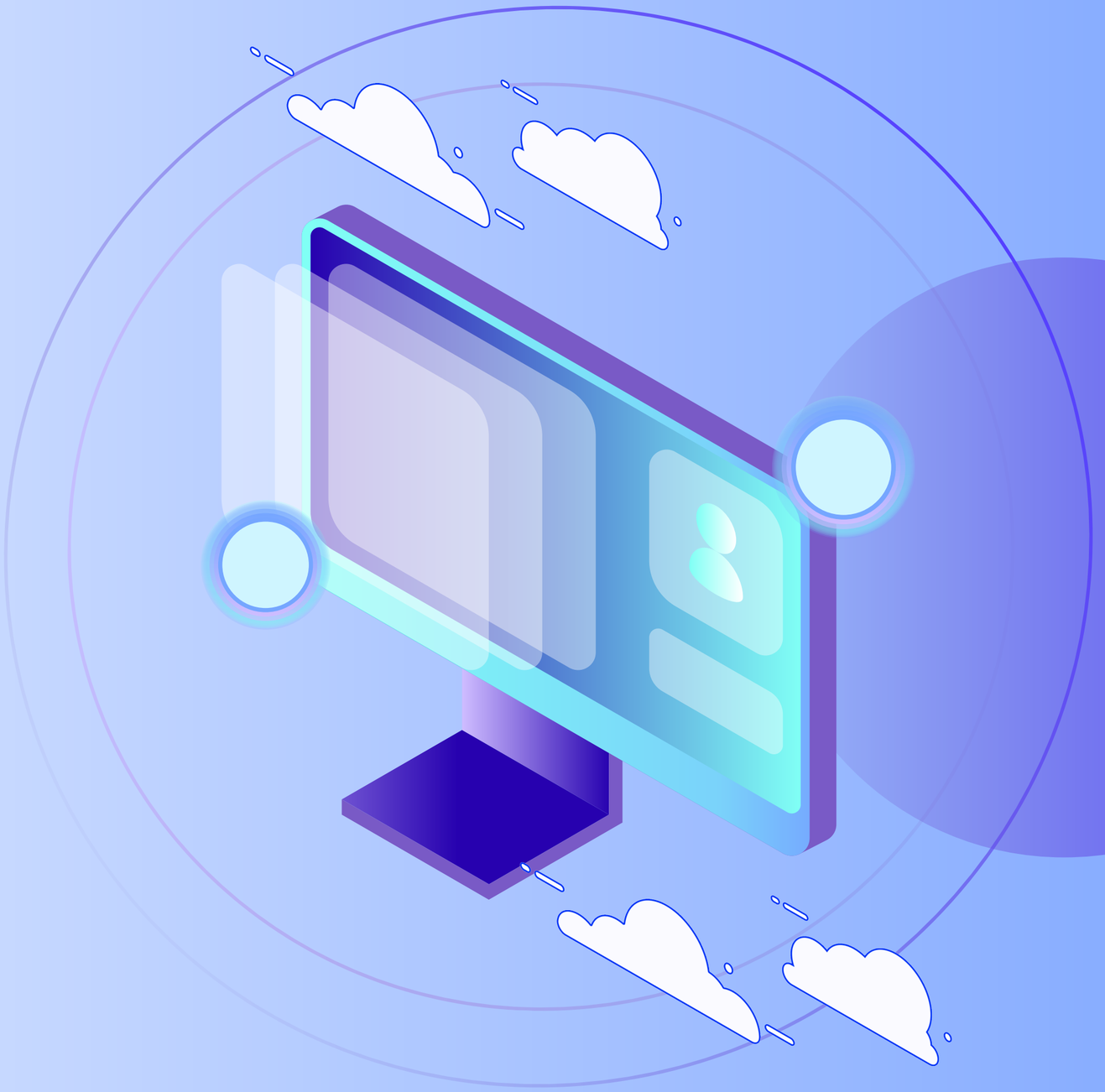
SSL CERTIFICATE MANAGER

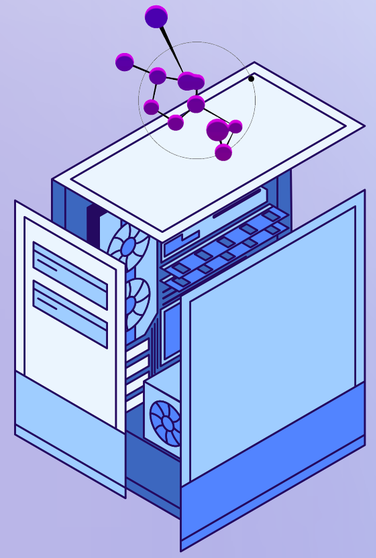


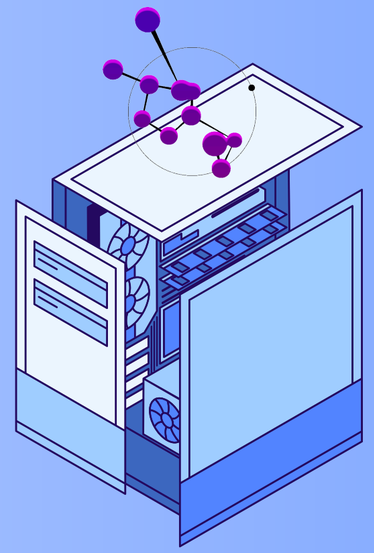
INCIDENTS

1. LinkedIn (2018)
2. Equifax (2017)
3. Microsoft Teams (2020)
4. New Zealand Stock Exchange (2020)
5. WhatsApp (2021)

WHAT IS SSL ?

SSL stands for Secure Sockets Layer. It’s a technology that encrypts the data transmitted between your web browser and the website you're visiting. When you visit a website, especially one where you enter personal information like passwords, credit card numbers, or other sensitive data, you want to make sure that this information is kept private and secure. This is where SSL certificates come into play.





HOW DOES IT WORK?

1. Encryption
2. Hashing
3. Data Integrity

IMPORTANCE

1. confidentiality
2. authenticity
3. Certificates

SSL CERTIFICATE MANAGER

Our project, the "SSL Certificate Manager," aims to simplify and automate the entire lifecycle of SSL certificates. By developing a Python-based solution, we intend to streamline the process of issuing, renewing, tracking, and managing SSL certificates, ensuring that websites remain secure and compliant with industry standards.

