados para apoiar o controle de acesso aos dados de pacientes críticos à privacidade, juntamente com o processo Fusion/UML para projetar um sistema compatível com o GDPR. É ilustrado esse processo de design no estudo de caso do monitoramento, baseado em IoT, de pacientes com Alzheimer.

O artigo de [Pappachan et al. 2020] identifica um caso de uso, no contexto de espaços inteligentes emergentes, nos quais os sistemas podem ser exigidos por legislações, como o GDPR da Europa e o CCPA da Califórnia, a capacitar os usuários

a especificar quem pode ter acesso aos seus dados e para quais propósitos. Apresenta o SIEVE, uma abordagem em camadas para implementar *Fine-Grained Access Control* (FGAC) em sistemas de banco de dados existentes, que explora uma variedade de suas características, como sugestões de uso de índices e explicação de consultas. Dada uma consulta, o SIEVE explora seu contexto para filtrar as políticas que precisam ser verificadas.

O trabalho de [Semantha et al. 2023] projeta um framework para Privacidade por Design nos Registros Eletrônicos de Saúde (PbDinEHR) que preserve a privacidade dos pacientes durante a coleta, armazenamento, acesso e compartilhamento de dados, O trabalho analisa os princípios fundamentais de privacidade por design e estratégias de design de privacidade e a compatibilidade dos princípios de assistência médica propostos com Avaliação de Impacto de Privacidade (PIA), Princípios de Privacidade Australiana (APPs) e Regulamento Geral de Proteção de Dados (GDPR).

Na proposta de [Lee and Lee 2021], é apresentado um método para gerenciar com segurança informações pessoais em dispositivos IoT em ambientes de aplicativos de IoT conforme a GDPR. Primeiro, são descritas as etapas do ciclo de vida das informações pessoais ocorrendo nos serviços de aplicativos de IoT e é proposto um método para gerenciar com segurança informações pessoais em cada etapa do ciclo de vida conforme o fluxo de informações pessoais. Também é avaliada a utilidade e aplicabilidade do esquema proposto por meio de dois cenários de serviço.

Em [Badii et al. 2020] é apresentada a arquitetura Snap4City e suas soluções de segurança que respeitam a GDPR. A solução Snap4City aborda a segurança completa da pilha, desde dispositivos IoT, IoT Edge local, aplicações IoT na nuvem e local, análise de dados e painéis, apresentando uma série de soluções de segurança integradas que vão além do estado da arte. O teste de estresse também incluiu a adoção de testes de penetração para verificar a robustez da solução em relação a inúmeros aspectos de vulnerabilidade potencial.

Destaca-se como diferencial da IoT DB-Audit, no que diz respeito aos trabalhos relacionados, a utilização de regras de associação no sentido de avaliar possíveis comportamentos anômalos no banco de dados do *middleware*, realizando a emissão de alerta para os operadores do sistema. Com isso a IoT DB-Audit acrescenta uma camada de segurança e auditoria dos dados pessoais envolvidos. Outro fator relevante é o descarte de dados após o término do tratamento, mantendo, ao mesmo tempo, um registro desses descartes, conforme o preceituado pela LGPD.

4. Middleware EXEHDA

O EXEHDA consiste de um *middleware* baseado em serviços, o qual visa criar e gerenciar um ambiente computacional largamente distribuído, bem como promover a execução de aplicações ciente de situação sobre ele. O *middleware* vem sendo explorado em frentes de pesquisa que tratam desafios da IoT [Souza et al. 2018].

O EXEHDA possui uma organização composta por um conjunto de células de execução, conforme pode ser observado na Figura 1. Cada célula, no que diz respeito ao provimento de Ciência de Situação, é composta por um Servidor de Contexto (SC), e por diversos Servidores de Borda (SB) e/ou Gateways.

