CENTRO UNIVERSITÁRIO UNIFACVEST
CURSO DE CIÊNCIA DA COMPUTAÇÃO
ALISSON VIEIRA DE SOUZA

HEALTH CHAT: SISTEMA WEB VOLTADO PARA SEGURANÇA NA COMUNICAÇÃO DIGITAL PARA HOSPITAIS

LAGES
2024

ALISSON VIEIRA DE SOUZA

HEALTH CHAT: SISTEMA WEB VOLTADO PARA SEGURANÇA NA COMUNICAÇÃO DIGITAL PARA HOSPITAIS

Trabalho de conclusão de curso apresentado ao Centro Universitário UNIFACVEST como parte dos requisitos para a obtenção do grau de Bacharel em Ciência da Computação.

Aluno: Alisson Vieira de Souza
Orientador: Prof. Cassandro Albino Devenz
Orientador: Prof. Willen Leolatto Carneiro
Orientador: Prof. Igor Muzeka

LAGES
2024

ALISSON VIEIRA DE SOUZA

HEALTH CHAT: SISTEMA WEB VOLTADO PARA SEGURANÇA NA COMUNICAÇÃO DIGITAL PARA HOSPITAIS

Trabalho de conclusão de curso apresentado ao Centro Universitário UNIFACVEST como parte dos requisitos para a obtenção do grau de Bacharel em Ciência da Computação.

Aluno: Alisson Vieira de Souza
Orientador: Prof. Cassandro Albino Devenz
Orientador: Prof. Willen Leolatto Carneiro
Orientador: Prof. Igor Muzeka

Lages, SC ___/___/2024. Nota _____ _____

(Data de aprovação) (Assinatura do orientador do trabalho)

_____

(Coordenador do curso de graduação, nome e assinatura)

LAGES

2024

HEALTH CHAT: SISTEMA WEB VOLTADO PARA SEGURANÇA NA COMUNICAÇÃO DIGITAL PARA HOSPITAIS

RESUMO

O sistema desenvolvido tem como objetivo garantir a troca de mensagens e arquivos entre profissionais de saúde, o objetivo deste trabalho é apresentar um serviço de troca de mensagens e arquivos em tempo real, para meios hospitalares, utilizando como diferencial a criptografia. Este estudo baseia-se em uma metodologia bibliográfica e de cunho tecnológico aplicado referente a criptografia. Os resultados incluem a melhoria significativa da segurança das comunicações via web em hospitais, a facilitação da usabilidade do sistema pelos usuários, juntamente com a contribuição para a pesquisa acadêmica em segurança da informação. A implementação de ferramentas *open source* demonstra viabilidade econômica e eficiência, além de promover a conformidade com regulamentos de proteção de dados.

Palavras-chave: Sistemas, Web Segurança em Comunicação, Comunicação digital em Hospitais.

HEALTH CHAT: A CASE STUDY ON SECURITY IN DIGITAL COMMUNICATION FOR HOSPITALS

ABSTRACT

The system developed aims to guarantee the exchange of messages and files between healthcare professionals. The aim of this work is to present a service for exchanging messages and files in real time, for hospital environments, using cryptography as a differential. This study is based on a bibliographic methodology and applied technology, referring to cryptography. The results include a significant improvement in the security of web communications in hospitals, facilitating the usability of the system by users, as well as contributing to academic research into information security. The implementation of open source tools demonstrates economic viability and efficiency, as well as promoting compliance with data protection regulations.

Keywords: Systems, Web Security in Communication, Digital Communication in Hospitals.

1 INTRODUÇÃO

O tema da pesquisa aborda a importância da segurança da informação em aplicativos de mensagens, com foco no desenvolvimento do "Health Chat", um aplicativo que busca proteger dados sensíveis trocados em ambientes digitais, especialmente em setores críticos como o de saúde. A presente pesquisa foi realizada com o objetivo de implementar mecanismos de criptografia como estratégia central para prevenir acessos não autorizados e mitigar riscos de ataques cibernéticos em ambientes hospitalares.

