**CIPHER AND DECIPHER USING CRYPTOGRAPHY-FERNET APPLICATION FOR SECURE DATA**

**Preface**

**TABLE OF CONTENTS**

**1. SOFTWARE DEVELOPMENT LIFE CYCLE**

**2. PLATFORM KNOWLEDGE**

**3. DOMAIN KNOWLEDGE**

3.1 METHODS

**4. ABOUT THE PROJECT**

4.1 ABSTRACT

4.2 SCOPE OF THE PROJECT

4.3 EXISTING SYSTEM

  4.3.1 DISADVANTAGES

     4.4 PROPOSED SYSTEM

  4.4.1 ADVANTAGES

**5. BOTTOM LINE AND FUTURE ENHANCEMENT**

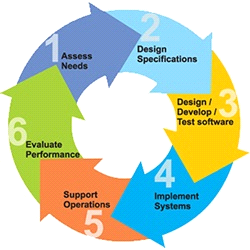
**6. HARDWARE AND SOFTWARE REQUIREMENTS**

**1. SDLC (Software Development Life Cycle)**

The Software Development Life Cycle is a systematic process for building software that ensures the quality and correctness of the software built. SDLC process aims to produce high-quality software which meets customer expectations. The software development should be completed within the pre-defined time frame and cost.

**SDLC Phases**

The entire SDLC process is divided into the following stages:



* Phase 1: Requirement collection and analysis
* Phase 2: A feasibility study
* Phase 3: Design
* Phase 4: Coding
* Phase 5: Testing
* Phase 6: Installation/Deployment
* Phase 7: Maintenance

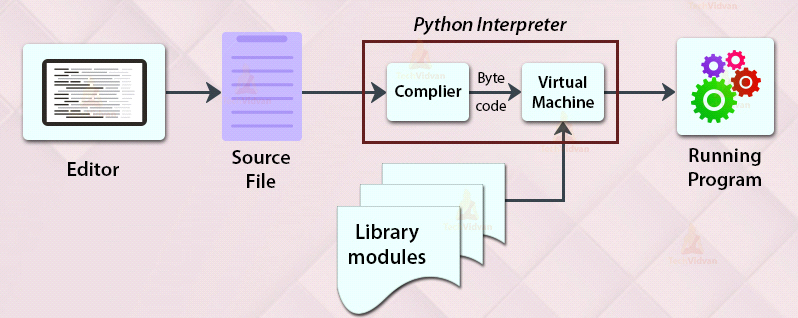
**2. Platform Knowledge**

**Introduction to Python:**

Python is developed by Guido van Rossum. Guido van Rossum started implementing Python in 1989. Python is a facile programming language so even if you are new to programming, you can learn python without facing any issues. Python is a general-purpose programming language that is becoming ever more popular for data science. Companies worldwide are using Python to harvest insights from their data and gain a competitive edge. Python specifically for data science. To store and manipulate data, and helpful data science tools to begin conducting your analyses.

**What is Python?**

Python is an interpreted, high-level, general-purpose programming language. It is dynamically typed and collected. Python is an interpreted language and not a compiled one, although compilation is a step. Python code, written in **.py** file is first compiled to what is called byte code which is stored with a **.**pyc or **.**pyo format. Instead of translating source code to machine code like C++, Python code it translated to byte code. This byte code is a low-level set of instructions that can be executed by an interpreter.  One popular advantage of interpreted languages is that they are platform-independent. As long as the Python byte code and the Virtual Machine have the same version, Python byte code can be executed on any platform (Windows, MacOS, etc). Dynamic typing is another advantage. In static-typed languages like C++, you have to declare the variable type and any discrepancy like adding a string and an integer is checked during compile time*.* In older programming languages, memory allocation was quite manual. Many times when you use variables that are no longer in use or referenced anywhere else in the program, they need to be cleaned from the memory. Garbage Collector does that for you.



**3. Domain**

**CYBER SECURITY**

Cybernetics is a trans disciplinary approach for exploring regulatory systems their structures,

constraints, and possibilities. The essential goal of the broad field of cybernetics is to

