UNIFEOB

CENTRO UNIVERSITÁRIO DA FUNDAÇÃO DE ENSINO OCTÁVIO BASTOS

ESCOLA DE NEGÓCIOS

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

PROJETO INTEGRADO

SISTEMA DE LOGIN COM RECONHECIMENTO DE PADRÕES

SÃO JOÃO DA BOA VISTA, SP

NOVEMBRO 2023

UNIFEOB

CENTRO UNIVERSITÁRIO DA FUNDAÇÃO DE ENSINO OCTÁVIO BASTOS

ESCOLA DE NEGÓCIOS

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

PROJETO INTEGRADO

SISTEMA DE LOGIN COM RECONHECIMENTO DE PADRÕES

MÓDULO - Inteligência Artificial

Inteligência Artificial – Prof. Rodrigo Marudi de Oliveira
Segurança em Sistema Computacionais - Prof. Nivaldo de Andrade

Estudantes:
Eduardo Coelho, RA 1012022100885

SÃO JOÃO DA BOA VISTA, SP

NOVEMBRO, 2023

Sumário

1 INTRODUÇÃO

No mundo digital contemporâneo, a segurança e a praticidade são elementos fundamentais na interação entre usuários e sistemas. Nesse contexto, a autenticação por meio de login é uma prática onipresente, porém, muitas vezes, torna-se suscetível a vulnerabilidades de segurança ou é percebida como uma barreira à experiência do usuário. Diante desse cenário, surge a necessidade de explorar soluções inovadoras que garantam a segurança dos dados e, ao mesmo tempo, ofereçam uma experiência de uso fluida e intuitiva.

Este projeto propõe o desenvolvimento de um Sistema de Login com Reconhecimento de Padrões, uma abordagem que visa unir a segurança da autenticação biométrica com a praticidade do reconhecimento de padrões visuais ou gestuais. Essa combinação busca superar as limitações dos métodos tradicionais de login, oferecendo uma alternativa eficiente, segura e amigável para os usuários.

2 DESCRIÇÃO DA EMPRESA

A empresa "TechGuard Solutions" é uma renomada fornecedora global de soluções de segurança cibernética e desenvolvimento de softwares. Reconhecida por sua expertise em proteção de dados e inovação tecnológica, a TechGuard Solutions atende a uma ampla gama de clientes corporativos, governamentais e institucionais em todo o mundo.

Com um compromisso contínuo com a segurança e a inovação, a empresa está buscando aprimorar a autenticação de seus sistemas, visando melhorar a experiência do usuário e reforçar a segurança dos dados. Em sua constante busca por soluções avançadas, a TechGuard Solutions decidiu implementar um Sistema de Login com Reconhecimento de Padrões.

3 PROJETO DE CONSULTORIA EMPRESARIAL

A TechGuard Solutions foi fundada em 2005 por um grupo de especialistas em segurança cibernética, com a missão de fornecer soluções inovadoras para proteger ativos digitais contra ameaças cibernéticas. Desde então, a empresa tem se destacado como uma líder em segurança da informação, oferecendo serviços de consultoria, desenvolvimento de software e soluções personalizadas para empresas de diversos setores.

3.0. RAMO DE ATUAÇÃO, MISSÃO, VISÃO E VALORES

Ramo de Atuação: A TechGuard Solutions atua no setor de segurança cibernética, oferecendo serviços de consultoria em segurança da informação, soluções de proteção de dados, desenvolvimento de software seguro e treinamento em cibersegurança para organizações de diferentes portes e segmentos.

Missão: Nossa missão é fornecer soluções inovadoras e eficazes para proteger os ativos digitais de nossos clientes contra ameaças cibernéticas, garantindo segurança, confiabilidade e conformidade.

Visão: Buscamos ser reconhecidos como um provedor líder em soluções de segurança cibernética, impulsionando a inovação e oferecendo proteção abrangente para os ambientes digitais de nossos clientes.

Valores: Compromisso com a segurança, inovação contínua, ética, transparência e excelência no atendimento ao cliente.

3.0.2 DESAFIOS ENFRENTADOS PELA EMPRESA E BUSCA PELA CONSULTORIA:

A TechGuard Solutions enfrenta constantemente desafios relacionados à evolução rápida e constante das ameaças cibernéticas. Com o aumento da sofisticação dos ataques, a empresa percebeu a necessidade de aprimorar ainda mais suas defesas para proteger não apenas os dados de seus clientes, mas também sua própria infraestrutura.