O propósito da pesquisa é explorar soluções de segurança para comunicações eletrônicas, com ênfase em dados de saúde. A criação do Health Chat visa assegurar um canal de mensagens seguro e eficaz, aproveitando o poder da criptografia para garantir a privacidade das informações.

O estudo possui relevância significativa diante do crescente número de ataques cibernéticos direcionados a aplicativos de mensagens, evidenciando a necessidade de proteger dados pessoais e médicos de maneira eficaz. A pesquisa visa contribuir teoricamente para o avanço do conhecimento em criptografia e segurança da informação, enquanto propõe uma aplicação prática voltada ao setor de saúde. Nesse contexto, destaca-se a importância do sigilo e da proteção de dados para preservar a confiança entre pacientes e profissionais, além de considerar a viabilidade econômica como um fator essencial para sua implementação.

A aquisição de software open source costuma ser bastante barata ou gratuita, pois geralmente é possível baixar esses softwares sem custos. No entanto, se você precisar de documentação e suporte, você pode ter de pagar por isso, embora os custos sejam usualmente bastante baixos. O outro benefício-chave do uso de produtos open source é que sistemas open source maduros geralmente são muito confiáveis. Richard Stallman (2007)

A linguagem de programação TypeScript é muito popular entre os programadores devido a sua rica oferta de ferramentas, ambientes de desenvolvimento e documentação clara e abrangente. Embora seja acessível para usuários de diversos níveis de habilidade, é necessária uma compreensão básica de programação de programação para tirar o máximo proveito de suas funcionalidades (Dan Vanderkam, 2019)

O software de código aberto possui benefícios consideráveis que o colocam como uma opção viável no avanço tecnológico. A aquisição desses sistemas costuma ser gratuita ou de custo reduzido, proporcionando maior acessibilidade para programadores e organizações.

> A razão para isso é que eles têm uma grande população de usuários dispostos a corrigir os problemas em vez de os reportar ao desenvolvedor e esperar por novos release do sistema. Os bugs são descobertos e recuperados mais rapidamente do que é possível, em geral, com softwares proprietários. (Sommerville, 2011 p. 139)

O autor reitera a importância do desenvolvimento de sistemas com construção *open source* visando à viabilidade econômica, e a maneira de realizar correções embora também a comunidade de usuários, que, em vez de apenas reportam os problemas aos desenvolvedores e aguardarem atualizações, atuam ativamente na identificação e resolução dos bugs.

Hansen et al. (2016) enfatizam que o uso de ferramentas *open source* para criação não apenas reduz os custos, mas também oferece mais transparência e flexibilidade, permitindo que as organizações personalizem as soluções de acordo com suas necessidades. Além disso, o amplo grupo de pessoas que usam e desenvolvem essas ferramentas ajuda a identificar e corrigir rapidamente os problemas, melhorando continuamente a segurança.

> Deve-se implementar autenticação com múltiplos fatores (MFA, também chamado de 2FA) nos equipamentos e escolher serviços on-line que permitam o uso de MFA/2FA. Como visto, grande parte dos ataques reportados ao CERT.br nos últimos 5 anos envolviam ou furto de senhas ou adivinhação de senhas. Esses ataques incluíam, entre outros, senhas de acesso a: serviços de nuvem, back-end de lojas virtuais, contas de e-mail, servidores locais nas empresas, desktops, dispositivos como câmeras e discos externos, credenciais de serviços on-line e contas de redes sociais
> (ALEXANDRE F, BARBOSA, 2020, p.123)

A implementação de múltiplos fatores de autenticação (MFA) como afirma o autor oferece uma proteção mais robusta ao exigir que o usuário forneça informações adicionais além da senha, como um código temporário. Com isso, mesmo que um atacante tenha acesso à senha, ele ainda precisaria de mais uma verificação para conseguir acessar a conta ou o sistema.

1.1 OBJETIVOS GERAL

Desenvolver um sistema web de trocas de mensagens e arquivos, utilizando chaves de criptografia, destinadas a hospitais.