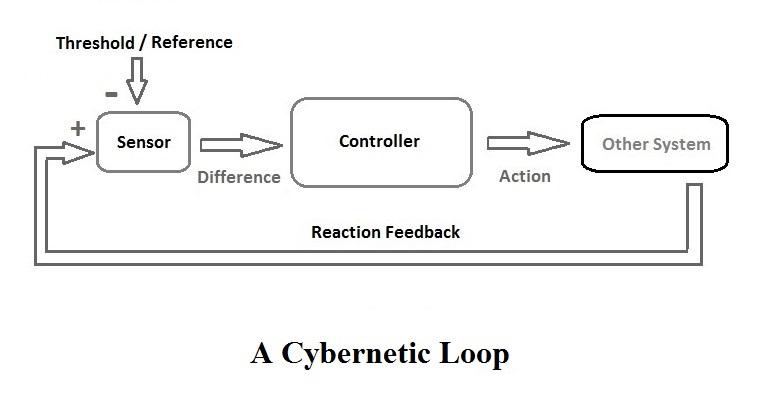
understand and define the functions and processes of systems that have goals and that

participate in circular, causal chains that move from action to sensing to comparison with

desired goal, and again to action. Its focus is how anything (digital, mechanical or biological)

processes information, reacts to information, and changes or can be changed to better

accomplish the first two tasks. Cybernetics includes the study of feedback, black boxes and derived concepts such as communication and control in living organisms, machines and organizations including self-organization. Cybernetics has been defined in a variety of ways, by a variety of people, from a variety of disciplines. Science concerned with the study of systems of any nature which are capable of receiving, storing and processing information so as to use it for control. Studies in cybernetics provide a means for examining the design and function of any system, including social systems such as business management and organizational learning, including for the purpose of making them more efficient and effective. Fields of study which have influenced or been influenced by cybernetics include game theory, system theory (a mathematical counterpart to cybernetics), perceptual control theory, sociology, psychology (especially neuropsychology,  behavioral psychology , cognitive psychology), philosophy, architecture, and organizational theory. System dynamics, originated with applications of electrical engineering control theory to other kinds of simulation models (especially business systems)



Intelligence (AI) use computer technology to build intelligent

machines; they consider implementation (that is, working examples) as the most important result. Practitioners of cybernetics use models of organizations, feedback, goals, and conversation to understand the capacity and limits of any system (technological, biological, or social); they consider powerful descriptions as the most important result. Cybernetics as a process operating in nature has been around for a long time; actually, for as long as nature has

been around. Cybernetics as a concept in society has been around at least since Plato used it to refer

to government. Cybernetics has always been a hard field to pin down. Wiener presented it a synthesis of

work in digital computing, information theory, and feedback control. As such, it represented a new kind of science, devoted to immaterial elements such as ‘bits’ of information rather than the material substances that define traditional sciences like physics, chemistry, and biology. Again, in contrast to the traditional organization of knowledge, cybernetics was strongly interdisciplinary. The Macy conferences brought anthropologists, sociologists, psychologists, and psychiatrists together with natural scientists, mathematicians, and engineers, and claims were made for cybernetics as a universal superscience capable of accommodating all of the disciplines. Cybernetics is concerned with concepts at the core of understanding complex systems such as learning, cognition, adaptation, emergence, communication, and efficiency. Cybernetics has been influenced by and, in turn, has applications in fields as diverse as psychology and

control theory, philosophy and mechanical engineering, architecture and evolutionary biology, or social sciences and electrical engineering.

There is little wonder that philosophers and scientists have different definition of cybernetics. Cybernetics is “the art of creating equilibrium in a world of constraints and possibilities,” according to the philosopher Ernst von Glasersfeld. The famous mathematician Andrey Nikolaevich Kolmogorov defines cybernetics as the “science concerned with the study of systems of any nature which are capable of receiving, storing, and processing information so

**4. About the project:**

**4.1 Abstract:**

The science of information security is called cryptography. The word is a translation of the Greek word kryptos, which means hidden. Microdots, fusing words and images, and other methods of obscuring information in storage or transit are only a few examples of the techniques used in cryptography. Electrical engineering, computer science, and mathematics all converge in modern cryptography. Among the uses for cryptography are electronic commerce, computer passwords, and ATM cards. There are open source cryptography projects that provide security for a variety of applications. In the paper we propose that that usage of cryptography algorithm which is used for security purposes when the data is received and the data will be further Encrypted and it will secure the information until the data is decrypted when the situation arises These Cryptography projects implement cryptographic algorithms and protocols that are designed to protect communications and data from being intercepted or tampered with in cryptography fernet guarantees ‘when the decryption read without the key also support the implementation of key rotation via multi fernet . It can also be used to verify the authenticity of digital signatures and to ensure the privacy of communications. Mostly cryptography is used web services application in order to prevent the phishing, Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain and other fraudulent activities. Likewise cryptography is widely used in various technologies