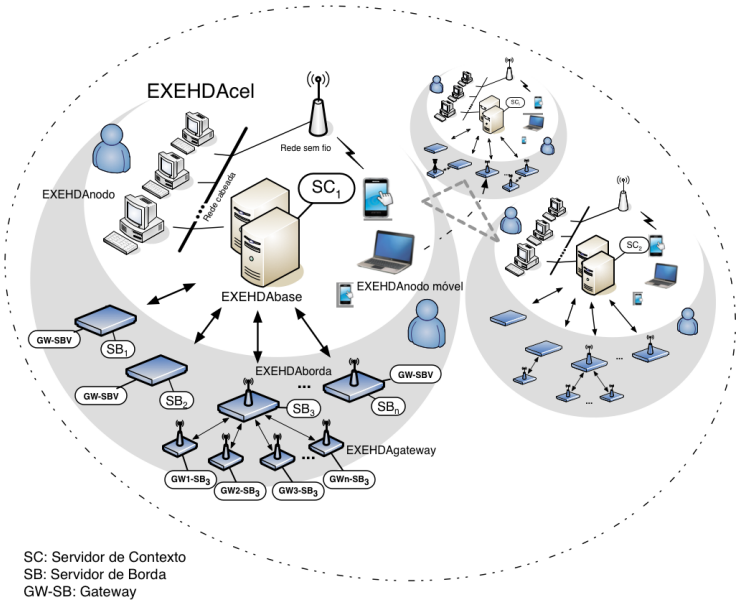

Figura 1. Ambiente para IoT gerenciado pelo EXEHDA

Os Gateways coletam dados contextuais de sensores físicos ou lógicos, com o objetivo de lidar com a heterogeneidade dos diversos tipos de sensores, tanto em termos de hardware quanto de protocolo, e, dessa forma, repassar essas informações de forma normalizada aos Servidores de Borda. No EXEHDA os Gateways são implementados sobre um hardware embarcado específico para a finalidade de interoperar com sensores e atuadores. No EXEHDA o processamento das informações contextuais é distribuído, ficando uma parte com o Servidor de Borda, e outra com o Servidor de Contexto (vide Figura 1).

Os dados recebidos pelos diversos Servidores de Borda são transmitidos ao Servidor de Contexto que os gerencia e realiza as etapas de armazenamento e processamento contextual. O Servidor de Contexto pode combinar os dados provenientes dos Servidores de Borda com informações históricas, que ficam registradas no Repositório de Informações Contextuais. Uma discussão mais ampla das diferentes funcionalidades tanto do *Gateway*, quanto dos Servidores de Borda está disponível em [Souza et al. 2018], por sua vez, uma avaliação das diferentes potencialidades do Servidor de Contexto pode ser encontrada em [Lopes et al. 2014].

5. Abordagem

A arquitetura de software concebida para a abordagem IoT DB-Audit está apresentada na Figura 2. A IoT DB-Audit permeia o *middleware* EXEHDA, como instrumento para o aumento na segurança e integridade dos dados armazenados em seu RIC, na expectativa de não gerar falsas análises e, por consequência, não emitir alertas desnecessários. Além disso, é também é analisado o banco de dados administrativo do EXEHDA com objetivo de avaliar o comportamento dos usuários. Na continuidade desta seção são tratadas as funcionalidades dos diferentes módulos, sendo discutidos seus perfis operacionais.