1.2 OBJETIVO ESPECÍFICOS

- 2.1.1 Melhorar a segurança e a privacidade de comunicações eletrônicas em hospitais por meio de chaves de criptografia pública e privada.
- 2.1.2 Garantir a confidencialidade e a integridade das mensagens enviadas e recebidas em hospitais.
- 2.1.3 Contribuir para que os serviços de mensagens nos hospitais possam funcionar de forma segura.

2 REFERENCIAL TEÓRICO

Em seu estudo sobre a história da criptografia, Kahn (1967) observou que, ao longo da história, codificar mensagens confidenciais tem sido crucial para estratégias militares,

diplomáticas e de inteligência, isso permite que países e organizações protejam seus segredos e comunicações estratégicas contra ameaças e ataques cibernéticos, essa ligação histórica, enfatiza o papel persistente da criptografia como uma ferramenta essencial para garantir a segurança da informação nos tempos modernos.

> A mensagem original, antes de ser transformada, é chamada de texto claro. Após transformada, ela é denominada simplesmente texto cifrado. Um algoritmo de criptografia transforma o texto claro em texto cifrado; um algoritmo de decriptografia transforma o texto cifrado de volta para texto claro. O emissor usa um algoritmo de criptografia e o receptor utiliza um algoritmo de decriptografia. (FOROUZAN, BEHROUZ A., A, 2008, p. 932).

Na comunicação segura, o emissor emprega a criptografia para assegurar a privacidade da mensagem, enquanto o receptor executa a decriptografia para recuperar o conteúdo original, este procedimento destaca a relevância dos algoritmos criptográficos no cenário de proteção de dados.

2.1 SEGURANÇA NA COMUNICAÇÃO DIGITAL

A aprovação da Lei Geral de Proteção de Dados (LGPD) em 2018 foi uma resposta à demanda crescente por normas para o uso de dados pessoais no Brasil, particularmente em áreas que manipulam informações delicadas, como a saúde. Ela define regras que exigem das entidades a garantia da segurança e privacidade dos dados, desde a sua recolha até o seu armazenamento, impondo sanções em caso de violação. No ambiente hospitalar, a LGPD é fundamental para salvaguardar os registros dos pacientes, garantindo que dados confidenciais sejam acessados e usados apenas com o seu consentimento ou por motivos legítimos, conforme estabelecido na legislação Brasil (2018)

Por meio da Resolução nº 1.821/2007, o Conselho Federal de Medicina (CFM) permite que as instituições de saúde utilizem o SIS para executar os processos informacionais necessários para guardar e manipular dados de pacientes no setor de saúde, disponibilizando esses dados quando solicitados pelo paciente. Assim, as entidades de saúde procuram informações que orientem as suas decisões com o objetivo de melhorar a saúde da população e os serviços de saúde em geral, utilizando o SIS que auxilia nesse processo.

Essas leis evidenciam que, para evitar complicações jurídicas, é de extrema importância adotar medidas de segurança que protejam as informações sensíveis, dessa forma, a adoção de tecnologias e protocolos de segurança não só cumpre a exigência legal, mas também fortalece a confiança do sistema.

2.2 CRIPTOGRAFIA

A criptografia estuda como o código escreve mensagens. Trata-se de um conjunto de métodos que tornam uma mensagem originalmente escrita muito clara para que apenas o destinatário possa decifrar e entender. (CAVALCANTE, 2004).

Com base em fragmentos de texto simples, o criptoanalista pode fazer uma estimativa, por exemplo, muitos computadores emitem a mensagem *"login"* quando reinicia. O trabalho do criptoanalista torna-se fácil com alguns pares de texto simples ou texto cifrado. Para ser seguro, o criptógrafo deve ser cauteloso e garantir que o sistema é inviolável, mesmo que seu oponente possa criptografar qualquer quantidade de texto simples que desejar Tanenbaum (2021).