Os desafios específicos incluem:

Aumento da complexidade das ameaças: O cenário de ameaças cibernéticas está em constante evolução, com ataques cada vez mais sofisticados, incluindo ameaças baseadas em inteligência artificial. Isso demanda a adoção de abordagens avançadas de segurança.

Maior volume de dados: Com o crescente volume de dados, proteger essas informações tornou-se uma tarefa desafiadora, exigindo soluções eficazes de gerenciamento e proteção de dados sensíveis.

Necessidade de modernização da infraestrutura de TI: A empresa reconhece a importância de modernizar sua infraestrutura de TI, integrando tecnologias de inteligência artificial para fortalecer suas defesas e aprimorar a eficiência operacional.

Diante desses desafios, a TechGuard Solutions buscou consultoria especializada em inteligência artificial e segurança em sistemas computacionais para aprimorar sua infraestrutura de TI, adotar soluções mais avançadas de segurança e garantir a proteção contínua de seus dados e dos dados de seus clientes contra ameaças cada vez mais sofisticadas.

3.1 INTELIGÊNCIA ARTIFICIAL

A Inteligência Artificial (IA) é um ramo da ciência da computação que se concentra no desenvolvimento de sistemas capazes de realizar tarefas que normalmente requerem inteligência humana. Ela envolve o uso de algoritmos e técnicas avançadas para permitir que máquinas e sistemas aprendam, raciocinem, tomem decisões, reconheçam padrões e resolvam problemas de maneira autônoma.

A relevância da Inteligência Artificial na atualidade é imensa, sendo uma das áreas de maior crescimento e impacto em diversos setores. Ela desempenha um papel fundamental em avanços tecnológicos significativos, desde assistentes virtuais em dispositivos móveis até sistemas complexos de análise de dados em empresas, medicina, automação industrial, carros autônomos, entre outros.

Integrar a Inteligência Artificial no contexto do projeto de um Sistema de Login com Reconhecimento de Padrões é essencial por diversas razões:

Capacidade de Reconhecimento de Padrões: A IA é crucial para o reconhecimento e análise de padrões visuais ou gestuais, permitindo a identificação precisa dos usuários por meio de técnicas avançadas de processamento de imagem ou análise de dados.

Aprimoramento da Segurança: Algoritmos de IA podem fortalecer a segurança do sistema, identificando comportamentos suspeitos ou tentativas de acesso não autorizado por meio da análise contínua de padrões de autenticação.

Melhoria da Experiência do Usuário: A IA pode adaptar-se às preferências individuais dos usuários, tornando o processo de autenticação mais intuitivo e personalizado, oferecendo uma experiência de login mais rápida e conveniente.

Detecção de Anomalias e Fraudes: Através de modelos de IA, é possível detectar padrões anômalos de comportamento que possam indicar tentativas de fraude ou atividades maliciosas.

Aprendizado Contínuo: Sistemas baseados em IA têm a capacidade de aprender e aprimorar suas habilidades ao longo do tempo, adaptando-se a novos padrões de autenticação e aprimorando a precisão do reconhecimento.

Em resumo, integrar a Inteligência Artificial no contexto do Sistema de Login com Reconhecimento de Padrões permite não apenas aumentar a segurança do sistema, mas também aprimorar a usabilidade e a eficiência, oferecendo uma solução mais inteligente, adaptável e confiável para autenticação de usuários.

3.1.1 INTRODUÇÃO À APLICAÇÃO DA IA

Um exemplo prático e impactante da aplicação da Inteligência Artificial no mundo real é a utilização de sistemas de reconhecimento facial em segurança e vigilância.

Grandes cidades ao redor do mundo têm adotado sistemas de câmeras de vigilância equipadas com algoritmos de IA para reconhecimento facial, a fim de fortalecer a segurança pública, identificar criminosos procurados e garantir a segurança em locais de grande fluxo de pessoas, como aeroportos, estações de metrô, eventos esportivos e áreas urbanas movimentadas.