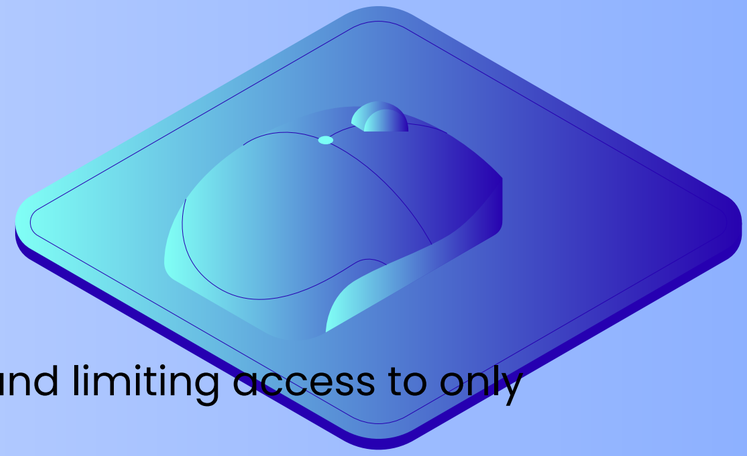
This project not only strengthens web security but also relieves website administrators from the burdensome task of manual certificate management, thereby preventing potential downtime and safeguarding user trust.

REQUIREMENTS TO ACHEIVE THE SSL CERTIFICATE MANNAGER PROJECT

1. Understanding the Basics of SSL/TLS
Certificate Management: It’s the process of handling these SSL certificates—creating, installing, monitoring, renewing, and, if necessary, canceling them.

2. Technical Requirements:-
To manage SSL certificates, you need:
A Certificate Authority (CA): This is the company (like Let’s Encrypt or DigiCert) that issues SSL certificates.

3. Designing Core Features:-
CRUD operations
Monitoring and alerts
set policies



4. Security Considerations:-
Protect the private keys that create certificates by storing them securely and limiting access to only authorized people.

