isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6 Issue: 3 Mar,2021,ISSN_NO: 2321-3337

Endorsement Guideline Protocol Actuality Problem

Mr.M.Selvam,M.E., Ph.D., Professor of Computer Science Department,
Mr.K.Ajith, Student of Computer Science Department,
Mr.C.Joy Jayanth Swaraj, Student of Computer Science Department,
Mr.A.Meenakshi sundaram, Student of Computer Science Department,
St. Joseph College of Engineering, Sriperumbudur, Chennai

Abstract

Access control is a fundamental aspect of the security of any multi-user computing system, and is typically based on the specification and enforcement of an authorization policy. Such a policy identifies which interactions between users and resources are to be allowed by the system. Over the last twenty years, authorization policies have become more complex, not least because of the introduction of constraints, which further refine an authorization policy. A separation-of-duty constraint also known as the two man rule or four-eyes policy may, for example, require that no single user is authorized for some particularly. sensitive group of resources. Such a constraint is typically used to prevent misuse of the system by a single user. The use of authorization policies and constraints, by design, limits which users may access resources. Nevertheless, the ability to perform one's duties requires access to particular resources, and overly prescriptive policies and constraints may mean that some resources are inaccessible. In short, tension may exist between authorization policies and operational demands: too lax a policy may suit organizational demands but lead to security violations; whereas too restrictive policy may compromise an organization's ability to meet its business objectives.

1. Introduction

Secure computing is a forward looking, highly sophisticated and secure distributed record keeping system which will help in the storage and analysis of large amount of documents database which can be traced down to all workers. The system would include all the entry and exit records documents involved in the and hence accord transparent The model is based on consensus and hence all the documents will have to be validated and approved of, by all the members of the group before it goes to contractor.The main purpose scope of the project is ONGC is the one of the leading corporation of india so the process is maintained highly secured only the authorised login only can access the documents and project .The concept of secure computing has taken the fancy of a lot of people and the technology became famous because of one of its most popular use cases.

Literature Survey

Pierre Berge,Jason Crompton [1] proposed The Authorization Policy Existency Problem. This paper is Access control is a fundamental aspect of the security of any multiuser computer system and is typically based on specifications and enforcement of an authorization policy.Such a policies identifies which interacts between user and resources are to be allowed by the system.Access control requirements have become increasing complex,leading to increasing sophisticated authorization policy often express in a term of constraints

Dr.U.M.Gokhale,D.Bajaj [2] proposed AES Algorithm for Encryption. Cryptography operation in wireless device which uses little memeory and a low power processor causes system overhead thereby implementing security hardware dedicated to cryptography neccessry now a days.Encryption is technique which convert data or information into code which is unreadable.in 2021,advance encryption standard is a symmetric block cipher that operated on 128 bit block as input and output data.The algorithm can encrypt as well as block using a secret key which has a key size of 256,192 or 128 bits.AES is simplicity that is achieved by repeatedly combining substitution and permutation computation at different rounds.

Parasoon Raghav,Rajad Parashar [3] proposed Security Data in Cloud using AES algorithm. The quickly growing variety of wireless communication users has lead to increase in demand for security measures and device to guard user information transmitted over wireless channel.Two kind of cryptological system developed for the symmetric and asymmetric cryptosystem,Symmetry cryptography likes AES,DES and asymmetric likes with a RSA uses completely different key for encoding and decoding, eliminating key exchange drawback.symmetric cryptography is more appropriate for the encoding of and outsized amount of information the AES algorithm can be symmetric block cypher that process data blocks of 128bit employing a cipher key of length 128bits

Parasoon Raghav,Rajad Parashar [4] proposed Security Data in Cloud using AES algorithm**.**The quickly growing variety of wireless communication users has lead to increase in demand for security measures and device to guard user information transmitted over wireless channel.Two kind ofcryptological system developed for the symmetric and asymmetric cryptosystem,Symmetry cryptography likes AES,DES and asymmetric likes with a RSA uses completely different key for encoding and decoding,eliminating key exchange drawback.symmetric cryptography is more appropriate for the encoding of and outsized amount of information the AES algorithm can be symmetric block cypher that process data blocks of 128bit employing a cipher key of length 128bits.

