INTERFACE TECNOLÓGICA

MONITORAMENTO PREDITIVO COM INTEGRAÇÃO DAS TECNOLOGIAS DE IA E IoT APLICADO À SEGURANÇA NAS UNIVERSIDADES

PREDICTIVE MONITORING WITH AI AND IoT APPLIED TO SECURITY IN UNIVERSITIES

Alex Feitoza Alves – alexfeitozaa96@gmail.com
Faculdade de Tecnologia do Estado de São Paulo – Praia Grande – SP – Brasil

Gustavo Ramos Guimaraes – gusramos.guima@gmail.com
Faculdade de Tecnologia do Estado de São Paulo – Praia Grande – SP – Brasil

Jônatas Cerqueira Dias – jonatasdias136@gmail.com
Faculdade de Tecnologia do Estado de São Paulo – Praia Grande – SP – Brasil

Jeferson Cerqueira Dias – jefersoncdias@hotmail.com
Fatec Itaquera do Estado de São Paulo – São Paulo – SP – Brasil

RESUMO

Este estudo investiga a aplicação conjunta de Inteligência Artificial (IA) e Internet das Coisas (IoT) no desenvolvimento de um sistema de monitoramento com análise preditiva para aprimorar a segurança nas universidades. O problema de pesquisa aborda a questão de como a integração dessas tecnologias pode contribuir para enfrentar os desafios de segurança enfrentados por essas instituições, como furtos, violência e acesso não autorizado. Este trabalho tem como objetivo propor a utilização de sensores e dispositivos IoT conectados para coleta de dados em tempo real, combinados com técnicas de IA para análise preditiva, visando identificar ameaças potenciais e prevenir incidentes de segurança. A metodologia adotada inclui uma abordagem exploratória aplicada, utilizando a plataforma Dimensions AI para a coleta de dados relevantes, com foco na análise qualitativa dos fenômenos observados. A revisão da literatura revelou que a integração de tecnologias como vigilância por vídeo, sensores IoT, aprendizado de máquina e análise preditiva pode proporcionar uma abordagem multifacetada para a segurança universitária. Essas tecnologias permitem a detecção precoce de anomalias, reconhecimento facial para controle de acesso, monitoramento de multidões e veículos, além da prevenção de acidentes. O aprendizado federado (FL) também se destaca como uma técnica promissora para aprimorar a segurança e a privacidade, permitindo o treinamento de modelos de IA sem a necessidade de compartilhar dados sensíveis. No entanto, a implementação desses sistemas enfrenta desafios relacionados à infraestrutura e expertise tecnológica. Conclui-se que, com planejamento adequado, colaboração institucional e a adoção de um modelo de referência, os sistemas de monitoramento com análise preditiva com IA e IoT representam uma solução viável e eficaz para enfrentar os problemas de segurança nas universidades, proporcionando um ambiente mais seguro e protegido para estudantes, professores e funcionários.

Palavras-chave: Inteligência Artificial. Internet das Coisas. Monitoramento com Análise Preditiva. Segurança Universitária. Tecnologia em Segurança.

ABSTRACT

This study investigates the joint application of Artificial Intelligence (AI) and the Internet of Things (IoT) in the development of a monitoring system with predictive analysis to enhance security in universities. The research problem addresses the question of how the integration of these technologies can contribute to addressing the security challenges faced by these institutions, such as theft, violence, and unauthorized access. This work aims to propose the use of connected IoT sensors and devices for real-time data collection, combined with AI techniques for predictive analysis, to identify potential threats and prevent security incidents. The adopted methodology includes an applied exploratory approach, using the Dimensions AI platform for the collection of relevant data, with a focus on qualitative analysis of the observed phenomena. The literature review revealed that the integration of technologies such as video surveillance, IoT sensors, machine learning, and predictive analysis can provide a multifaceted approach to university security. These technologies enable early detection of anomalies, facial recognition for access control, crowd and vehicle monitoring, and accident prevention. Federated Learning (FL) also stands out as a promising technique to enhance security and privacy, allowing the training of AI models without the need to share sensitive data. However, the implementation of these systems faces challenges related to infrastructure and technological expertise. It is concluded that, with proper planning, institutional collaboration, and the adoption of a reference model, monitoring systems with predictive analysis using AI and IoT represent a viable and effective solution to address security problems in universities, providing a safer and more protected environment for students, teachers, and staff.

