Homomorphic Encryption

Whitepaper

2022

TechInspire
Inspire for innovation

Authored by:
Aras Arasilango

ENERGY SHIELD

Homomorphic Encryption

IN A NUTSHELL

In this project, we considered the potential security threats in the energy sector to develop a searchable encryption tool that can allow the security analyst to sanitize and search necessary information in an encrypted domain using the computationally secure homomorphic encryption technique. Any type of security event data can be extracted by multiple parties at different access control levels and threat graphs on the anonymised data can be developed by them to protect the privacy of the data and the devices in the tool. The tool will be GDPR compliant with the features of handing single and multiple key queries and ranked searches in the encrypted databases.

CONTEXT

The scope of this tool is to develop a searchable encryption platform as part of the EnergyShield project in order to provide data privacy and data security mechanism. Most of the cloud service providers store the data in plaintext format and users need to use their own encryption algorithm to secure their data if required. The data needs to be decrypted whenever it is to be processed [1]. The focus is to utilise a relevant Homomorphic Encryption (HE) scheme to encrypt the anonymised data which can be searched without decrypting. Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key. When we decrypt the result of any operation, it is the same as if we have carried out the calculations on the plain data [1].

In addition, the tool is GDPR compliant and provide a mechanism to search using single and multiple string queries, ranked search and to allow security analysts to produce threat graphs that can help in identifying the cyber threat links.

“

A system that provides data privacy and security mechanism for energy sector using Homomorphic Encryption

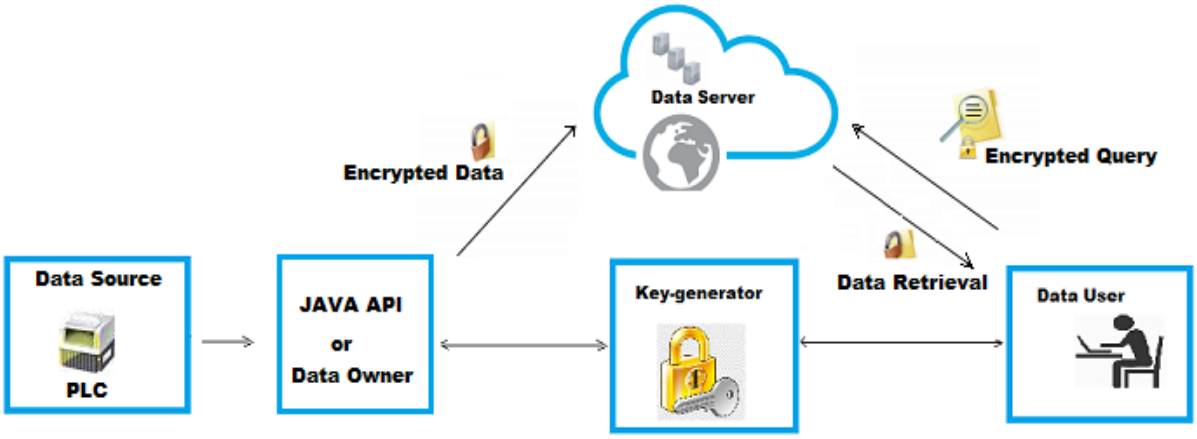
Aras Arasilango,

Tech Inspire Ltd

TECHNICAL DETAILS

Design and Methodologies. The data model necessary for this project was identified from sample anomaly detection records supplied by the respective project partner of EnergyShield. This model includes the entities such as Company, PLC, Measurement, Security Analyst, and Anomaly.

The following diagram shows the architecture of HE tool.



Java Swing user interface has been implemented to connect to a database in the cloud server using Web Socket Bi-directional full-duplex protocols. Java Swing technology has been used for producing user interface and analytical reports in the system, because HTML is vulnerable to JavaScript injection.

WebSocket programming models and respective libraries have been used for remote communication between the client and server components of the system. Paillier Homomorphic scheme has been used to encrypt the data which are received in a form JSON records, from the Anomaly Detection tool of the project. Up on receiving the JSON records Web API encrypts and stores into MySql database so that the encrypted data are used by the HE tool for producing Analytical reports on the UI and by the SIEM tool for developing various threat graphs.

ENERGYSHIELD DEMONSTRATOR

The HE tool has been developed to support the following features.

a) Encrypting the anonymized data from any kind of security event alert.

b) Provide a mechanism to search encrypted data using single and multiple keyword-based queries.

c) Provide a mechanism for ranked search on the encrypted data.

d) Making the encrypted data to be extracted by multiple parties at different access control levels.

e) Allowing security analysts to create threat graphs on the anonymized data to protect the privacy of the data and the devices in the smart grid environment.