Em contraste, o algoritmo RSA, criado por Ron Rivest, Adi Shamir e Leonard Adleman em 1977, é um dos primeiros algoritmos de criptografia de chave pública e é amplamente utilizado para proteger dados enviados.

Conforme explicado por Rivest et al. (1978), o RSA é considerado extremamente seguro para transações eletrônicas, incluindo assinaturas digitais e trocas de chaves, devido à complexidade de calcular grandes números primos. A dificuldade da fatoração de números grandes é um fator fundamental na segurança do RSA e é usada com frequência em conjunto com outros algoritmos, como o *Advanced Encryption Standard* (AES), para garantir uma comunicação segura.

A Máquina Enigma criada por Arthur Scherbius, foi uma das máquinas de criptografia eletromecânica complexas, desenvolvida na Alemanha durante os anos 1920, amplamente utilizada durante a Segunda Guerra Mundial, ela era capaz de cifrar mensagens de maneira muito mais complexa do que os métodos manuais anteriores, oferecendo diversas combinações (ORDONEZ, et al. 2005).

> Já se falou que a Primeira Guerra Mundial foi a guerra dos químicos, devido ao emprego, pela primeira vez, do gás mostarda e do cloro, que a Segunda Guerra Mundial foi a guerra dos físicos devido à bomba atômica. De modo semelhante se fala que uma Terceira Guerra Mundial seria a guerra dos matemáticos, pois os matemáticos teriam o controle sobre a próxima grande arma de guerra, a informação. Os matemáticos têm sido responsáveis pelo desenvolvimento dos códigos usados atualmente para a proteção das informações militares. E não nos surpreende que os matemáticos também estejam na linha de frente da batalha para tentar decifrar esses códigos. (SINGH, 2007, p.13)

No contexto, a criptografia assegura que somente os destinatários pretendidos possam acessar o conteúdo das mensagens, isso é particularmente importante em todos os ambientes, onde informações confidenciais.

Ferguson Bruce (2003) destaca que, muitas vezes, a quebra da segurança de um sistema criptográfico não ocorre devido a falhas no algoritmo em si, mas sim devido a vulnerabilidades na implementação ou ao comprometimento das chaves de criptografia.

Segundo Paar et al. (2010) como os invasores tendem a usar os pontos mais fracos para

quebrar a criptografia, os ataques de implementação sempre preocuparam a segurança de um criptossistema. Para corrigir essas deficiências e tornar os ataques de implementação menos eficazes, é fundamental reforçar todas as etapas do processo de implementação.

O uso inadequado de um sistema criptográfico pode criar vulnerabilidades que os adversários podem usar para comprometer a segurança dos dados. Isso abrange problemas como geração de chaves insuficientes, falhas na proteção de chaves em repouso ou em trânsito e erros de configuração do sistema. Além disso, falhas na gestão de chaves de criptografia, como uso de chaves fracas ou rotação incorreta, podem ameaçar a segurança do sistema.

Um dos algoritmos mais importantes para criptografia de dados no mundo moderno são o *Advanced Encryption Standard* (AES) e o *Rivest-Shamir-Adleman* (RSA). O AES, um padrão de criptografia simétrica adotado pelo governo dos Estados Unidos desde 2001, suporta chaves de 128, 192 e 256 bits e oferece vários níveis de segurança, frequentemente usado em uma variedade de aplicações, como criptografia de e-mails e proteção de dados eletrônicos, porque foi desenvolvido para resistir a ataques como criptoanálise e ataques de força bruta Daemen e Rijmen, (2002).

2.3 SEGURANÇA DIGITAL EM HOSPITAIS

Ayala (2016) destaca que, para proteger sistemas e dados hospitalares de ameaças cibernéticas, é essencial adotar estratégias específicas de segurança, que incluem a avaliação contínua de vulnerabilidades e a implementação de práticas de mitigação, visando a proteção de informações críticas no ambiente de saúde.