Por exemplo, a cidade de Pequim, na China, implementou extensivamente sistemas de reconhecimento facial para monitoramento e segurança. Com uma vasta rede de câmeras equipadas com IA, o sistema é capaz de identificar e rastrear indivíduos em tempo real, ajudando na localização de pessoas desaparecidas, detectando comportamentos suspeitos e até mesmo auxiliando na captura de criminosos.

Outro exemplo é o uso de reconhecimento facial em aeroportos ao redor do mundo. Esses sistemas de IA são empregados para identificar passageiros nos pontos de controle de segurança e nos balcões de embarque, agilizando o processo de verificação de identidade e melhorando a segurança, ao mesmo tempo em que reduzem filas e aumentam a eficiência.

Esses sistemas de reconhecimento facial utilizam algoritmos de aprendizado de máquina para analisar e identificar padrões únicos no rosto das pessoas, como características faciais, formato dos olhos, nariz e boca, para criar modelos precisos de identificação. Com a capacidade de processar grandes volumes de dados em tempo real, esses sistemas conseguem realizar comparações rápidas e precisas, permitindo a identificação de indivíduos de interesse em questão de segundos.

Este exemplo ilustra como a Inteligência Artificial, em particular o reconhecimento facial, tem sido aplicada de forma prática e tangível no mundo real, demonstrando sua viabilidade, eficácia e utilidade em melhorar a segurança e otimizar processos em ambientes do cotidiano.

3.1.2 IMPLEMENTAÇÃO E TÉCNICAS ULTILIZADAS

Alguns detalhes das técnicas específicas de Inteligência Artificial mencionadas e as ferramentas comuns associadas a elas, destacando sua relevância para o projeto de um Sistema de Login com Reconhecimento de Padrões.

Redes Neurais Convolucionais (CNNs):

- As Redes Neurais Convolucionais são amplamente usadas em reconhecimento de padrões visuais, como reconhecimento facial. Essas redes são projetadas para processar dados de imagem, aplicando camadas de convolução que extraem características relevantes das imagens. Aprofundando as análises em diferentes camadas, as CNNs são capazes de identificar padrões complexos.

Redes Multicamada (MLPs - Multi-Layer Perceptrons):

- As Redes Multicamada (MLPs) são redes neurais artificiais compostas por várias camadas de neurônios interconectados. Cada neurônio em uma camada está conectado a todos os neurônios na camada seguinte, permitindo a aprendizagem de representações complexas dos dados.

Perceptrons:

- Os Perceptrons são uma forma básica de neurônios artificiais que realizam uma soma ponderada das entradas, seguida de uma função de ativação. Embora sejam o conceito fundamental dos neurônios, geralmente são utilizados em redes mais complexas, como as MLPs.

Ferramentas e Linguagens:

Teachable Machine do Google: Uma ferramenta que permite treinar modelos de aprendizado de máquina com facilidade, sem exigir experiência em programação. Ela utiliza técnicas de aprendizado de máquina para reconhecimento de imagem, áudio e gestos.

Python: Uma linguagem de programação comumente utilizada em projetos de IA devido à sua ampla gama de bibliotecas especializadas, como TensorFlow, Keras e PyTorch, que facilitam o desenvolvimento e implementação de modelos de redes neurais.

Estruturas de Dados em Python: Bibliotecas como NumPy e Pandas são usadas para manipular e processar dados, enquanto Matplotlib e Seaborn são usadas para visualização, todas fundamentais no pré-processamento e análise de dados para treinamento de modelos de IA.

A relevância da Inteligência Artificial para o projeto do Sistema de Login com Reconhecimento de Padrões é significativa. As técnicas mencionadas, como Redes Neurais Convolucionais e Redes Multicamada, são essenciais para o reconhecimento e validação de padrões biométricos, fornecendo a base para a identificação precisa dos usuários.

As ferramentas como a Teachable Machine do Google e linguagens como Python com suas bibliotecas especializadas proporcionam uma infraestrutura sólida para desenvolver e implementar modelos de IA, facilitando a criação de algoritmos avançados para reconhecimento de padrões no sistema de autenticação.

Dessa forma, a utilização de técnicas de Inteligência Artificial é fundamental para aprimorar a segurança e a usabilidade do sistema, permitindo uma autenticação biométrica eficaz, precisa e adaptável, além de promover uma experiência de login mais intuitiva para os usuários.