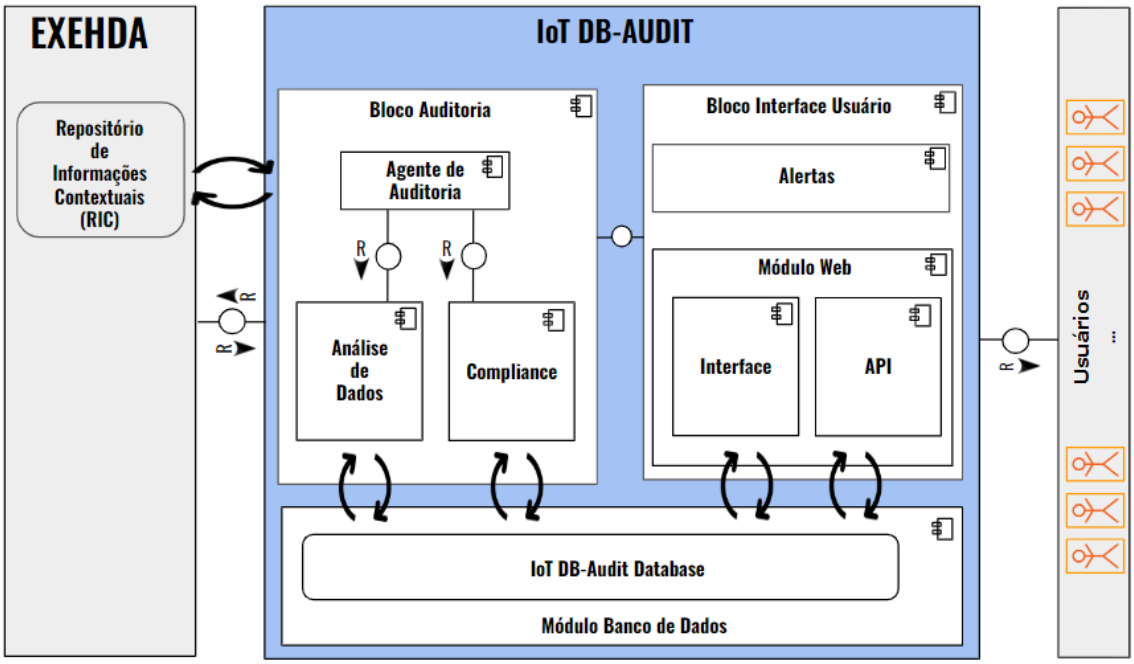

Figura 2. Arquitetura da IoT DB-Audit

5.1. Bloco de Auditoria

O Bloco de Auditoria é composto pelo Agente de Auditoria, Componente Análise de Dados e Componente *Compliance*. Ele adquire dados do RIC, grava tabelas de auditoria, gera regras de associação para identificar relacionamentos ou padrões frequentes entre conjuntos de dados e analisa dados fora desses padrões.

Componente Agente de Auditoria

O Componente Agente de Auditoria é responsável por consumir a API do EXEHDA, com objetivo de replicar no banco de dados da IoT DB-Audit a tabela de auditoria gerada no RIC.

Componente Análise de Dados

No Componente Análise de Dados, ocorre a mineração dos dados das tabelas de auditoria, que registram todas as transações realizadas pelos usuários e sensores do EXEHDA, ao qual a abordagem está conectada. Esses dados são armazenados em uma tabela especialmente modelada para a tarefa de auditoria, utilizando o formato JSON, por meio de gatilhos (triggers) do banco de dados.

Os dados registrados nas tabelas de auditoria são aproveitados para gerar Regras de Associação, que identificam elementos que frequentemente aparecem juntos em uma mesma transação, procurando relacionamentos ou padrões entre conjuntos de dados. O Algoritmo Apriori é empregado nessa análise. Atualmente, o Componente Análise de Dados visa estabelecer regras de associação entre: (i) Usuários e horários de login; (ii) Senhas erradas e usuários; (iii) Sensores e valores publicados; e (iv) Sensores e intervalos de tempo de publicação.

Além disso, como resultado da mineração de dados, são obtidos registros que estão fora do ciclo de vida, onde o término do tratamento de dados pessoais ocorre, conforme o artigo 15º da LGPD. Esses registros são gravados em tabelas específicas no banco de dados da abordagem para posterior utilização pelos demais componentes.

Componente *Compliance*

O Componente Compliance audita os dados gerados pelo Componente Análise de Dados. Ele compara os padrões provenientes das Regras de Associação com os dados nas tabelas de auditoria. Quando são identificados dados que não seguem o padrão estabelecido, o administrador do EXEHDA recebe alerta. Além disso, o Componente Compliance valida e informa sobre o término do tratamento de dados pessoais. Após a validação, ele descarta esses dados de forma definitiva e irreversível, seguindo os requisitos legais, incluindo as cópias de segurança. Também mantém registros específicos que evidenciam o processo de descarte, conforme as exigências da LGPD.