O direito do paciente ao sigilo está profundamente ligado ao sistema jurídico do Brasil, alinhado com os princípios constitucionais de proteção à dignidade humana e ao meio ambiente. Honra, reputação e vida pessoal, garantindo ao paciente o direito fundamental à privacidade, honra e privacidade. De acordo com o inciso X do artigo 5° da Constituição Federal, a privacidade é assegurada Brasil (1988)

Segundo Murphy (2015), a segurança digital em hospitais é crucial para salvaguardar informações confidenciais dos pacientes e assegurar a privacidade no contexto da saúde. Para alcançar isso, é preciso estabelecer uma combinação de políticas de privacidade, recursos tecnológicos e capacitação da equipe. Esses componentes contribuem para prevenir o vazamento de dados e minimizar os riscos ligados a ataques cibernéticos, que podem colocar em risco tanto a segurança dos pacientes quanto a operação do hospital.

> A segurança dos dispositivos médicos conectados é uma prioridade crítica, considerando que qualquer vulnerabilidade pode comprometer não apenas a integridade dos dados dos pacientes, mas também a eficácia do tratamento e, em casos

> mais graves, a segurança física dos indivíduos. À medida que os dispositivos se tornam mais interconectados, a proteção contra ataques cibernéticos torna-se uma necessidade imperativa para o setor da saúde. (Wirth, A., Brandt, D., & Crisafulli, J., 2020, p. 35)

Estes aparelhos, fundamentais para o acompanhamento e tratamento de pacientes, apresentam vulnerabilidades que podem afetar tanto as informações confidenciais quanto a saúde e a proteção física dos utilizadores. Com o aumento da interconexão na área da saúde, são essenciais medidas sólidas de defesa contra ataques cibernéticos para assegurar a integridade dos sistemas e a continuidade dos atendimentos médicos, reforçando a importância da segurança como uma prioridade neste segmento.

3 METODOLOGIA

A pesquisa bibliográfica consiste na coleta ou revisão de trabalhos publicados acerca da teoria que orientará o estudo científico, exigindo do pesquisador uma colaboração, estudo e análise. Seu objetivo é reunir e examinar textos já publicados para respaldar a pesquisa científica. Para Gil (2002), a pesquisa bibliográfica "[...] é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos". Para Severino (2007), a pesquisa bibliográfica realiza-se pelo:

> Registro disponível, decorrente de pesquisas anteriores, em documentos impressos, como livros, artigos, teses etc. Utilizam-se dados de categorias teóricas já trabalhadas por outros pesquisadores e devidamente registrados. Os textos tornam-se fontes dos temas a serem pesquisados. O pesquisador trabalha a partir de contribuições dos autores dos estudos analíticos constantes dos textos (SEVERINO, 2007, p. 122)

Conforme explica Santos (2004), "são os métodos práticos utilizados para juntar as informações necessárias à construção dos raciocínios em torno de um ato/fenômeno/problema".

3.1 METODOLOGIA COMPUTACIONAL

Quadro 1: Base de informações através da internet das ferramentas utilizadas.

Ferramentas Utilizadas	Descrição	Referências
2FA	Método de segurança que exige duas formas de verificação para acesso, combinando uma senha e algo que o usuário possui, como um celular para receber um código, aumentando a proteção contra acessos não autorizados.	RSA Security
Criptografia RSA	Algoritmo de criptografia assimétrica amplamente utilizado para proteger dados e comunicações. Baseia-se na dificuldade de fatorar grandes números primos, utilizando uma chave pública para criptografar mensagens e uma chave privada para descriptografá-las. RSA é utilizado em diversas aplicações, como segurança de dados em transações online, assinatura digital e troca segura de chaves, garantindo a confidencialidade e	Rivest, Shamir e Adleman (1977)