Keywords: Artificial Intelligence. Internet of Things. Monitoring with Predictive Analysis. University Security. Security Technology.

1. INTRODUÇÃO

A segurança em universidades é um tema complexo e multifacetado, abrangendo uma ampla gama de desafios. Estudos como os de Regehr et al. (2017), Dlamini & Olanrewaju (2021) e Azevedo et al. (2022) evidenciam a necessidade de uma abordagem holística para a gestão da segurança em instituições de ensino superior. Além dos incidentes mais visíveis, como violência física e roubos, as universidades enfrentam desafios relacionados à saúde mental, bem-estar, cibersegurança e a própria percepção de segurança por parte dos estudantes. Azevedo et al. (2022), por exemplo, destacam a importância de compreender as percepções de (in)segurança dos estudantes para implementar medidas eficazes. Nesse contexto, a segurança

em universidades transcende a mera prevenção de incidentes, englobando a criação de ambientes que promovam a sensação de bem-estar e a proteção integral dos membros da comunidade universitária.

Tradicionalmente, medidas como vigilância e sistemas de alarme são adotadas para garantir a segurança em universidades. No entanto, a complexidade dos desafios atuais exige soluções mais sofisticadas. A integração de Inteligência Artificial (IA) e Internet das Coisas (IoT) em sistemas de monitoramento com análise preditiva emerge como uma abordagem promissora. A IoT, ao permitir a coleta de dados em tempo real, possibilita a identificação de padrões e anomalias através de algoritmos de aprendizado de máquina. Essa abordagem, como destacado por Ghadi et al. e Yang et al. (2023; 2023), permite a detecção antecipada de situações de risco, contribuindo para a prevenção de incidentes.

Além disso, técnicas como processamento de linguagem natural e visão computacional, exploradas por Yang et al. (2023), permitem analisar dados de diversas fontes, como câmeras e registros de acesso, proporcionando uma visão mais completa da situação e facilitando a identificação de ameaças potenciais.

A implementação dessas tecnologias, embora promissora, enfrenta desafios. Como apontam Fox e Burstein (2010), é fundamental basear as soluções em evidências e considerar as especificidades de cada instituição. Silva e Silva (2020) destacam a importância da segurança para a escolha do meio de transporte, reforçando a necessidade de ambientes seguros nas universidades. No contexto brasileiro, a implementação dessas tecnologias apresenta desafios específicos relacionados à infraestrutura e expertise.

Diante desse cenário, este estudo busca responder à seguinte questão: *Quais os principais desafios enfrentados na implementação de um sistema preditivo de segurança nas universidades por meio da integração das tecnologias de IA e IoT?*

O objetivo é identificar as principais barreiras para a adoção dessas tecnologias em instituições de ensino superior brasileiras e propor soluções práticas para superá-las. Ao compreender os desafios e as oportunidades, este estudo visa contribuir para a otimização da segurança nas universidades, proporcionando um ambiente mais seguro para estudantes, professores e funcionários.

Os resultados esperados incluem a identificação de melhores práticas para a implementação desses sistemas, a definição de um “roadmap” para a adoção gradual dessas

tecnologias e a avaliação dos benefícios associados. Além disso, a pesquisa poderá servir como referência para outras instituições de ensino superior que buscam implementar soluções semelhantes.

2. MATERIAIS E MÉTODOS

Com base nas características desta pesquisa, ela pode ser categorizada como pesquisa aplicada com ênfase exploratória. Essa pesquisa tem como objetivo resolver um problema real existente (GIL, 2002). A estratégia adotada incluiu duas abordagens principais: a) uma abordagem amplamente abstrata dos fenômenos da natureza e da sociedade, chamada de "Método de abordagem", e b) outra abordagem que esclarece os "Procedimentos técnicos" utilizados (LAKATOS; MARCONI, 2003).

Quanto ao método de abordagem para a formação das conclusões foi baseada em uma abordagem dedutiva, que começou com as observações e se apoiou no conhecimento prévio disponível na literatura. A abordagem adotada foi qualitativa, com foco na análise de conteúdo, buscando interpretar e analisar o fenômeno observado a partir dos dados coletados.