5.2. Bloco de Interface do Usuário

O Bloco de Interface do Usuário é composto pelo Componente Alertas e pelo Componente Web.

Componente Alertas

Na abordagem IoT DB-Audit, o papel dos alertas é preponderante, considerando as características dos dados envolvidos. Alertas serão emitidos à equipe responsável pelo *middleware* segundo a auditoria feita no módulo Auditoria. A proposta explora 2 serviços de mensagens que utilizam a Internet como meio: Pushover e Telegram; e o serviço de *Short Message Service* (SMS) da rede GSM (*Global System for Mobile Communications*) de telefonia celular.

Componente Web

O Componente Web é responsável por toda interface visual da proposta. Suas funções vão das rotinas de login até as visualizações de *dashboards* dos alertas e do funcionamento das regras de associação.

Componente API

Uma API (Interface de Programação de Aplicações, em português) é um conjunto de regras, protocolos e ferramentas que permite que diferentes softwares se comuniquem entre si. Na IoT DB-Audit foi construída uma API que permite a interoperabilidade com sistemas diferentes, fazendo com que sites e aplicativos acessem seus serviços e dados.

5.3. Bloco Banco de Dados

No Bloco Banco de Dados é utilizado o *database* Mysql visando armazenar as *triggers* que gravam nas tabelas de auditoria toda a movimentação dos dados armazenados no RIC do EXEHDA. Também são armazenados os logs dos dados descartados pelo Componente *Compliance*.

6. IoT DB-Audit Avaliação

Este Capítulo apresenta uma visão das avaliações realizadas na IoT DB-Audit. A concepção de sistemas complexos demanda diversos testes para garantir sua funcionalidade, interoperabilidade e estabilidade operacional.

6.1. Testes de Unidade, Integração e de Sistema

Tendo como premissa os princípios de boas práticas para o desenvolvimento de *software* discutidos no trabalho ([Ghedin 2022]), foram aplicados testes funcionais em três níveis para validar a estrutura de *software* proposta para a IoT DB-Audit.

No Teste de Unidade, unidades individuais de código são testadas isoladamente para garantir seu correto funcionamento, identificando e corrigindo falhas precocemente [Buchgeher et al. 2020]. O Teste de Unidade permite a detecção precoce de bugs, antecipando a manutenção e aumentando a qualidade do software. Testando unidades de código isoladamente, os problemas foram identificados e corrigidos antecipadamente, promovendo um desenvolvimento mais ágil e eficiente da IoT DB-Audit.

Durante o Teste de Integração, os diversos módulos da IoT DB-Audit foram testados em conjunto. Objetivando verificar a interação adequada entre esses elementos e se a integração entre eles está conforme o esperado [Sisinni 2021]. No Teste de Integração, foram identificados e corrigidos problemas de compatibilidade, comunicação e interação entre os módulos. Os resultados deste teste foram fundamentais para garantir a estabilidade e confiabilidade da abordagem IoT DB-Audit, ajudando a mitigar os riscos e problemas relacionados a possíveis falhas, e garantindo que ela atenda aos requisitos e expectativas estabelecidos durante o processo de desenvolvimento.

No Teste de Sistema, conduzido por pessoas não envolvidas diretamente no desenvolvimento, garantindo uma perspectiva imparcial e focada no usuário final, a IoT DB-Audit foi avaliada em sua totalidade, verificando-se sua conformidade com os requisitos estabelecidos [Aniche 2022]. Foram realizadas diversas atividades para validação do comportamento da IoT DB-Audit em cenários de uso real. Além disso, o Teste de Sistema teve em vista garantir que a IoT DB-Audit atenda às expectativas dos usuários finais, replicando suas experiências e identificando possíveis falhas ou inconsistências.

