Insight Innovators

May 2024

PROJECT PROPOSAL

Encryption, Decryption and Dealing with Data Leaks

Presented to
CNSS

Presented by
Insight Innovators

TABLE OF CONTENTS

ABOUT

Insight Innovators

We are Insight Innovators, a team of passionate and driven students from Tunku Abdul Rahman University of Management and Technology. As first-year students, we are at the beginning of our academic journey, but our enthusiasm for learning and growth is boundless. Our team is dedicated to honing our skills and capabilities, particularly in the sectors of cybersecurity, data science, and software development.

At Insight Innovators, our primary goal is to become proficient problem-solvers who can tackle challenges across various technological domains. Cybersecurity is one of our focal points, as we recognize the critical importance of protecting data and maintaining the integrity of information systems. We are committed to understanding the latest security protocols and developing innovative solutions to safeguard against cyber threats.

Data science is another area where we aim to excel. We are fascinated by the power of data to drive decision-making and create impactful solutions. Our team is eager to learn advanced data analytics techniques, machine learning algorithms, and data visualization tools to transform raw data into actionable insights. By mastering these skills, we hope to contribute to advancements in fields ranging from healthcare to finance.

In addition to our focus on cybersecurity and data science, we are enthusiastic about software development. We believe that creating efficient and user-friendly applications is essential in

today's digital world. Our team is dedicated to learning the latest programming languages, development frameworks, and best practices in software engineering. Through hands-on projects and continuous improvement, we aspire to build innovative applications that address real-world problems.

Despite being at the early stages of our university education, our determination to learn and improve is unwavering. We actively seek opportunities to participate in workshops, hackathons, and collaborative projects that challenge us to apply our knowledge and expand our skill set. At Insight Innovators, we believe that our dedication and passion will drive us to achieve great things and make meaningful contributions to the fields of cybersecurity, data science, and software development.

We are Insight Innovators, and we are ready to embark on this exciting journey of learning, growth, and innovation. Join us as we strive to make a positive impact on the technological landscape and pave the way for a secure, data-driven future.

Organization

Liew Qi Jian
Student

Ng Wan Xin
Student

Ho Shao Mun
Student

MISSION AND VISION

Mission

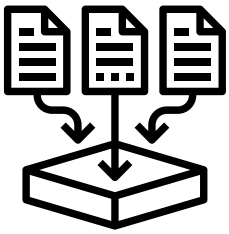
Our mission at Insight Innovators is to empower students with the knowledge and skills to address real-world challenges in cybersecurity, data science, and software development. Through hands-on projects, collaborative learning, and a commitment to continuous improvement, we aim to develop innovative solutions that enhance data security, drive data-driven decision-making, and create impactful technological advancements. As a team of dedicated and passionate students, we strive to make meaningful contributions to the technological landscape while fostering a culture of curiosity, learning, and growth.

Vision

Our vision is to become a leading student-led team renowned for our expertise and innovative approaches in cybersecurity, data science, and software development. We aspire to create a safer and more efficient digital world by pioneering solutions that safeguard sensitive information, leverage data for impactful insights, and develop cutting-edge applications. By nurturing our talents and collaborating with industry experts, we envision a future where Insight Innovators plays a pivotal role in shaping the technological advancements of tomorrow, setting new standards of excellence and innovation in the field.

GOALS FOR THIS PROJECT

Detect and Mitigate Data Leaks

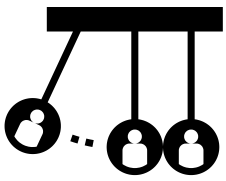


Implement real-time detection mechanisms to identify unauthorized disclosure of sensitive words or numbers across different digital platforms and minimize the consequences of data breaches through constant logging.

Enhance Data Security and Compliance

Enhance data security through advanced encryption and decryption methods. Align the solutions with stringent data privacy and security regulations such as GDPR, HIPAA, and PCI DSS to ensure legal compliance

Scalability and Adaptability



Design a solution capable of handling various data volumes and adaptable across multiple digital platforms. This ensures that our solution can grow and evolve with emerging security challenges and technological advancements.

Our comprehensive strategy encompasses proactive measures to detect and prevent data leaks, safeguard against unauthorized disclosures, mitigate the impact of breaches, ensure regulatory compliance, and ensure

scalability. Real-time detection mechanisms enable the prompt identification of potential breaches, while advanced encryption methods enhance data security and prevent unauthorized access. Swift response plans and continuous logging mitigate the impact of breaches, minimizing disruption and protecting affected parties. Alignment with regulatory standards such as GDPR, HIPAA, and PCI DSS ensures legal compliance and upholds user privacy. Additionally, our scalable solution is adaptable to evolving security challenges and technological advancements, ensuring long-term effectiveness and relevance.

