ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 7, Issue 1, pp: (105-111), Month: January - March 2019, Available at: www.researchpublish.com

Secure Multilevel System (FLS & RLS) for a Cyber-Physical System in Association with Data Mining

Dr. M. Sharada Varalakshmi

Professor & HOD, Department of Computer Science and Engineering
St.Peters Engineering college, Hyderabad

Abstract: **The main scope of this research paper is to protect the information from the unauthorized usage by applying the Cyber-Physical System (CPS). It is implemented by classifying the data in multilevels through a secure multilevel classifier (SMC) based on Field Level Security (FLS) and Record level security (RLS) in the network, primarily for any network transactions. The core aim of this theme is to heighten the security with flip key and cryp key, for the data preserved in different encoded locations and the evaluation of the performance of the data security through CPS.**

Keywords: **Classification, multilevel security, field level, a record level, flip key, cryp key, cluster analysis, regression, cyber-physical system, data mining.**

I. INTRODUCTION

When we start thinking about the research, especially on the future technologies, we may get the idea about Big Data Analysis, Cloud Security, Managing the network traffic in the IOT and the emerging role of CPS. Providing the Security at multi-level is receiving a lot of attention from both academic, research and industrial worlds. A Cyber-Physical System (CPS) is the new frontier for security. It consist of both physical and computational elements and are becoming more and more popular in today's society.

The number of connected devices is expected to grow to 50 billion by the year 2020. Innovations are determining this increase in the areas of smart cities, Defense sectors, Internet of Things (IOT), Body Area Networks, smart grids and wearable sensors. With digital technologies becoming embedded in daily objects and infrastructures.

CPS offers both big opportunities and big effort of security in the modern social club. They bring up major research challenges on the protection of the data and information. The research agendas set up by these questions are interdisciplinary and can be tackled from a range of technological, behavioral and socioeconomic perspectives.

The proposed position will consequently base in Security for our interdisciplinary research centre on Security and Protection Science. The CPS is controlling the functions in a network like classification, clustering, regression, association, storage and retrieval, which leverages secure cryptographic protocols for encoding to make the data more confidential.

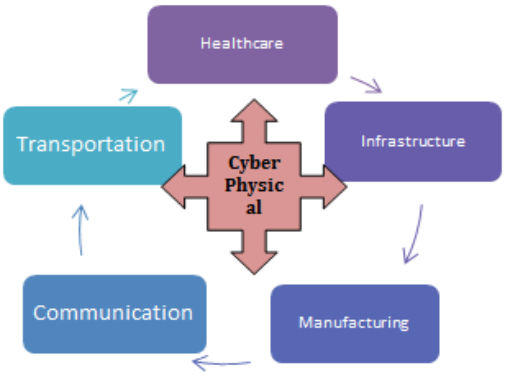


Fig No: 1. CPS Domains and its Applications

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 7, Issue 1, pp: (105-111), Month: January - March 2019, Available at: www.researchpublish.com

Cyber-physical systems (CPS) refer to novel hardware and software compositions creating smart, autonomously acting devices, enabling efficient end-to-end workflows and new forms of user-machine interaction [1].

In numerous emerging application areas such as health maintenance, traffic management or energy supply, CPS carry a high potential for creating new markets and solutions to societal hazards, but impose highest requirements to quality regarding resilience, safety, protection, and privacy [1], [3].The heterogeneous, evolving and distributed nature of CPS bears significant challenges continuously to assure these quality requirements employing state of the art methods and engineering sciences.

Foundational research efforts are required to achieve a predictable quality level in an effective, traceable and measurable way, coping efficiently with external and national changes, supporting necessary transitions between mechanical, electrical and software technology, as well as integrating management, design and deployment aspects[3].

Cyber Security is one of the essential requirements for the security system is to provide information security whose key attributes are confidentiality, data integrity, and authentication and data availability [34]. The foremost measure in the direction of protecting a computer or network is to spot the risks and get intimate with the terminologies associated with them.The method of analyzing data from networks and information systems to settle if a security breach or security violation has taken place [2].

II. DATA MINING

Data mining (the analysis step of the "Knowledge Discovery in Databases" process, or KDD) [3], is a field of computer science, which involves identifying patterns from massive data sets through methods of artificial intelligence, machine learning, statistics, and database systems [34]. Apart from fundamental analysis, the data mining process covers database and data management aspects, data pre-processing, inference considerations, complexity considerations, post - processing of discovered structures, and online updating.