The system has been developed to encrypt the data using Homomorphic Encryption scheme and with the Web Socket technique for the remote communication between the Anomaly detection tool and the server.

The technology used are Java, Java Swing, MySql, Jetty Servlet server, AES and Paillier Encryption scheme.

The tool has been tested with the energy sector data received from the Anomaly Detection tool developed by one of the partners of the project. The data was sent in JSON record.

BEST PRACTICES & LESSONS LEARNED

Two challenges were faced during the implementation of the tools which are 1) encrypting the database tables for storing the encrypted data and 2) producing the analytical graph from the encrypted result.

Firstly, none of the database software provide standard method to convert the plain database structure to encrypted database structures including table name and fields. We have devised an algorithm and implemented a function to take the table name as a parameter along with other database connection parameters and to go through every column and encrypt them to create a new table with the encrypted table name. Every field needs to store 310-character string data, because the searchable encrypted data can fit within 310 characters. By doing this way, the table names and fields will not be vulnerable to hackers.

We have overcome the second problem by devising an algorithm to collect the decrypted result and to form arrays of plain data suitable for passing to a graph function.

This tool can be integrated and used not only for energy sector, but also for any sector with little modification of the data model and rewriting respective modules of the tool.

All the traditional encryption schemes such as AES, RC4, DES, 3DES, RC5, RC6, and the Searchable Encryption schemes use either public and private keys or private key only for asymmetric and symmetric encryption respectively. The major problems in encryption are 1) protecting the keys and managing the keys 2) Hackers generate keys randomly to match the actual key. These problems can be overcome by not using the key external to the software or tool which encrypts files or data. In this case, the user

does not handle the key at all and not necessary to manage the key as well. Furthermore, the hackers have no opportunity to get hold of the keys to decrypt the files or data and there is no way that a randomly generated key can be applied with the software.

An AES encrypted scheme-based application has been implemented by me in another project called “Testenium meta-computing cloud platform” of Testenium Limited, UK. This platform enables users to use pair of encryption/decryption software which were dynamically generated by the meta-computing engine with unique key embedded for every user so that users do not have to use encryption keys at all. Similar techniques may be used for any encryption schemes including Searchable Encryption to ensure the security of the data or files.

DISSEMINATION & COMMUNICATION

Articles published:

Homomorphic Encryption: The ‘Holy Grail’ for Big Data Analytics and Legal Compliance in the Pharmaceutical and Healthcare Sector, Marcelo Corrales Compagnucci, Janos Meszaros, Timo Minssen, Arasaratnam Arasilango, Talal Ous, Muttukrishnan Rajarajan, European Pharmaceutical Law Review, Volume 3 (2019), Issue 4, Page 144 - 155

Available **literature** :

[1] Maha TEBAA, Said EL HAJII Laboratory of Mathematics, Computer and Applications, University Mohammed V–Agdal, 2013

[2] Manish M Potey, Dr C A Dhote, Homomorphic Encryption for Security of Cloud Data, 7th International Conference on Communication, Computing and Virtualization,2016

ABOUT THE COMPANY

Tech Inspire Ltd is a fast growing UK start-up company focusing on the security and privacy aspects of intelligent information infrastructure, mobile computing and Cloud computing. Our team is internationally known in the areas of data security, end-to-end encryption and privacy preserving searchable encryption. Since its inception in 2013, Tech has been actively engaged in a number of cutting-edge research, innovation and commercialization projects within EU and internationally. Tech is currently involved in Horizon 2020 and Horizon Europe projects working in collaboration with major European partners to develop the security strategies and implement novel techniques under the Innovation Action (IA) and Research and Innovation Action (RIA) Schemes.

Tech is also involved in Close-to-Market product developments such as continuous authentication for mobile phones and secure data encryption in Cloud storage. The core expertise of Tech's team are: - Security protocol design, implementation and validation - Security Architectures - Risk assessment and compliance - Security certification and audit - Threat and Vulnerability Management - Critical infrastructure protection - Data Privacy - Searching in the encrypted domain - Classifying data in the encrypted domain

This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement No. 832907

Website: www.energy-shield.eu **Twitter**: @EnergyShield_
LinkedIn Group; https://www.linkedin.com/groups/8831159/
Youtube channel: https://www.youtube.com/channel/UCtNRIf0uXvDsxVCSo1NfF_Q
E-mail: EnergyShield@siveco.ro