Quanto aos procedimentos técnicos a investigação envolveu um viés “comparativo”, conforme (LAKATOS; MARCONI, 2003), com a utilização da plataforma bibliográfica de pesquisa Dimensions AI[1], acessada por meio do portal de pesquisa. Essa plataforma representa uma solução de busca e descoberta que integra recursos de diversas instituições nacionais e internacionais. Dentro desse portal, é possível realizar pesquisas abrangentes em todas as coleções disponíveis. Os termos-chave selecionados para a pesquisa no mecanismo de busca desta ferramenta estão presentes no **Quadro 1**.

Quadro 1 – Lista de Descritores de Busca de Artigos na Plataforma Bibliográfica

Item	Descritores: Termos-chave de Busca	Operador Lógico
1	IoT OR "Internet of Things"	AND
2	AI OR “Artificial Intelligence”	AND
3	Security	AND
4	University	AND

Fonte: Elaborado pelos Autores

[1] O Dimensions é o maior banco de dados de informações de pesquisa do mundo, com o objetivo de enriquecer e vincular os dados com palavras-chave e conceitos, organizações, pesquisadores ou classificações baseadas em aprendizado de máquina. Isso reúne milhares de silos de dados em um conjunto de dados vinculados para exploração de material bibliográfico - https://www.dimensions.ai/dimensions-data/.

Os descritores apresentados acima foram selecionados após testes com outros termos-chave, visando obter os resultados mais relevantes para o trabalho de acordo com a plataforma de busca. Além disso, foram selecionados material dos últimos cinco anos e sem restrição da língua de escrita.

O portfólio de artigos resultante da plataforma bibliográfica será selecionado com base em critérios consistentes, como relevância, precisão e atualidade das informações. A análise abrangerá aspectos como metodologia, resultados, abordagem teórica e prática, bem como a contribuição para o campo. A qualidade e a originalidade do conteúdo também serão consideradas na seleção do material. Além disso, será dada especial atenção à pertinência dos artigos em relação ao tema central da pesquisa.

Para realizar uma segregação básica inicial, foram utilizadas técnicas de leitura exploratória e seletiva no material coletado. Em seguida, foi empregada a técnica de leitura analítica. Por fim, ocorreu a leitura interpretativa, que pode ou não ocorrer separadamente da leitura analítica, com o objetivo de estabelecer uma relação entre o conteúdo das fontes pesquisadas e outros conhecimentos (GIL, 2002).

3. REVISÃO DA LITERATURA

Esta revisão da literatura destaca os artigos aderentes ao objetivo deste estudo, provenientes da plataforma bibliográfica conforme o método proposto.

Quadro 2 – Lista de artigos selecionados para análise (Portfólio de Artigos)

ID	Título do Artigo	Referências
1	*Integration of Federated Learning with IoT for Smart Cities Applications, Challenges, and Solutions*	(**GHADI** et al., 2023)
2	*Computer Vision Technology for Monitoring of Indoor and Outdoor Environments and HVAC Equipment: A Review.*	(**YANG** et al., 2023)
3	*Artificial Intelligence-Powered Contactless Face Recognition Technique for Internet of Things Access for Smart Mobility.*	(**HIREMANI** et al., 2022)

Fonte: Elaborado pelos Autores

A integração de IA e IoT oferece um vasto potencial para transformar diversos setores. No entanto, a implementação em larga escala dessas tecnologias exige a consideração de desafios complexos, como a privacidade, a segurança e a interoperabilidade. As pesquisas apresentadas por Ghadi et al., Yang et al. e Hiremani et al. demonstram o avanço dessas tecnologias e suas aplicações em áreas como gestão urbana, monitoramento ambiental e sistemas de acesso. O **Quadro 3** e **4**, a seguir, apresentam os desafios identificados no uso destas tecnologias.

Quadro 3 – Desafios na implementação da segurança em universidades com Inteligência Artificial (IA)