Roots of Data Mining [2] are statistics, Artificial Intelligence & Machine Learning, Databases, Pattern discovery, visualization, business Intelligence, etc. The various Data mining techniques are listed in the below figure.

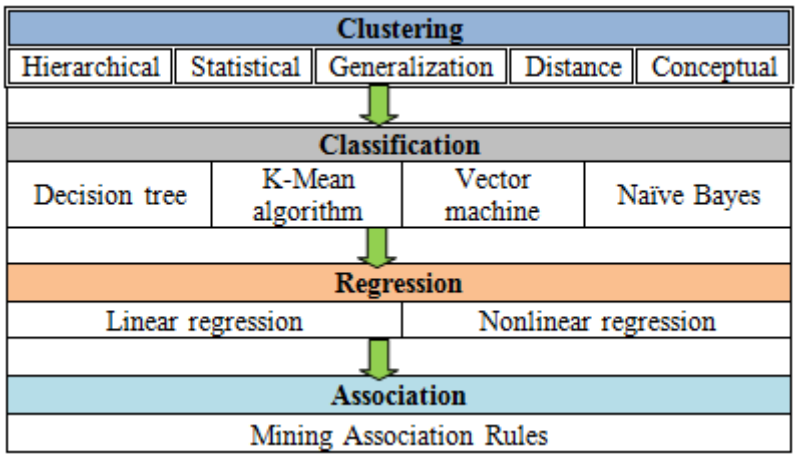


Fig No: 2. various types of data mining techniques

- **Clustering** –It is the job of discovering groups and structures in the data exclusive of using known structures in the data.
- **Classification** –It is the task of generalizing known structure which can be applied to new data.
- **Regression** -Attempts to find a function which models the data with the least error.
- **Association Rule Learning** -Searches for relationships between variables.

III. CONTRIBUTIONS

The inputs of this work are:

1. Enhanced security: Our Multi-level security method generates field level security (FLS) and Record level Security (RLS) by using the Cyber-physical system via data driven bit selection procedure. It can resist any level, frequency-based cryptanalysis attack.

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 7, Issue 1, pp: (105-111), Month: January - March 2019, Available at: www.researchpublish.com

2. Top data preserving: After implementation of FLS & RLS, the resulting ciphertext is transformed to the nearest neighbour data cluster with references to data mining [4] that maintains a high degree of accuracy.

3. The empirical evaluation: We perform the evaluation of multilevel security strategy with several computing approaches using real time dataset received from the CPS of a pharmaceutical system.

4. Clustering analysis plays an important role in scientific research and commercial application.

5. Naive Bayes algorithm is used for classification of our data.

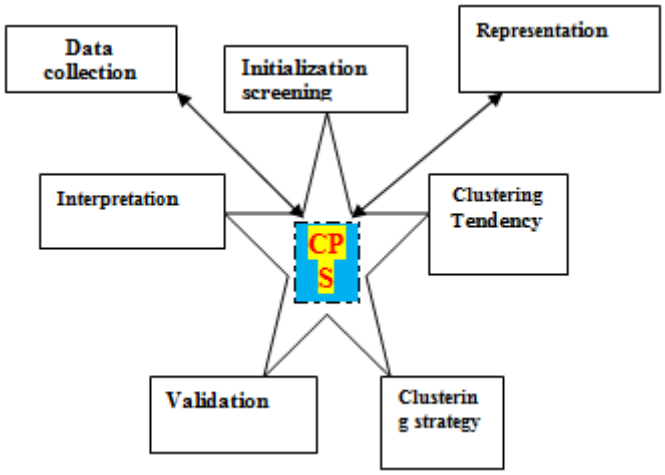
IV. ORGANISATION

Section II introduces the data mining concepts and techniques like clustering, classification, regression and Association used in this research. In the next section III, we described the contributions and objects of the research. Section V deals with background clustering and functions which are executed by the CPS. In the last section, we are highlighting the conclusion and the future scope of this research.

V. BACKGROUND

Cluster Analysis: Clustering analysis is an important technique in the exponentially growing field and is known as exploratory data analysis and is being functional in the variety of areas in the engineering. It organizes the data by analyzing a group of individuals or hierarchy of groups. Clusters are comprised of some objects that are collected and grouped together.