PROPOSED TIMELINE

Week 01	• Planning and Discussion
Week 02	• Background Learning
Week 03	• Proposal Drafting, Develop Code Structures
Week 04	• Combining Front & Back End
Week 05	• Final Testing and Submission

Our project timeline was divided into distinct phases, each contributing to our overall success. In Week 1, we planned and discussed our project's direction, ensuring alignment among team members. Week 2 focused on background learning, equipping us with essential knowledge and skills. In Week 3, we drafted proposals, refining our ideas for execution. Week 4 saw us developing code structures, translating concepts into tangible code. Finally, in Week 5, we combined front-end and back-end elements, conducting rigorous testing to ensure optimal functionality. Throughout this journey, we celebrated achievements, from implementing real-time detection mechanisms to ensuring compliance with data privacy regulations, highlighting our dedication and collaboration.

PROJECT FEATURES

Sensitive Data Detection	Detect whether data is sensitive, such as IC numbers, bank account passwords, personal home addresses, and similar information, and provide real-time alerts upon detection.
Encryption	The encryption part of the project utilizes AES encryption with a 256-bit key generated. Data is padded to ensure compatibility and encrypted with a randomly generated initialization vector (IV) before being encoded in base64 for secure transmission.
Decryption	The decryption part of the project is achieved by reversing AES encryption by utilizing the same 256-bit key and initialization vector (IV). Data is then unpadded to retrieve the original plaintext.
Demo Programs	The encryption and decryption features are showcased across diverse sectors in prototype programs, including healthcare, social media messaging, and financial transactions, demonstrating their applicability across various industry domains.

The project entails real-time sensitive data detection, alerting upon identification of information like IC numbers, bank account passwords, and personal addresses. Encryption employs AES with a 256-bit key, padding data for compatibility, and encoding it in base64 post-encryption for secure transmission. Decryption reverses AES encryption, utilizing the same key and initialization vector, ensuring data integrity.

These encryption and decryption functionalities are demonstrated across healthcare, social media messaging, and financial transactions, illustrating their adaptability across different sectors. By showcasing their applicability in prototype programs, the project highlights the versatility of these security features in safeguarding sensitive information across diverse industry domains.

FUTURE ENHANCEMENT

For future enhancements, the project could implement database encryption to bolster data security at rest, ensuring that sensitive information remains protected even when stored. Additionally, integrating network layer encryption would provide an extra layer of security by encrypting data packets transmitted over networks, safeguarding against interception and unauthorized access. Furthermore, implementing transport layer encryption, such as TLS/SSL protocols, would enhance data integrity during transmission, securing communications between clients and servers.

Expanding the repertoire of encryption methods could involve incorporating asymmetric encryption, such as RSA, for key exchange mechanisms, complementing the existing symmetric encryption approach. Additionally, adopting homomorphic encryption could enable computations on encrypted data directly, enhancing privacy-preserving data processing capabilities. Moreover, the integration of post-quantum encryption algorithms would future-proof the system against potential quantum computing threats, ensuring long-term resilience in safeguarding sensitive data. These advancements would fortify the project's security infrastructure, ensuring robust protection against evolving cyber threats.

CONCLUSION

Finally, our presentation at the CNSS Voluptate at TARUMT showcased our project as a comprehensive solution to the contemporary network security challenges. By implementing advanced information detection and encryption/decryption processes nationwide, we aim to bolster personal data protection amidst the proliferation of electronic platforms.

The primary objective of our project is to develop the first monitoring platform solution for preventing data leaks, addressing a critical threat across various industries including social networks, e-commerce, banking, healthcare, and transportation. We prioritize real-time monitoring to swiftly respond to unauthorized disclosures, ensuring compliance with data privacy regulations.

Moving forward, our project's objectives encompass leak detection in real-time, prevention of unauthorized disclosures, mitigating the impact of breaches, ensuring regulatory compliance, and providing a customizable solution adaptable to future challenges. Leveraging Flask framework, AES encryption, and a mock email server, our system offers smart and effective tools for identifying and protecting sensitive information, along with robust incident handling capabilities.

In future enhancements, we plan to integrate database encryption, network layer encryption, and transport layer encryption to fortify our security infrastructure. Additionally, expanding encryption methods to include asymmetric encryption, homomorphic encryption, and post-quantum encryption algorithms will ensure long-term resilience against evolving cyber threats, further solidifying our commitment to maintaining high standards of security and confidentiality in the ever-changing landscape of cybersecurity.

Insight Innovators

For inquiries, contact us.

Liew Qi Jian: +60127173985

Ng Wan Xin: +60127540827

Ho Shao Mun: +60104389954