Grupo de Desafios	Descrição
Reconhecimento Facial e *Deep Learning*	A IA é utilizada para implementar algoritmos de reconhecimento facial que aprendem e se adaptam a diferentes condições, aumentando a precisão e a confiabilidade do reconhecimento (HIREMANI et al., 2022). Desafios Identificados: **a) Variabilidade dos dados:** Fatores como iluminação, expressões faciais e ângulos de captura podem afetar a precisão dos algoritmos, exigindo técnicas de *deep learning* robustas para garantir resultados confiáveis Hiremani et al. (2022). **b) Privacidade:** A privacidade é uma preocupação central na implementação de sistemas de reconhecimento facial. Como apontam Ghadi et al. (2023), Hiremani et al. (2022) e Yang et al. (2023), a coleta e o armazenamento de dados biométricos sensíveis levantam questões éticas sobre vigilância e o uso indevido de informações pessoais. **c) Ética e viés algorítmico:** Além dos desafios técnicos, o reconhecimento facial suscita questões éticas importantes. Estudos demonstram que algoritmos de reconhecimento facial podem apresentar vieses em relação a gênero, raça e etnia (Buolamwini & Gebru, 2018). Garantir a imparcialidade e a equidade desses sistemas é fundamental para evitar a discriminação e a perpetuação de desigualdades.
Análise de Dados	Processamento e análise de grandes volumes de dados para identificar padrões e anomalias podem indicar problemas de segurança (YANG et al., 2023). Desafios Identificados: **a) Velocidade:** Os dados precisam ser processados rapidamente para que as ameaças possam ser detectadas e contidas a tempo. **b) Veracidade:** Nem todos os dados são confiáveis. Ruídos, erros e informações falsas podem complicar a análise. **c) Complexidade dos padrões:** Os padrões que indicam uma ameaça podem ser complexos e difíceis de identificar, especialmente em meio a uma grande quantidade de dados normais. **d) Evolução das ameaças:** Os atacantes estão sempre desenvolvendo novas técnicas. Os sistemas de detecção precisam se adaptar constantemente.
Detecção de Anomalias	Ghadi et al., 2023 tem foco mais centrado nas anomalias relacionadas à segurança e integridade dos dispositivos IoT, como acesso não autorizado e falhas específicas de hardware ou software. Enquanto que Yang et al., 2023 aborda um espectro mais amplo de anomalias como a aplicação de algoritmos de aprendizado de máquina para detectar comportamentos anômalos em ambientes monitorados, ajudando a prever e prevenir incidentes de segurança. Desafios Identificados: **a) O que é "normal"?:** Definir o que é um comportamento normal pode ser complexo, especialmente em ambientes dinâmicos e com grande volume de dados. O que é normal hoje pode não ser normal amanhã (YANG et al., 2023). **b) Novos tipos de ataques:** Os atacantes estão sempre desenvolvendo novas técnicas. Os sistemas de detecção precisam ser capazes de identificar ameaças desconhecidas (GHADI et al., 2023) e (YANG et al., 2023). **c) Falsos positivos:** É comum que os sistemas de detecção gerem alertas falsos, ou seja, identifiquem como anômalas atividades que são, na verdade, normais. Por outro lado, podem deixar passar atividades maliciosas sem serem detectadas (GHADI et al., 2023) e (YANG et al., 2023). **d) Volume de dados:** A quantidade de dados gerados por esses sistemas digitais é muito grande. Processar e analisar esses dados em tempo real é um grande desafio computacional (GHADI et al., 2023) e (YANG et al., 2023).

	e) Diversidade de dados: Os dispositivos IoT geram dados muito variados, desde imagens de câmeras até dados de sensores. Cada tipo de dado exige técnicas de análise diferentes (YANG et al., 2023) e (GHADI et al., 2023).
Automação de Respostas	Automação de respostas a eventos de segurança, como ajustes em sistemas de ventilação em resposta a mudanças na qualidade do ar (YANG et al., 2023). Desafios Identificados: **a) Complexidade dos sistemas:** Edifícios inteligentes são sistemas complexos com muitos componentes interconectados. Isolar a causa de uma anomalia pode ser difícil, bem como o fato de afetar outros sistemas (GHADI et al., 2023; YANG et al., 2023). **b) Variabilidade dos eventos:** Os eventos de segurança podem ser diversos e imprevisíveis. Um sistema de automação precisa ser capaz de lidar com uma ampla gama de situações. **c) Tempo de resposta:** A resposta a um evento de segurança precisa ser rápida para minimizar os riscos. Isso exige sistemas de comunicação eficientes e algoritmos de decisão rápidos. **d) Integração com outros sistemas:** Os sistemas de automação precisam ser integrados a outros sistemas, como sistemas de controle de acesso, sistemas de detecção de incêndio e sistemas de gerenciamento de energia.
Modelos de Aprendizado Federado	A IA permite o treinamento de modelos localmente em dispositivos IoT, protegendo a privacidade dos usuários e reduzindo a superfície de ataque ao evitar a transmissão de dados sensíveis pela rede (GHADI et al., 2023). Desafios Identificados: **a) Heterogeneidade de dispositivos*:** Dispositivos IoT podem ter diferentes capacidades de processamento, armazenamento e conectividade. [***Nível: Médio***] **b) Comunicação:** É necessário estabelecer um protocolo de comunicação eficiente e seguro para coordenar o treinamento dos modelos. **c) Privacidade:** Garantir a privacidade dos dados é um desafio constante, especialmente em ambientes distribuídos. **d) Eficiência:** O treinamento de modelos em dispositivos com recursos limitados pode ser computacionalmente caro. **e) Complexidade:** Coordenar o treinamento de um modelo distribuído em muitos dispositivos é um problema complexo com muitos desafios técnicos.