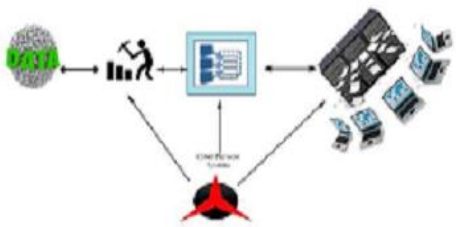
We used this tool to identify the related entities in the database, after that the data set is again classified into fields and records[8]. The data clustering methodology is revealed in figure 2.



Rafael Etges, Karen McNeil, described -The process of identifying and categorizing the information is more important than the specific control requirements shown in the example below. Different organizations will select different sets of control elements based on their perspective of business processes and priorities and alignment with industry standards such as ISO 17799 [6]

VI. PROPOSED WORK

The goal of this project was to design a model for a secure cyber-physical system. The chosen approach was that of a hierarchical type of system, where users would have access to information based on their degree of access [7]



ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 7, Issue 1, pp: (105-111), Month: January - March 2019, Available at: www.researchpublish.com

Field Level Security (FLS): Many industrial sectors have sensitive data that should be controlled by only certain users. There are various fields in them like branch/entrepreneur address, name, surname, , transaction details, etc. With field level security, we can restrict access to custom fields and now other fields.

For example, administrator (CPS) can enable the account number field to be a view but not changeable for members of the supervisory team [15]. FLS will now be available to work off of system fields. Previously this was only available for Custom Fields [35]. The Hierarchical Security model does grant extra permissions based on users, administrators, and positions.

Read Access: Propagates up the chain to a particular configurable level .

Write, Update, Append To: This has been granted just to the direct parent of the user/positions

Here, there are also some performance considerations to keep in mind when enabling the hierarchy security:

- Use with other security methods for more complex scenarios. E.g., security roles, business units, teams, etc.
- Target 4 levels of hierarchy, i.e. one network with three financial institutions, and one to two lack potential users underneath.
- The security performance is studied on the number of users.

Record Level Security: It is a quality of Authentication. It allows you to restrict access to records based on the current user's profile data. With record level security [36], we can allow access based on

- Records that were created by the current user.
- Records that were assigned to them personally.
- Malicious users access no other records. CPS identifies the malicious and unauthenticated users.

Alternatively, you can also restrict record access based on an individual's department or group. Record level security can also be used to reduce the number of visible options in dropdown fields and list boxes [36].

The information or data are denoted by D, which will encrypt under the cluster x, the resultant data $C = E\ (D, x)$. Here E has encrypted data in the location. $-\tau$ the current timestamp is attached to the encoded message in that particular location. Now the $C = E\ (D, \tau, x,)$.

The information is classified into different clusters like public, private, confidential and high confidential. Each clustered data is located and stored in a unique address. By using cryptanalysis technique even we encrypted the location of that particular address. It is one part of the security which is the part of a multi-level security system.

Let D is the dataset in the storage location $\{d_1, d_2, d_3, d_4 \ldots .d_n\}$,
$C_1, C_2, C_3, \ldots .C_n$ are the trained classes,

D class is determined with (D,t)

$C_n = \{C_1, C_2, C_3, C_4 \ldots \ldots .C_N\}$

$D_n = \{d_1, d2, d3, d4 \ldots .d_n\}$

Each item in D_n should map to at least one class in C_n

$d_i \in c_n, \forall$;

i is the scalable and relative attribute

$\forall$ C in $\{ C_1, C_2, C_3, C_4 \}$

$\forall$ D is the finate object

$d_i \in c_n \Rightarrow N_i \in d_i$

Ni → New version of d_i;

$\forall N_i \cong d_i$

D = {a,b,c,d,e}

C= { class1,class2, class3,class4}

Classify each d_i in C

i.e f(n) = f(d) % f(c)

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 7, Issue 1, pp: (105-111), Month: January - March 2019, Available at: www.researchpublish.com

for each c value d is defined for 'n '

we stated the classification of the data into various data sets like fields and records with an example