3.2 SEGURANÇA EM SISTEMAS COMPUTACIONAIS

A importância da segurança em sistemas computacionais é fundamental devido à natureza cada vez mais interconectada e digitalizada do mundo moderno. A dependência crescente de sistemas computacionais em praticamente todos os aspectos da vida, desde transações financeiras até dados pessoais, torna a segurança uma preocupação central.

Proteção de Dados Sensíveis:

Os sistemas computacionais armazenam uma quantidade imensa de dados sensíveis, como informações pessoais, financeiras, médicas e comerciais. Garantir a segurança desses dados é essencial para proteger a privacidade dos indivíduos e prevenir o uso indevido de informações confidenciais.

Prevenção contra Ameaças Cibernéticas:

Ameaças cibernéticas, como malware, phishing, ataques de negação de serviço (DDoS) e ransomware, representam uma ameaça constante aos sistemas computacionais. Investir em medidas de segurança robustas é crucial para mitigar essas ameaças e proteger contra perdas financeiras, interrupções de serviços e danos à reputação.

Confidencialidade e Integridade dos Dados:

A garantia de confidencialidade e integridade dos dados é essencial para assegurar que informações críticas não sejam acessadas por pessoas não autorizadas e que os dados não sejam alterados indevidamente, mantendo sua precisão e valor.

Garantia da Continuidade dos Negócios:

A interrupção dos sistemas computacionais devido a violações de segurança pode ter impactos severos nos negócios, resultando em perda de receita, interrupção de serviços essenciais e danos à reputação da empresa. A implementação de medidas de segurança adequadas é essencial para garantir a continuidade operacional.

Conformidade com Regulamentações e Leis de Proteção de Dados:

Diversas regulamentações, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil, impõem requisitos rigorosos para proteger a privacidade e a segurança dos dados. As organizações devem cumprir essas regulamentações para evitar penalidades legais e proteger a confiança dos clientes.

Em um Sistema de Login com Reconhecimento de Padrões, a segurança é crucial para proteger a identidade dos usuários. A integração de técnicas de Inteligência Artificial visa reforçar essa segurança, permitindo a identificação biométrica precisa e dificultando a possibilidade de acesso não autorizado. Garantir a segurança nesse contexto não apenas protege as informações dos usuários, mas também fortalece a confiança no sistema, essencial para sua aceitação e utilização contínua.

3.2.1 CONCEITOS E IMPLEMENTAÇÕES DE SEGURANÇA

Conceitos de Segurança Lógica e Física:

Segurança Lógica: Refere-se à proteção de dados e informações por meio de mecanismos digitais, como firewalls, criptografia, controles de acesso e políticas de segurança. Envolve salvaguardar os dados contra acessos não autorizados, alterações indevidas, roubo ou qualquer tipo de manipulação por meio de medidas e controles digitais.

Segurança Física: Trata da proteção dos ativos físicos de uma organização, incluindo instalações, equipamentos de hardware, servidores e dispositivos de armazenamento. Envolve medidas como restrições de acesso físico, vigilância por vídeo, sistemas de alarme e proteções contra desastres naturais ou provocados pelo homem.

Conceito e Valor da Informação:

Conceito de Informação: Refere-se a dados organizados e processados que têm significado e valor para um indivíduo, organização ou sistema. A informação é essencial para tomar decisões, realizar operações e executar processos.

Valor da Informação: O valor da informação está associado à sua relevância, precisão, integridade, disponibilidade e confidencialidade. A informação é considerada valiosa quando é precisa, confiável, oportuna e protegida contra acessos não autorizados, permitindo que os usuários tomem decisões informadas e obtenham vantagens competitivas.

Estes conceitos são fundamentais para compreender a importância de proteger não apenas os ativos físicos de uma organização, mas também as informações que residem nesses ativos. A segurança lógica e física são interdependentes e complementares, trabalhando juntas para proteger a integridade, confidencialidade e disponibilidade das informações, garantindo que elas permaneçam acessíveis apenas para aqueles que têm permissão e autorização para utilizá-las.