System Design

Secure computing is a forward looking, highly sophisticated and secure distributed record keeping system which will help in the storage and analysis of large amount of documents database which can be traced down to all workers. The system would include all the entry and exit records documents involved in the and hence accord transparent The model is based on consensus and hence all the documents will have to be validated and approved of, by all the members of the group before it goes to contractor. The main purpose scope of the project is ONGC is the one of the leading corporation of india so the process is maintained highly secured only the authorised login only can access the documents and project .The concept of secure computing has taken the fancy of a lot of people and the technology became famous because of one of its most popular use cases.

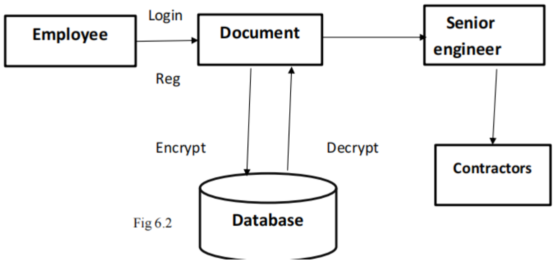
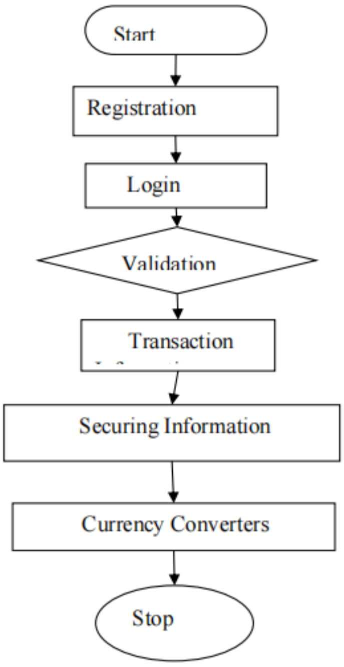


Fig 6.2

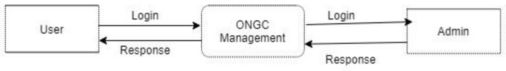
The client-side application is developed for three entities, namely admin, driver and passenger. The admin has complete control of the data flow between server and client.



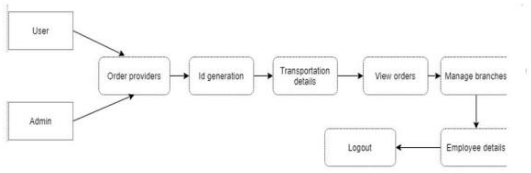
A data flow diagram is a graphical tool used to describe and analyze the

movement of data through a system. These are the central tool and the basis from which the other components are developed. These are known as the logical data flow diagrams. The physical data flow diagrams show the actual implements and movement of data between people, departments and workstations.Using two familiar notations Yourdon, Gane and Sarson notation develops the data flow diagrams.

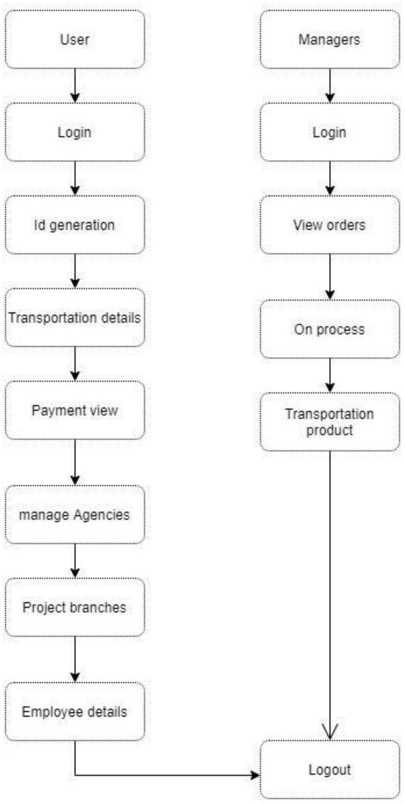
LEVEL 0



LEVEL 1



LEVEL 2



Implementation

- AES is based on symmetric algorithm and work with 128 bit keys.
- AES works only with 128 bit key i.e secret key should be less than 16 symbols.
- AES is able to encrypt anything which consists of bytes
- types of files does not matter.