	a integridade das informações.	
Git hub	Plataforma de hospedagem de código-fonte e controle de versão que utiliza o Git. Permite que desenvolvedores colaborem em projetos, compartilhem código e gerenciem alterações por meio de repositórios. Oferece funcionalidades como pull requests, issues, wikis e integração contínua, facilitando o trabalho em equipe e o desenvolvimento ágil de software.	github.com
Google Cloud	Plataforma de serviços em nuvem que oferece soluções para armazenamento de dados, computação, inteligência artificial, bancos de dados, análise de dados, segurança, desenvolvimento e Internet das Coisas (IoT)	cloud.google.com
Neon Tech	Plataforma de computação em nuvem focada em fornecer soluções de infraestrutura e serviços para empresas, permitindo o desenvolvimento, gerenciamento e escalabilidade de aplicativos. Oferece serviços como hospedagem de sites, bancos de dados gerenciados e suporte para tecnologias modernas, como contêineres e microsserviços	neon.tech
Next Auth	Biblioteca de autenticação para aplicações Next.js que facilita a implementação de autenticação em projetos web. Suporta autenticação com provedores externos (como *Google, Facebook* e *GitHub*) e autenticação baseada em credenciais, oferecendo uma configuração simples e segura. Inclui funcionalidades como gerenciamento de sessão e suporte a (*JSON Web Tokens*) JWT	next-auth.js.org
NextJS	É um framework de desenvolvimento para React que permite a construção de aplicações web.	nextjs.org
Prisma	É um (Object-Relational Mapping) ORM moderno para Node.js e TypeScript. Ele facilita o trabalho com bancos de dados através de uma API intuitiva e fornece recursos como migrações de banco de dados, consultas fortemente tipadas e um modelo de dados declarativo.	prisma.io
React	Biblioteca JavaScript desenvolvida pelo Facebook para a construção de interfaces de usuário. Permite a criação de componentes reutilizáveis e facilita o desenvolvimento de aplicações web, React melhora a performance e a experiência do desenvolvedor, sendo amplamente adotado em projetos de front-end.	reactjs.org
Socket.io	Biblioteca JavaScript que permite a comunicação em tempo real entre servidores e clientes por meio de WebSockets. Facilita a criação de aplicações interativas, como chats e jogos online,	socket.io

	permitindo troca de dados bidirecionais de forma eficiente.	
Tailwind CSS	Framework CSS utilitário que permite criar designs personalizados de forma rápida, também fornece componentes pré-estilizados, que podem ser combinados para construir interfaces de usuário. Isso possibilita uma abordagem altamente flexível e responsiva, tornando o desenvolvimento de layouts mais ágil e facilitando a manutenção do código	tailwindcss.com
TypeScript	Linguagem de programação desenvolvida pela Microsoft que é uma superconjunto do JavaScript, adicionando tipagem estática opcional e outros recursos avançados. Permite detectar erros em tempo de compilação e melhora a manutenção do código, tornando-o mais robusto e escalável.	typescriptlang.org
Uploadthing	Refere-se aos serviços de hospedagem e compartilhamento de arquivos oferecidos pela T3 Tools por meio da Amazon Web Services.	uploadthing.com
Visual Studio	Ambiente de desenvolvimento integrado (IDE) da Microsoft que permite criar aplicativos para Windows, web e dispositivos móveis. Oferece suporte a várias linguagens de programação, como C#, Visual Basic e F#, além de ferramentas de depuração, design de interface e integração com sistemas de controle de versão, facilitando o desenvolvimento de software de maneira eficiente.	visualstudio.microsoft.com

Fonte: Autoria própria.