3.2.2 DETECÇÃO E PREVENÇÃO DE ATAQUES

As medidas proativas e reativas adotadas por uma empresa para garantir a segurança dos seus sistemas podem ser variadas e devem ser parte de uma estratégia abrangente de segurança cibernética. Aqui estão algumas das principais estratégias, métodos e ferramentas utilizados para identificar possíveis ameaças:

Medidas Proativas:

Auditorias de Segurança: Realização de auditorias regulares para avaliar a infraestrutura de segurança, identificar vulnerabilidades e garantir conformidade com as políticas de segurança.

Monitoramento de Rede: Implementação de ferramentas de monitoramento de rede para detectar atividades suspeitas, tráfego incomum ou tentativas de intrusão nos sistemas.

Testes de Penetração (Pen Testing): Realização de testes de penetração regulares para simular ataques cibernéticos e identificar vulnerabilidades que possam ser exploradas por hackers.

Atualizações e Patches de Segurança: Aplicação regular de atualizações e patches de segurança nos sistemas e softwares para corrigir falhas conhecidas e vulnerabilidades.

Conscientização e Treinamento dos Funcionários: Realização de programas de treinamento para funcionários visando a conscientização sobre boas práticas de segurança, incluindo identificação de phishing e práticas seguras de uso de sistemas.

Medidas Reativas:

Sistemas de Detecção de Intrusão (IDS) e Prevenção de Intrusão (IPS): Implementação de sistemas que identificam e respondem a possíveis intrusões na rede, alertando e bloqueando atividades suspeitas.

Análise de Incidentes de Segurança: Realização de investigações detalhadas após incidentes de segurança para identificar a origem, escopo e impacto do incidente e tomar medidas corretivas.

Resposta a Incidentes: Desenvolvimento de planos de resposta a incidentes para lidar com violações de segurança, incluindo procedimentos de contenção, recuperação e comunicação.

Monitoramento de Logs e Registros de Segurança: Análise constante de logs e registros de segurança para identificar padrões incomuns que possam indicar uma ameaça ou atividade maliciosa.

Análise de Malware e Antivírus: Utilização de softwares de análise de malware e antivírus para identificar e mitigar ameaças de software malicioso.

Essas medidas, quando implementadas de maneira integrada e contínua, ajudam a garantir que uma empresa possa identificar possíveis ameaças à segurança de seus sistemas, respondendo de forma proativa e reativa para mitigar riscos e proteger seus ativos e informações críticas.

4 CONCLUSÃO

Ao longo deste trabalho, foi possível explorar e analisar profundamente as estratégias e medidas de segurança em sistemas computacionais, com foco na aplicação de um Sistema de Login com Reconhecimento de Padrões. Identificamos a importância crucial da segurança lógica e física, assim como a relevância da Inteligência Artificial (IA) para aprimorar a autenticação biométrica, garantindo segurança e usabilidade. As descobertas revelaram que a integração de técnicas avançadas de IA, como Redes Neurais Convolucionais, juntamente com estratégias proativas e reativas de segurança, são essenciais para identificar ameaças, proteger dados sensíveis e garantir a confiabilidade dos sistemas. A importância de tomar decisões estratégicas informadas em TI tornou-se evidente, considerando não apenas os aspectos técnicos, como a implementação de tecnologias de IA e segurança, mas também os aspectos administrativos, como políticas de segurança, treinamento de funcionários e planos de resposta a incidentes. A combinação desses elementos é essencial para mitigar riscos e manter a integridade dos sistemas. Portanto, a implementação bem-sucedida desse Sistema de Login com Reconhecimento de Padrões representa não apenas uma atualização tecnológica, mas também uma mudança estratégica significativa, permitindo a empresa "TechGuard Solutions" mitigar riscos, melhorar a eficiência e assegurar um futuro mais seguro e confiável em seus processos e operações.

REFERÊNCIAS

https://brasilescola.uol.com.br/informatica/inteligencia-artificial.htm#:~:text=A%20Intelig%C3%AAncia%20artificial%20atua%20na,tarefas%20realizadas%20pelos%20seres%20humanos

https://www.deeplearningbook.com.br/introducao-as-redes-neurais-convolucionais/

https://medium.com/ensina-ai/rede-neural-perceptron-multicamadas-f9de8471f1a9

https://www.controle.net/faq/ciberseguranca-a-seguranca-da-informacao-em-sistemas-computacionais