Observação: *A "Heterogeneidade de Dispositivos" foi considerada com um desafio de Nível: 2 - Médio*

Fonte: Elaborado pelos Autores

Quadro 4 – Desafios na implementação da segurança em universidades com Internet das Coisas (IoT)

Grupo de Desafios	Descrição
Monitoramento e Controle em Tempo Real**	A IoT permite que dispositivos interconectados monitorem e controlem o ambiente em tempo real, detectando atividades suspeitas e respondendo rapidamente a incidentes (HIREMANI et al., 2022) e (GHADI et al., 2023). Desafios Identificados: **a) Latência:** A necessidade de responder rapidamente a eventos em tempo real exige sistemas de comunicação com baixa latência. Qualquer atraso na comunicação pode comprometer a tomada de decisões em tempo real. **b) Complexidade:** Sistemas IoT são complexos e interconectados. Uma falha em um componente pode afetar todo o sistema.

Validação de Credenciais de Acesso	O módulo de gerenciamento de identidade e acesso (IAM) utiliza IoT para validar credenciais de acesso de forma segura, garantindo que apenas usuários autorizados tenham acesso (HIREMANI et al., 2022). Desafios Identificados: **a) Escala:** Em ambientes com muitos dispositivos IoT, a gestão de identidades e acesso se torna complexa. É preciso garantir que as credenciais sejam validadas de forma eficiente e segura para um grande número de usuários. **b) Heterogeneidade:** Dispositivos IoT são fabricados por diferentes fabricantes e podem utilizar protocolos de comunicação diferentes, o que dificulta a padronização dos processos de autenticação. **c) Ataques cibernéticos:** Sistemas de autenticação são alvos frequentes de ataques cibernéticos, como *phishing*, força bruta e ataques de *replay*.
Integração de Dados	Integração de dados de diferentes fontes, como sensores ambientais e sistemas de controle de edifícios, para uma análise abrangente da segurança (YANG et al., 2023) e (GHADI et al., 2023). Desafios Identificados: **a) Heterogeneidade dos dados:** A variedade proveniente de dados coletados por diferentes sensores e sistemas IoT podem ter formatos, unidades de medida e níveis de granularidade diferentes. Essa variedade de dispositivos e de protocolos de comunicação utilizados dificulta a criação de soluções de segurança padronizadas. **b) Qualidade dos dados:** A qualidade dos dados pode ser afetada por diversos fatores, como falhas nos sensores, interferências e erros de transmissão.
Coleta Contínua de Dados em Tempo Real	A IoT possibilita a coleta contínua de dados de sensores e dispositivos conectados, essencial para vigilância e monitoramento em tempo real, permitindo a identificação imediata de problemas ou comportamentos suspeitos (GHADI et al., 2023) e (HIREMANI et al., 2022). Desafios Identificados: **a) Volume de dados:** A quantidade de dados gerados por um grande número de sensores pode ser imensa, exigindo infraestruturas robustas de armazenamento e processamento. **b) Velocidade:** A necessidade de analisar os dados em tempo real impõe requisitos de processamento muito altos.
Implementação de Medidas de Segurança	Dispositivos IoT podem ser equipados com funcionalidades de segurança, como criptografia e autenticação, que protegem a comunicação entre dispositivos e servidores, mitigando riscos e protegendo dados sensíveis (GHADI et al., 2023). Desafios Identificados: **a) Limitações dos dispositivos:** Muitos dispositivos IoT possuem recursos computacionais limitados, o que dificulta a implementação de algoritmos de criptografia complexos e outros mecanismos de segurança. **b) Atualizações de segurança:** Manter os dispositivos IoT atualizados com as últimas correções de segurança é um desafio constante, especialmente em ambientes com um grande número de dispositivos.