4 RESULTADOS

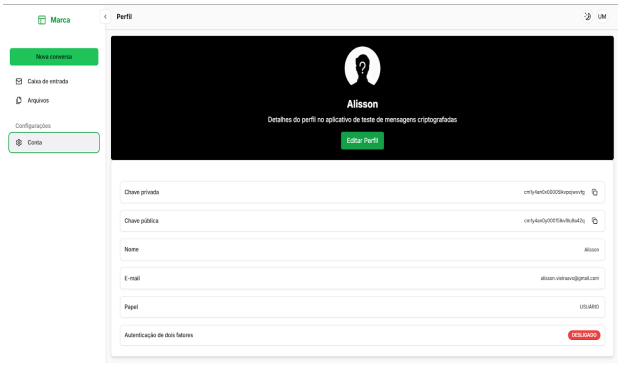
O desenvolvimento do Health Chat foi desenvolvido a partir de uma necessidade de proteção digital não somente aos pacientes, mas também à instituição hospitalar. A decisão da escolha da linguagem foi baseada no seu custo-benefício e na visão em escalonamento do sistema e na possibilidade de futuras atualizações, satisfazendo assim as demandas específicas aos hospitais e seus usuários. Para assegurar a proteção das comunicações e a integridade dos dados, foram implementadas ações sólidas, como a aplicação da autenticação de dois fatores (2FA), um recurso eficiente para intensificar a segurança no processo de registro.

Esta estratégia não apenas aprimorou a defesa contra acessos não permitidos, mas também proporciona um nível extra de confiança aos usuários, garantindo que somente indivíduos autorizados tenham acesso ao sistema.

Embora a solução implemente a criptografia RSA de 256 bits e adote boas práticas de

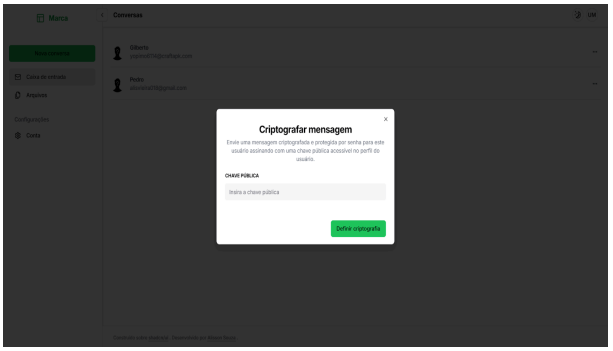
segurança, ela não garante proteção total contra todas as ameaças cibernéticas emergentes. Ademais, as avaliações feitas em cenários controlados e simulações de rede local podem não espelhar completamente as circunstâncias reais de uso, abrindo espaço para comportamentos imprevistos.

Figura 1 – Página do perfil do usuário.



Fonte: Elaborada pelo autor (2024)

Figura 2 – Página para criptografar a conversa



Fonte: Elaborada pelo autor (2024)

5 CONSIDERAÇÕES FINAIS

O Health Chat confirmou a aplicabilidade e efetividade da criptografia RSA para garantir a proteção e privacidade das comunicações no âmbito hospitalar, cumprindo os requisitos da LGPD. O projeto enfatizou a necessidade de soluções tecnológicas ajustadas às demandas críticas do setor de saúde, enfatizando a importância da segurança digital como uma questão ética e jurídica prioritária. Portanto, conclui-se que o sistema é um instrumento sólido e promissor, com capacidade para futuras ampliações que incorporam novas funcionalidades e atendem às crescentes necessidades de proteção de dados em ambientes delicados.

6 REFERÊNCIAS

CAVALCANTE, A. L. B. **Matemática I**: Notas de aula. UPIS, 2004.

DAEMEN, J.; RIJMEN, V. **The design of Rijndael: AES** - The advanced encryption standard. Springer, 2002.

FERGUSON, N.; SCHNEIER, B. **Practical cryptography.** Wiley Publishing, 2003.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores.** 4. ed. Amgh Editora Ltda, 2008.

HANSEN, S.; HANSEN, J. **Open source security tools**: Practical applications for security. O'Reilly Media, 2016.

KAHN, D. The codebreakers: **The comprehensive history of secret communication from ancient times to the internet**. Scribner, 1967.

NEMETH, E.; SNYDER, G.; HEIN, T. R.; WHALEY, B.; MACKIN, D. **UNIX and Linux system administration handbook.** Addison-Wesley Professional, 2017.

ORDONEZ, E.; PEREIRA, F.CHIARAMONTE, R. **Cryptographic techniques and network security.** Wiley, 2005.