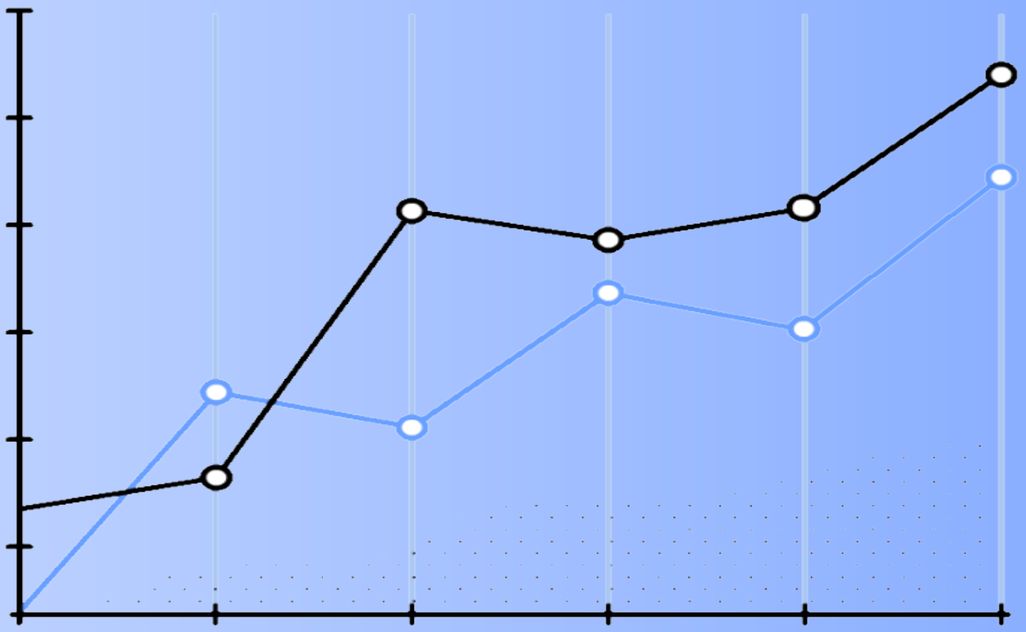
5. Integration with Existing Systems:-

HOW DOES SSL MANAGER WORKS?

An SSL manager is a crucial tool that facilitates the acquisition, installation, and maintenance of SSL certificates to ensure secure communication for websites. Its primary function involves generating a private key and a Certificate Signing Request (CSR), which is submitted to a Certificate Authority (CA) for verification. Once the CA issues the SSL certificate, the SSL manager installs it on the web server, enabling HTTPS and protecting data transmitted between users and the site. Additionally, it monitors certificate expiration dates, manages renewals, and handles any revocations if a certificate is compromised. By keeping SSL certificates up to date and ensuring secure configurations, the SSL manager plays a vital role in safeguarding sensitive information and enhancing overall website security.

FUTURE TRENDS

AND POTENTIAL MODIFICATIONS



Automated Certificate Management (ACME Protocol): The ACME protocol, used by services like Let's Encrypt, is becoming a standard for automating SSL certificate issuance and renewal. Future iterations of the project could incorporate ACME clients to streamline certificate management further.

Increased Adoption of HTTPS Everywhere: With more of the web moving to HTTPS, there will be a growing need for comprehensive SSL management solutions. The project can evolve to handle larger volumes of certificates efficiently.

Graphical User Interface (GUI): While the initial project might use a CLI, future versions could include a full-featured GUI, making it easier for non-technical users to manage SSL certificates.

CONCLUSION

Achieving the SSL Certificate Manager project requires a combination of technical knowledge, careful planning, and a clear understanding of future trends in digital security. By addressing the requirements outlined above, we can develop a robust tool that not only solves today's challenges but is also adaptable to future needs. As the digital landscape continues to evolve, so too can this project, growing to meet the needs of users and organizations in a world where secure communication is increasingly essential.

THANK YOU!

PRESENTED BY

SHAIK KHAJA
SARASWATH H.D.
K.DRUVI
SANJANA BHARADE
INDU V