6.2. Avaliação junto a usuários do EXEHDA

Por sua vez, para avaliação junto aos usuários do EXEHDA foi utilizado o *Technology Acceptance Model* (TAM), um modelo, proposto por [Davis et al. 1989], específico para tecnologia da informação que tem uma forte base teórica. O modelo sugere que, quando usuários são apresentados a uma nova tecnologia, vários fatores influenciam sua decisão sobre como e quando eles a usarão, notadamente: (i) Utilidade percebida (*Perceived Usefulness* - PU) - é o grau em que uma pessoa acredita que usar uma determinada tecnologia aumentaria seu desempenho no trabalho; e (ii) Facilidade de uso percebida (*Perceived Ease of Use* - PEOU) - é o grau em que uma pessoa acredita que usar uma determinada tecnologia estaria livre de esforço. Desta forma, foi elaborado um questionário cujas questões estão mostradas na tabela 1, empregando a escala Likert: Discordo totalmente; Discordo parcialmente; Indiferente; Concordo parcialmente e Concordo totalmente.

É fundamental avaliar se o questionário utilizado na pesquisa consegue inferir ou medir aquilo a que realmente se propõe, justamente, para dar relevância à pesquisa. O Co-

Tabela 1. Questionário TAM Respondido Pelos Usuários do EXEHDA

Construto	Afirmativa
Facilidade de uso percebida	1 - Considero os alertas da IoT DB-Audit claros e objetivos.
	2 - A interação com a IoT DB-Audit se mostra facilitada pela estratégia de interfaceamento hierárquico empregado.
Utilidade Percebida	3 - Considero os dados disponibilizados pela IoT DB-Audit suficientes para a avaliação da compliance à LGPD.
	4 - A utilização da IoT DB-Audit contribuiu para a realização da análise dos *gaps* de segurança.
	5- O emprego da IoT DB-Audit aumentou a eficiência quanto a avaliação do tratamento dos dados pessoais, conforme preconiza a LGPD.
	6 - A utilização da IoT DB-Audit contribuiu para a aderência do EXEHDA à LGPD.

eficiente Alfa de Cronbach é uma medida bastante utilizada de confiabilidade (avaliação da consistência interna dos questionários) para um conjunto de indicadores de construto. O Coeficiente Alfa de Cronbach mede a correlação entre as respostas, considerando a análise do perfil das respostas dadas. É calculado a partir do somatório da variância dos itens individuais e da soma da variância de cada avaliador. Na literatura encontra-se que os valores aceitáveis de alfa, variam de 0,70 a 0,95. Baseado no valor obtido para o Alfa de Cronbach, superior a 0,7, podemos considerar que a avaliação feita pelos usuários do EXEHDA, seguindo a metodologia da proposta TAM, possui uma considerável confiabilidade, podendo ser entendida como um instrumento representativo da sua opinião.

7. Considerações Finais

Com a concepção da IoT DB-Audit se tornou possível a adequação do *middleware* EXEHDA à LGPD, mediante auditoria no seu RIC. Dentre os serviços providos pela IoT DB-Audit, temos o processamento desta auditoria propriamente dito, o envio de alertas, e a disponibilização de uma interface gráfica para gerenciamento dos eventos gerados pelas regras processadas pelo algoritmo Apriori.

Os resultados obtidos junto aos usuários na avaliação da Utilidade e Facilidade de Uso percebidas (TAM), mostram-se promissores e apontam para o prosseguimento das pesquisas da IoT DB-Audit. Na concepção da IoT DB-Audit está sendo explorada a arquitetura de software do EXEHDA, com objetivo de validação, porém a IoT DB-Audit tem potencial para ser utilizada em qualquer *middleware*, baseado em serviços, voltado a IoT, baseado em serviços.

Dentre os trabalhos futuros previstos tem-se de avaliar diferentes algoritmos de regras de associação, o desenvolvimento de uma interface para a gestão do tratamento dos dados pessoais e a construção de um aplicativo nativo para smartphones para visualização e gerenciamento dos eventos de segurança gerados pela IoT DB-Audit.