PAAR, C.; PELZL, J. **Understanding cryptography**: A textbook for students and practitioners. Springer, 2010.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. **A method for obtaining digital signatures and public-key cryptosystems**. Communications of the ACM, v. 21, n. 2, p. 120-126, 1978.

SONICWALL. **Relatório de ameaças cibernéticas de 2021**. SonicWall Inc, 2021.

STALLINGS, **W. Criptografia e segurança de redes**: Princípios e práticas. 6. ed. Pearson, 2015.

STALLINGS, **W. Cryptography and network security**: Principles and practice. 7. ed. Pearson, 2017.

TANENBAUM, Andrew; FEAMSTER, Nick. **Redes de computadores**. 6. ed. Porto Alegre: Bookman, 2021.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico**. 24. ed. rev. e ampl. São Paulo: Cortez, 2016.

BARBOSA AF. **SEGURANÇA DIGITAL: uma análise de gestão de risco em empresas brasileiras.** São Paulo: Editora Segurança & Tecnologia; 2020.

MICROSOFT. Documentação do TypeScript [Internet]. 2018 [citado 2024 Oct 24]. Disponível em: https://www.typescriptlang.org/docs/

MURPHY, S. P. **Healthcare Information Security and Privacy**. 1. ed. Nova Jersey: McGraw-Hill Education, 2015.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal.

AYALA, L. **Cybersecurity for Hospitals and Healthcare Facilities: A Practical Guide.** Nova York: Apress, 2016.

WIRTH, A., BRANDT, D., & CRISAFULLI, J. (2020). **Medical Device Cybersecurity for Engineers and Manufacturers**. Boston: Artech House.

BRASIL: Presidência da República. Lei nº 13.709, de 14 de Agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD) [Internet]**. Brasília: Presidência da República**; 2020 [citado 14 Abr 2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.html

GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo, SP: Atlas, 2002.

SOMMERVILLE I. **Software Engineering**. 9th ed. Boston: Addison-Wesley; 2011.

NEXT.JS: **The React Framework** [Internet]. [citado em 2024 Nov 23]. Disponível em: https://nextjs.org

PRISMA: **Next-generation ORM for Node.js and TypeScript** [Internet]. Prisma; 2018 [citado em 2024 Nov 23]. Disponível em: https://www.prisma.io

TYPESCRIPT: **JavaScript com sintaxe para tipos** [Internet]. [citado em 2024 Nov 23]. Disponível em: https ://www .typescriptlang .org

REACT: **Uma biblioteca JavaScript para construção de interfaces de usuário** [Internet]. [citado em 23 de novembro de 2024]. Disponível em : https://reactjs.org

SOCKET.IO: **Comunicação bidirecional e de baixa latência para todas as plataformas** [Internet]. [citado em 23 de novembro de 2024]. Disponível em : https://socket.io

NEXTAUTH.JS: **Autenticação para Next.js** [Internet]. [citado em 23 de novembro de 2024]. Disponível em: https : //next -auth.js.org

NEON: **Postgres web server** – Envio mais rápido [Internet]. [citado em 23 de novembro de 2024]. Disponível em : https://neon.tech

UPLOADTHING: **Uploads de arquivos facilitados** [Internet]. [citado em 23 de novembro de 2024]. Disponível em : https://uploadthing.com

VISUAL STUDIO: **As melhores ferramentas de desenvolvedor para Windows e Mac** [Internet]. [citado em 23 de novembro de 2024]. Disponível em : https://visualstudio.microsoft.com

GOOGLE CLOUD: **Serviços de computação em nuvem** [Internet]. [citado em 23 de novembro de 2024]. Disponível em : https://cloud.google.com

SANTOS, A. R. dos. **Metodologia científica: a construção do conhecimento.** 6. ed. Rio de Janeiro: DP&A, 2004.

CONSELHO FEDERAL DE MEDICINA: Resolução CFM nº 1.821, de 16 de dezembro de 2007. **Aprova as normas éticas para o uso de sistemas de informação em saúde.** [Internet]. [citado em 2024 Nov 23]. Disponível em: https://www.cfm.org.br