Observação: *Os desafios indicados nos grupos de desafios não apresentaram desafios considerados como de Nível 4- Muito Alto.*

Fonte: Elaborado pelos Autores

4. RESULTADOS E DISCUSSÃO

As subseções a seguir realiza uma classificação dos desafios de segurança associados as tecnologias de IA e IoT no contexto de predição para o provimento da segurança nas instituições de ensino superior e universidades. Será considerado fatores como complexidade técnica,

tempo necessário para implementação, impacto na operação, riscos de segurança e disponibilidade de ferramentas e recursos. Essa classificação, conforme os **Quadros 3** e **4**, permitirá identificar as áreas que requerem maior atenção e propor estratégias para otimizar a implementação dessas tecnologias, na prevenção de incidentes e a minimização dos riscos para a organização.

Quadro 5 – Critérios utilizados para a classificação dos desafios de implementação tecnológica.

Critérios	Descrição
1. Impacto Potencial	Avalia o quanto o desafio pode afetar a segurança geral do campus.
2. Probabilidade de Ocorrência	Considera a frequência com que o desafio pode se manifestar ou se tornar um problema.
3. Dificuldade de Resolução	Refere-se à complexidade e aos recursos necessários para abordar e resolver o desafio.
4. Urgência	Avalia a necessidade imediata de ação em relação ao desafio, considerando a gravidade da situação.

Fonte: Elaborado pelos Autores

Com base nos critérios estabelecidos no **Quadro 3** foram identificados os níveis de classificação dos desafios de segurança, conforme o **Quadro 4**, a serem aplicados em universidades.

Quadro 6 – Desafios de implementação tecnológica.

Código	Classificação	Descrição
4	Muito Alto	Desafios com alto impacto, alta probabilidade de ocorrência, difícil resolução e urgência imediata. Exemplo: Baixa conscientização de segurança.
3	Alto	Desafios com impacto significativo, probabilidade considerável de ocorrência, dificuldade moderada de resolução e urgência. Exemplo: Ambiente complexo.
2	Médio	Desafios com impacto moderado, probabilidade média de ocorrência, resolução viável e alguma urgência. Exemplo: Falta de integração de novas tecnologias.
1	Baixo	Desafios com baixo impacto, baixa probabilidade de ocorrência, fácil resolução e baixa urgência. Exemplo: Recursos e suporte limitados (dependendo da situação específica).

Fonte: Elaborado pelos Autores

Quadro 7 – Proposta de solução para os desafios de Nível "4 – Muito Alto" na implementação da segurança em universidades com Inteligência Artificial (IA) e Internet das Coisas (IoT)

Grupo de Desafios	Desafios Classificados como Nível "4 – Muito Alto"	Proposta de Solução para os desafios de Nível "4 - Muito Alto"
Reconhecimento Facial e *Deep Learning*	▪ Privacidade	Algumas soluções podem ser consideradas: ▪ **Privacidade Diferencial:** (DWORK; ROTH, 2013) Essa técnica é útil para o reconhecimento facial, pois permite adicionar ruído aos dados de forma que seja difícil identificar um indivíduo específico, sem comprometer significativamente a precisão do modelo. No entanto, a aplicação da privacidade diferencial no aprendizado