D	C
{a,d}	Class 1
{d}	Class 2
{c}	Class 3
{e}	Class 4

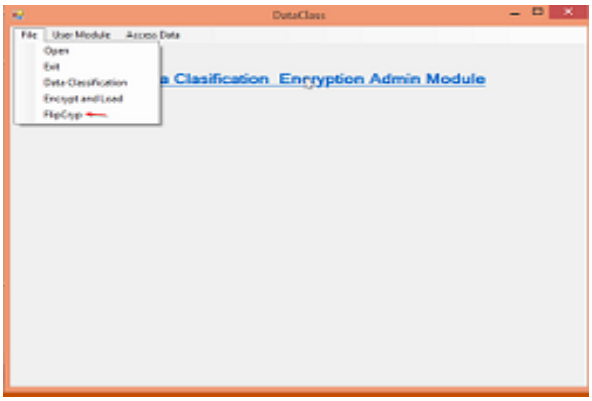
$\Rightarrow d_i \in C$
$\forall$ i values

Hence, $d \in C \Rightarrow Ni \in C$,
Derive N_i value for each d_i

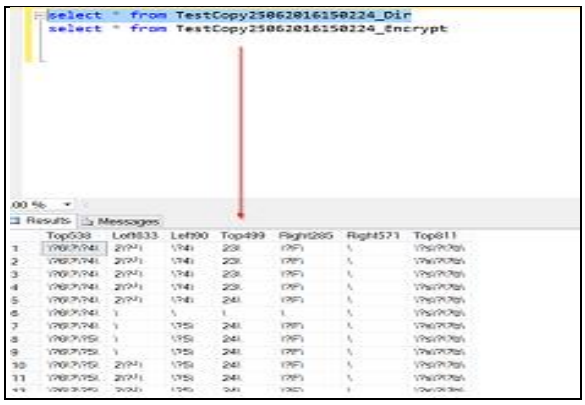
D	C	N
a,d	Class 1	X,Y
b	Class 2	T
c	Class 3	P
e	Class 4	J

$\Rightarrow$ f(n) = f(D) % f(c)
*F(c) is random Selection

The below figure representing the main console of the classification of data in various levels like public, private, confidential and high confidential of records and files



The encoded message of the information after applying Cryp key and Flip key in data mining



After implementation of SMC (Secure multilevel Classifier) for each and every field and record of information, we stated encrypt the data by using the flip key and Cryp key with variable key length. Time taken for Encryption and Decryption is 0.65 and 2.5 milliseconds when the number of bytes is 1024, and key size is 512 bits is

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 7, Issue 1, pp: (105-111), Month: January - March 2019, Available at: www.researchpublish.com

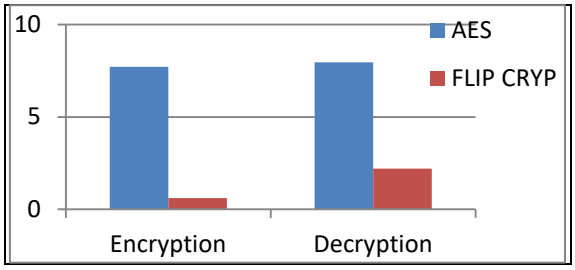
	Encryption
Size of data in bytes	1024
Key length in bits	512
Time in Milliseconds	0.6541
	Decryption
Size of data in bytes	1024
Key length in bits	512
Time in MilliSeconds	2.5404

With the sample of data size with 1024 bytes, we have examined the time taken for Encryption and Decryption when the number of bytes is 1024, and key size 256 bits.

ENCRYPTION	
Size of data in bytes	1024
Key length in bits	256
Time in Milliseconds	0.60242
DECRYPTION	
Size of data in bytes	1024
Key length in bits	256
Time in Milliseconds	2.1203

Time Comparison of Flip Crypt Algorithm and AES algorithm when the data size is 1024 bytes and bit size is 256 bits

Algorithm	Encryption	Decryption
AES	7.712	7.654
FLIPCRYP	0.60242	2.1203



VII. CONCLUSION & FUTURE SCOPE

In this work, the multi-level security is provided with the administrative control of the cyber-physical system by using data mining and secure cryptographic algorithm called flip key and Cryp key . Finally, we examined the high performance regarding classification of data as well as time reduction in encryption and decryption when compared to existing cryptographic algorithms. In future, we may extend this work by machine learning process, completely with CPS for a huge amount of data with infinite number of key length.

REFERENCES

[1] P.Agarwal, Chaturvedi,"Application of Data Mining Techniques for Information Security in a Cloud: A Survey "International Journal of Computer Applications (0975–8887) Volume 80 – No 13, October 2011.