Referências

Abbass, W., Baina, A., and Bellafkih, M. (2020). Evaluation of security risks using apriori algorithm. In *Proceedings of the 13th International Conference on Intelligent Systems: Theories and Applications*, pages 1–6.

Aniche, M. (2022). *Effective Software Testing: A developer's guide*. Simon and Schuster.

Anwar, M. R., Panjaitan, R., and Supriati, R. (2021). Implementation of database auditing by synchronization dbms. *International Journal of Cyber and IT Service Management*, 1(2):197–205.

Badii, C., Bellini, P., Difino, A., and Nesi, P. (2020). Smart city iot platform respecting gdpr privacy and security aspects. *IEEE Access*, 8:23601–23623.

Buchgeher, G., Fischer, S., Moser, M., and Pichler, J. (2020). An early investigation of unit testing practices of component-based software systems. In *2020 IEEE Workshop on Validation, Analysis and Evolution of Software Tests (VST)*, pages 12–15. IEEE.

da República, P. (2018). Lei geral de proteção de dados pessoais. Último acesso 17 março 2023.

Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management science*, 35(8):982–1003.

de Oliveira, N. S., Gomes, M. A., Lopes, R., and Nobre, J. C. (2019). Segurança da informaçao para internet das coisas (iot): uma abordagem sobre a lei geral de proteçao de dados (lgpd). *Revista Eletrônica de Iniciação Científica em Computação*, 17(4).

Ghedin, W. (2022). Metodologia para cobertura e qualidade no processo de teste de software em nuvem para aplicações web.

Hipp, J., Güntzer, U., and Nakhaeizadeh, G. (2000). Algorithms for association rule mining—a general survey and comparison. *ACM sigkdd explorations newsletter*, 2(1):58–64.

Hon, W. K., Millard, C., and Singh, J. (2016). Twenty legal considerations for clouds of things. *Queen Mary School of Law Legal Studies Research Paper*, (216).

Kammüller, F., Ogunyanwo, O. O., and Probst, C. W. (2019). Designing data protection for gdpr compliance into iot healthcare systems. *arXiv preprint arXiv:1901.02426*.

Lee, Y. and Lee, G. Y. (2021). Security management suitable for lifecycle of personal information in multi-user iot environment. *Sensors*, 21(22):7592.

Lopes, J. L., Geyer, C. F. R., Barbosa, J. L., Pernas, A. M., and Yamin, A. C. (2014). A middleware architecture for dynamic adaptation in ubiquitous computing. *Journal of Universal Computer Science*, 20(9):1327–1351.

Pappachan, P., Yus, R., Mehrotra, S., and Freytag, J.-C. (2020). Sieve: A middleware approach to scalable access control for database management systems. *arXiv preprint arXiv:2004.07498*.

Pereira, I., Mendes, J., Viana, D., Rivero, L., Ferreira, W., and Soares, S. (2022). Extending an lgpd compliance inspection checklist to assess iot solutions: An initial proposal. In *Anais Estendidos do XIII Congresso Brasileiro de Software: Teoria e Prática*, pages 28–31. SBC.

Semantha, F. H., Azam, S., Shanmugam, B., and Yeo, K. C. (2023). Pbdinehr: A novel privacy by design developed framework using distributed data storage and sharing for secure and scalable electronic health records management. *Journal of Sensor and Actuator Networks*, 12(2):36.

Sisinni, S. (2021). *Verification of Software Integrity in Distributed Systems*. PhD thesis, Politecnico di Torino.

Souza, R., Lopes, J., Geyer, C., Cardozo, A., Yamin, A., and Barbosa, J. (2018). An architecture for iot management targeted to context awareness of ubiquitous applications. *Journal of Universal Computer Science*, 24(10):1452–1471.

Weber, R. H. (2010). Internet of things–new security and privacy challenges. *Computer law & security review*, 26(1):23–30.