Modelos de Aprendizado Federado		federado ainda é um campo de pesquisa ativo, e sua eficácia pode variar dependendo da arquitetura do sistema. ▪ **Aprendizado Federado:** Embora seja um desafio apresentado neste estudo é também a solução proposta (H. BRENDAN MCMAHAN, EIDER MOORE, DANIEL RAMAGE, SETH HAMPSON, 2017). É uma solução promissora para preservar a privacidade dos dados, especialmente no contexto do reconhecimento facial. Ao treinar modelos de *machine learning* nos próprios dispositivos dos usuários, em vez de centralizar os dados, é possível reduzir os riscos de vazamento de informações sensíveis.
Análise de Dados	▪ Complexidade dos padrões ▪ Evolução das ameaças*****	Duas técnicas são sugeridas para atuarem com ambos os desafios: **Redes Neurais Convolucionais (CNNs)** que são projetadas para trabalhar com dados que possuem uma estrutura espacial intrínseca, como imagens, vídeos e sinais de áudio e **Redes Neurais Recorrentes (RNNs)** são projetadas para trabalhar com dados que possuem uma ordem temporal, como séries temporais, texto e fala.
Detecção de Anomalias	▪ O que é "normal"? ▪ Novos tipos de ataques*****	É sugerido uma **definição dinâmica de "normal"**. E como a IA e a IoT poderiam contribuir para a solução? ▪ **Perfil comportamental**: Utilizando algoritmos de aprendizado de máquina, é possível criar perfis comportamentais para cada indivíduo ou grupo, considerando fatores como horários, locais frequentados e padrões de movimento. ▪ **Adaptação em tempo real**: Os modelos de IA podem se adaptar a mudanças nos padrões de comportamento, como eventos especiais ou feriados, ajustando a definição de "normal" em tempo real.
Automação de Respostas	▪ Complexidade dos sistemas	Uma possibilidade de solução para esta complexidade é a utilização de Gêmeos Digitais: ▪ **Representação virtual:** Criar uma representação digital detalhada do edifício, incluindo todos os seus componentes e suas interações. ▪ **Simulação:** Simular diferentes cenários e condições para testar hipóteses e identificar as causas potenciais de anomalias. ▪ **Otimização:** Utilizar o gêmeo digital para otimizar o desempenho do edifício e identificar oportunidades de melhoria.

***Observação:** a proposta de solução para os "Novos Tipos de Ataques" no grupo de desafios "Detecção de Anomalias" é a mesma descrita para "Evolução de Ameaças".*

Fonte: Elaborado pelos Autores

Os demais desafios foram classificados como "3 - Alto" e tendem a ser mais estáveis ou possuem soluções mais consolidadas, embora ainda representem obstáculos significativos.

5. CONSIDERAÇÕES FINAIS

A implementação de sistemas IoT aliado a IA em universidades, embora promissora, apresenta uma série de desafios que exigem soluções inovadoras. Ao longo deste trabalho,

explorou-se alguns dos principais desafios relacionados à segurança, integração de dados, coleta de dados em tempo real e implementação de medidas de segurança em dispositivos IoT e IA. Uma análise realizada pelos autores, nos grupos de desafios apresentadas no material bibliográfico estudado, sugeriu uma reclassificação em três categorias principais: a) Privacidade, b) Segurança e c) Interoperabilidade.

Essa reclassificação oferece uma estrutura mais clara e abrangente para analisar os desafios inerentes à implementação de sistemas IoT e IA em universidades. Além de facilitar a identificação de soluções específicas para cada categoria.

Quadro 8 – Reclassificação propostas de solução

Grupo de Desafios	
Segurança	A segurança é um dos maiores desafios na implementação de sistemas IoT. A heterogeneidade dos dispositivos, a complexidade das redes e a constante evolução das ameaças exigem uma abordagem multifacetada. A adoção de protocolos de criptografia robustos, a implementação de sistemas de detecção de intrusão e a atualização constante dos sistemas são medidas recomendadas para garantir a segurança dos dados.
Privacidade	A coleta e o armazenamento de grandes volumes de dados geram preocupações com a privacidade dos usuários. É fundamental garantir que os dados sejam coletados, armazenados e processados de forma ética e transparente, respeitando as leis de proteção de dados. A implementação de mecanismos de anonimização e a adoção de políticas de privacidade claras são medidas essenciais.
Interoperabilidade	A heterogeneidade dos dispositivos IoT dificulta a integração de dados e a criação de soluções padronizadas. A adoção de padrões abertos e a utilização de plataformas de integração de dados podem ajudar a superar esse desafio.

Fonte: Elaborado pelos Autores

Quadro 9 – Proposta de solução para os desafios de Nível "4 – Muito Alto" na implementação da segurança em universidades com Inteligência Artificial (IA) e Internet das Coisas (IoT)

Grupo de Desafios	
Privacidade	a) **Reconhecimento Facial e Deep Learning:** O uso de reconhecimento facial levanta preocupações significativas sobre a privacidade dos indivíduos, especialmente em ambientes universitários. A coleta e o armazenamento de dados biométricos exigem cuidados especiais para evitar o uso indevido dessas informações. b) **Modelos de Aprendizado Federado:** Embora o aprendizado federado seja uma abordagem promissora para proteger a privacidade dos dados, a implementação eficaz dessa técnica ainda enfrenta desafios, como a garantia da segurança dos modelos durante o treinamento e a avaliação.