[2] http://www.chistera.eu/sites/chistera.eu/files/Announcement.pdf

[3] www.kpk.gov.pl/wpcontent/uploads/2014/05/chistera_call_2014_topics_flyer.pdf

[4] Mrs. Sharada Mangipudi, J. Vijay Gopal, Dr. P. Suresh Verma, Dr. M.Srinivasa Rao "Developing Multi-Level Security System Using Esp Technique By An Advanced Data Mining Concepts,". Abbrev., in press.

[5] http://www.indiastat.com/banksandfinancialinstitutions/3/publicsectorbanks/234/stats.aspx

[6] Laura Vegh, Liviu Maclean et al. "Enhancing Security in Cyber-Physical Systems Through Cryptographic and Steganographic Techniques" 2014 IEEE

[7] Anil K Jain, Richard C. Dubes, " Algorithm for Clustering data" Prentice Hall, Eaglewood Cliffs, New Jersey 07632.

[8] http://rbidocs.rbi.org.in/rdocs/Publications/PDFs/APB30091213F.pdf

[9] http://www.tcs.com/sitecollectiondocuments/case%20studies/bancs_case_sbi.pdf

[10] 11.https://www.irda.gov.in/ADMINCMS/cms/frmGeneral

[11] http://www.census.gov/data/developers/datasets/population estimates-and-projections.html

[12] *Ron S. Jarmin, Thomas A. Louis et al.*" Synthetic Data: Public-Use Micro Data for a Big Data World", October 14, 2014.

[13] .http://www.columbusglobal.com/en/Shared/Technology/US_technology/media/09616A1A0E01433CB9C2FFB12233851C.pdf

[14] Okman, L., Gal-Oz, N., Gonen, Y., Gudes, E., Abramo, J.: Security issues in NoSQL databases, http://jmiller. uaa.alaska.edu/csce465fall2013/papers/okman2011.pdf

[15] MongoDBOverview,http://www.mongodb.com/mo ngodb.overview

[16] Lane, A.: Securing big data-Security recommendations for Hadoop and NoSqlenvironment,https://securosis.com/ assets/library/reports/SecuringBigData_FINAL.pdf

[17] Bhatewara, A., Waghmare, K.: Improving network scalability using NoSQL database. IJACR (December 2012)

[18] http://public.dhe.ibm.com/common/ssi/ecm/en/nib03019usen/NIB03019USEN.PDF

[19] http://www.infoq.com/articles/nosql-data-security-virtual-panel

[20] Kaur, H., Kaur, J., Kaur, K.: A review of non-relational databases, their types, advantages, and disadvantages. IJERT (February 2013)

[21] http://blog.spiderlabs.com/2013/03/mongodb-security-weaknesses-in-a-typical-nosql-database.html

[22] https://help.ubuntu.com/community/kerberos

[23] http://docs.mongodb.org/manual/tutorial/control-access-mongodb-with-kerberos-authentication

[24] http://docs.monggodb.org/ecosystem/tutorial/authenticate-with-java-driver

[25] Kerberos- community help wiki, https://help.ubuntu.com/community/kerberos

[26] http://en.wikipedia.org/wiki/MongoDB

[27] Lakshman, A., Malik, P.: Cassandra: a decentralized structured storage system. SIGOPS Open. Syst. Rev. 44, 35–40 (2010), http://doi.acm.org/10.1145/1773912.1773927 CrossRef

[28] http://securosis.com/blog/nosql-and-nosecurity

[29] MongoDB, Official website, http://www.mongodb.org

[30] http://IBMpublic.dhe.ibm.com/common/ssi/ecm/en/NIB03019USEN.PDF

[31] Neuman, B.C.: Kerberos: an authentication service for computer networks. Inf. Sci. Inst., Univ. of Southern California, Marina del Rey, CA, USA

[32] http://www.centos.org/docs/5/html/ /chkerberos.html

[33] www. Caspio.com/authentications and connections /authentication /record-level-security.

[34] Preeti Agarwal et al. "Application of Data Mining Techniques for Information Security in a Cloud: A Survey", http://research.ijcaonline.org/volume80/number13/pxc3891804.pdf

[35] http://community.dynamics.com/crm/b/sonomapartners/archive/2014/10/01/dynamics-crm-2015-hierarchical-security

[36] http:caspio.com/authentications-and-connections/authentication/record-level-security