symmetry key algorithm

```
void generate symmetric key(byte [16]key)
{
    byte row index,coloumn index;
    byte shift count =get shiftcount(key);
    byte [ ]symmetry key =generate primary key();
    for (i=0;i<16,i++)
    {
        get properindex (key [i].outrow index,outcoloumn index);
        shift row (row index,shift count);
        shift coloumn(coloumn index,shift count);
        swap (rowindex,coloumn index);
    }
}
```

manage.py

```
importos
importsys
if__name__=="__main__":
os.environ.setdefault("DJANGO_SETT
INGS_MODULE",
"authorization_policy.settings")
    try:
        fromdjango.core.management
importexecute_from_command_line
    exceptImportError as exc:
        raiseImportError(
            "Couldn't import Django.
Are you sure it's installed and "
            "availableonyour
PYTHONPATH
environment variable? Didyou"
            "forget to activate a v"
            "irtual environment?"
        )fromexc

execute_from_command_line(sys.argv)
```

emailsettings.py

```
SET_EMAIL_USE_TLS=True
SET_EMAIL_HOST='smtp.gmail.com'
SET_EMAIL_HOST_USER='cloudauthenti
cate@gmail.com'
SET_EMAIL_HOST_PASSWORD='cloudau
thenticate12'
SET_EMAIL_PORT=587
SET_EMAIL_BACKEND=
'django.core.mail.backends.smtp.Email
Backend'
SET_DEFAULT_FROM_EMAIL=
'cloudauthenticate@gmail.com'
```

wsgi.py

```
  importos
  fromdjango.core.wsgiimport
get_wsgi_application
os.environ.setdefault("DJANGO_SETT
INGS_MODULE",
"authorization_policy.settings")
application = get_wsgi_application()
```

Conclusion and Future Enhancement

In this paper we have introduced a general framework within which we can specify problems concerned with finding authorization relations (“policies”) that must satisfy certain kinds of constraints. We have shown that there exist FPT algorithms to solve the authorization policy existence problem when all constraints are user-independent and are bounded in an appropriate way. We have also shown that many constraints of practical interest are indeed user independent and bounded. Our prior work on implementing FPT algorithms for We believe there are many opportunities for future work, not least exploring what types of authorization constraints might be useful in practice and determining whether those constraints are user-independent and bounded.

References

1.P.Berge,”The authorization policy existence problem “,iconf.Data Appl.secure,privacy,2017

2.J.Crampton ,”Resiliency policies in access control revisited”,in proc.21st ACM
symp.Access control Models Technol.,2016.

3.N.Li,Q.wang ,”Resiliency policies in access control”.ACM trans.inf.syst.,2009

4.Q.Wang ,”Satisifiability and resiliency workflow in authorization system”,ACM trans.inf.syst.secure.,No.4,2010.

5.A.Bjorkhand,”Set partitioning via inclusion-exclusion ,”SIAM J.compute,2019.

6.Gregory gutin,”Authorization policy existence problem,IEEE paper,2016.

7 .U.M.Gokhale,”AES Algorithm for encryption”,IEEE PAPER,2016.

8.Prasoon Raghav,Rajat Parashar “Securing data in cloud using AES algorithm”,IEEE,2016.

9.Bih-Hwang Lee Data security in cloud computing using AES under HEROKU cloud,IEEE PAPER,2016

10.Jason crampton,"The authorization policy existence problem",IEEE PAPER,2018.