Segurança	a) **Análise de Dados - Complexidade dos padrões:** A complexidade dos padrões de dados gerados por sistemas IoT e IA dificulta a identificação de ataques e anomalias, tornando os sistemas mais vulneráveis a exploração por agentes maliciosos. b) **Análise de Dados - Evolução das ameaças:** A constante evolução das ameaças cibernéticas exige que os sistemas de segurança sejam continuamente atualizados e adaptados, o que representa um desafio significativo. c) **Detecção de Anomalias - O que é "normal"?** Definir o que é considerado "normal" em um sistema complexo e dinâmico como um ambiente universitário é desafiador e fundamental para a detecção de anomalias. d) **Detecção de Anomalias** - Novos tipos de ataques: A emergência de novos tipos de ataques, como ataques adversariais e ataques baseados em *deepfakes*, exige o desenvolvimento de novas técnicas de detecção. e) **Automação de Respostas** - Complexidade dos sistemas: A automação de respostas em sistemas complexos pode levar a consequências inesperadas e indesejadas, exigindo um alto grau de confiabilidade e segurança nos sistemas automatizados.
Interoperabilidade	Nenhum dos desafios listados se encaixa diretamente na categoria de interoperabilidade. A interoperabilidade se refere à capacidade de diferentes sistemas e dispositivos se comunicarem e trocarem informações de forma eficaz. Os desafios listados estão mais relacionados à segurança, privacidade e complexidade dos dados.

Fonte: Elaborado pelos Autores

Como sugestões para trabalhos futuros é observada a necessidade da ampliação dessas propostas de solução ampliadas para os desafios de Nível 3 – Alto.

REFERÊNCIAS

AZEVEDO, V.; NUNES, L. M.; SANI, A. Is Campus a Place of (In)Security and Crime? Perceptions and Predictors among Higher Education Students. **European Journal of Investigation in Health, Psychology and Education**, v. 12, n. 2, p. 193–208, 2 fev. 2022.

CAPASSO DA SILVA, D.; RODRIGUES DA SILVA, A. N. Sustainable modes and violence: Perceived safety and exposure to crimes on trips to and from a Brazilian university campus. **Journal of Transport & Health**, v. 16, p. 100817, mar. 2020.

DLAMINI, N.; OLANREWAJU, O. A. **An Investigation into Campus Safety and Security**. Proceedings of the International Conference on Industrial Engineering and Operations Management. **Anais**...Michigan, USA: IEOM Society International, 7 mar. 2021. Disponível em: <https://index.ieomsociety.org/index.cfm/article/view/ID/620>

DWORK, C.; ROTH, A. The Algorithmic Foundations of Differential Privacy. **Foundations and Trends® in Theoretical Computer Science**, v. 9, n. 3–4, p. 211–407, 2013.

FOX, J. A.; BURSTEIN, H. **Violence and Security on Campus**. [s.l.] ABC-CLIO, LLC, 2010.

GHADI, Y. Y. et al. Integration of federated learning with IoT for smart cities applications, challenges, and solutions. **PeerJ Computer Science**, v. 9, p. 1–23, 2023.

H. BRENDAN MCMAHAN, EIDER MOORE, DANIEL RAMAGE, SETH HAMPSON, B. A. Y A. Communication-Efficient Learning of Deep Networks from Decentralized Data. **Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS) 2017**, v. 54, p. 10, 2017.

HIREMANI, N. et al. Artificial Intelligence-Powered Contactless Face Recognition Technique for Internet of Things Access for Smart Mobility. **Wireless Communications and Mobile Computing**, v. 2022, 2022.

REGEHR, C. et al. A comprehensive approach to managing threats of violence on a university or

college campus. **International Journal of Law and Psychiatry**, v. 54, p. 140–147, set. 2017.

YANG, B. et al. Computer Vision Technology for Monitoring of Indoor and Outdoor Environments and HVAC Equipment: A Review. **Sensors**, v. 23, n. 13, p. 1–42, 2023.

SILVA, D., & SILVA, A. (2020). Sustainable modes and violence: Perceived safety and exposure to crimes on trips to and from a Brazilian university campus. **Journal of transport and health**, 16, 100817-100817. https://doi.org/10.1016/j.jth.2019.100817.