**4.2 Scope of the project:**

The most crucial concern in today's computer world is the security, integrity, and confidentiality of the organization's data. In this paper we propose that how the cryptography Method are used to ensure secrecy and integrity of the data presence in which our cases used in the bio industry in order to prevent data leakage in bio industry the fuel processing process is a crucial it may varies from firm to firm to prevent those data we use cryptography method to cipher and decipher, to prevent that will lead to downstairs the company profit and the economic growth so the process will secured by using Cryptography method, overcome the data theft in the bio industry, Symmetric cryptography and asymmetric cryptography are the two categories of cryptographic techniques. The same key is used for encryption and decryption in the symmetric approach. The usage of two keys Asymmetric cryptography uses two keys: a public key for encrypting data and a private key for decrypting it. So in our project we using symmetric approach to encrypt the data with generated fernet key and uses encrypt and further the encrypted code will be encoded with the asymmetric key file into the readable file.

**4.3 Existing system:**

Any computer system that is connected to the internet is vulnerable to attacks from hackers who might try to take control the system in order to steal information for illicit purposes. In an effort to undermine a company's business activities, they can potentially try to crash a system. A variety of system attacks have been developed to undermine computer system.To prevent the attacks may encryption and decryption method are used like Triple DES, AES,RSA, and Blowfish etc.…most of the pervious mentioned methods protects information stored on smartphones, laptops, and other devices - in some cases by default, At the same time, encryption is relied on by criminals to avoid investigation and prosecution, including criminals who may unknowingly benefit from default settings as well as those who deliberately use encryption the mentioned encryption algorithm is complicated and slow performance to overcome this we use simple cryptography method for encrypting and decrypting purposes. Thus, encryption complicates law enforcement and intelligence investigations.

**4.3.1 Disadvantages:**

• **Forgetting Passwords:** A disadvantage of encrypting files is if you forget the password that you used, you may never be able to recover the data.

**. Raising Suspicious-** a significant other may want to know what terrible secrets you are keeping that require you to encrypt files on your compute

. **Developing False Sense of Security-** . A determined person may marshal overwhelming computer resources to decrypt your secret files.

**. Requiring cooperation-** Using encrypted files that are designed to be opened and shared by two or more people can be disadvantageous when one or more participants finds it a burden to use encryption.

. **Slow performances-** each recipient receive the key through different channel

**4.4 Proposed system:**

Due to the recent increase in demand for digital signal transmission, the issue of massive losses from unauthorized data access has emerged as a pressing concern. As a result, data security has emerged as a crucial and pressing issue in applications for multimedia data transfer. Various sorts of cryptographic systems are required to secure sensitive information from unwelcome users or against unauthorized duplication and modification. In our project we used the Cryptography as to prevent the massive losses from unauthorized data access and transmitting a data in a secure way using symmetric way, the symmetric cryptography is normally used to encrypt private data for its high performance the use of single shared secret to share encrypt data between parties comparatively symmetric cryptography is usually faster than asymmetric because of the single key encryption . There have been various data encryption techniques on multimedia data proposed. Genetic Algorithms (GAs) are among such techniques.

**Advantages:**

### ****Confidentiality**** - Confidentiality ensures that only the recipient can decrypt the message and read its content.

* **Integrity**- Integrity focuses on the ability to ensure the information contained in the message cannot be modified
* **Authenticity -** Authenticity ensures the sender and recipient can verify each other’s identities and the destination of the message.
* **Simple-** the provided result helps encryption and decryption easily.
* **Convenient-**  hence it is fast and convenient

**5. BOTTOM LINE AND FUTURE ENHANCEMENT:**

In this project, a general study of the performance of Cryptography is conducted by means of during syncing data for upload we use fernet key to encrypt the data which the key is encoded while receiving the data. There are many different Encryption and Decryption proposed to meet the requirement of discovering preferred items in a large information space. In this project the Cryptography system helps in encrypting and decrypting important process, May the data inaccuracy the result may vary hence in this modern technology asymmetric cryptography is become vulnerable hence the hackers intercept key before encryption process where future is going for quantum cryptography which using the quantum mechanics for transmitting the data for large purposes, So it is important to enhancement the data analysis and improves the Cryptography by using various algorithms, methods and techniques and can lead to usage of Cryptography system in various industries.

**6. System Requirement;**

**Hardware requirements:**

* Processor: Intel (R) Pentium (R)
* Speed: 1.6 GHz and Above
* RAM: 4 GB and Above
* Hard Disk: 120 GB
* Monitor: 15’’ LED SVGA
* Input Devices: Keyboard, Mouse

**Software requirements:**

* Operating system: Windows 7 / 8 / 8.1 / 10
* Coding Language: PYTHON
* IDE: PyCharm
* Database: MySQL









































