**Major Project Synopsis**

***on***

**TITLE OF PROJECT**

***In partial fulfillment of requirements for the degree***

***of***

**BACHELOR OF TECHNOLOGY**

**IN**

**COMPUTER SCIENCE & ENGINEERING**

***Submitted by:***

SNEHIL JAIN [16010BTCS00435]

GOVINDA RATHI [16010BTCS00456]

LEENA JOSHI [1601DMTCS00850]

***Under the guidance of***

PROF. NAME



**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**

**SHRI VAISHNAV INSTITUTE OF INFORMATION TECHNOLOGY**

**SHRI VAISHNAV VIDYAPEETH VISHWAVIDYALAYA, INDORE**

**JULY-DEC 2019**

**SHRI VAISHNAV INSTITUTE OF INFORMATION TECHNOLOGY**

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**

**GUIDELINES FOR MINOR PROJECT SYNOPSIS**

**Abstract (250 Words Approx.)** < Times New Roman, 12, Bold >

    The synopsis must begin with an abstract of 250 words. The abstract must clearly indicate the idea of the proposed work, suggested solution framework and significance of your work. < **Times New Roman, 12, Normal**>

1. **INTRODUCTION (250 Words Approx.)**< Times New Roman, 12, Bold >

    This section should provide the concept and overview of the domain of proposed work   giving the references of work being in the field under same context. < Times New Roman, 12, Normal >

2. **PROBLEM DOMAIN** (150 Words Approx.) < Times New Roman, 12, Bold >

    This section should indicate problem and explain clearly “What exactly is the problem. Also enlist the objectives of the proposed work. < Times New Roman, 12, Normal >

3. **SOLUTION DOMAIN** (300 Words Approx.)  < Times New Roman, 12, Bold >

    This section should provide the description of the proposed solution e.g. requirement, techniques, algorithms, schema, architecture, design, plan, framework (whatever is applicable) explained in a cogent manner. < Times New Roman, 12, Normal >

4. **SYSTEM DOMAIN** (150 Words Approx.) < Times New Roman, 12, Bold >

     This section describes the tools, technology, environment, platform and hardware/software specifications needed for implementing the proposed idea. Proper justification for the choice of any of the systems elements must also be given in these section. < Times New Roman, 12, Normal >

5. **APPLICATION DOMAIN** (100 Words Approx.) < Times New Roman, 12, Bold >

     This section must provide scope of the work. Where it is applicable. It should also depict the variants if any and impact of the work on real life / end user.

6. **EXPECTED OUTCOME** (70 Words Approx.)  < Times New Roman, 12, Bold >

     A point wise description of expected outcome must be given here. A list shall be preferred. < Times New Roman, 12, Normal >

7. **REFERENCES**< Times New Roman, 12, Bold>

**ABSTRACT**

Currently, data security and privacy policy has been regarded as one of the biggest concerns in cloud computing. Data stored at remote storage is unsafe and susceptible to get hacked. Due to this, users do not trust their data over the cloud. Cloud consumers wants an assurance that they can access their data where ever they want and no one else is able to get it. Moreover, authentication of users over the cloud is also an important concern to think about. After doing the survey and studying the research papers it is found that the major security concerns of cloud computing includes Data leakage, Distributed Denial of Service (DDOS). The data security can be improved by implementing various symmetric key algorithms so that data on the server is stored in a manner that even if a person gets access then also he can't open the original data. As it needs to be decrypted. Apart from storage security, authorised access of users enable may help in avoiding DDOS as only genuine users will have access to the cloud.

A hybrid model is proposed which is a mixture of elliptical curve cryptography and symmetric key algorithm. ECC is used to achieve the process of user's verification and to keep the private data secure. AES algorithm is used which allow the user to store and access their data securely to the cloud by encrypting the data in the client side and decrypting the data after downloading from the cloud. Since the private key is owned by the user of the data, no one can decrypt the data, even though the hacker can get the data through some approaches. Moreover, user will securely authenticate itself by using different input parameters at the time of login to the cloud server. This scheme can make users assure about the security of data stored in the cloud. Here, we will apply an ECC and ECDH algorithm that provide same level of security as of other public key crypto systems with less key size and strengthens the security of the algorithm. The whole prototype of the proposed solution would benefit by enabling a proper access mechanism to avoid unauthorised access to the information system and a secure storage to allow access of data over the cloud network.

**Introduction**

After doing the survey and studying the research papers it is found that the major security concerns of cloud computing includes Data leakage, Distributed Denial of Service (DDOS). The data security can be improved by implementing various symmetric key algorithms so that data on the server is stored in a manner that even if a person gets access then also he can't open the original data. As it needs to be decrypted. Apart from storage security, authorised access of users enable may help in avoiding DDOS as only genuine users will have access to the cloud.

**Problem Domain**

Need of data security is an essential issue in the domain of computing traditionally. There are various algorithms are developed in order to improve the security of data, but they having their own issues. Now in these days the traditional algorithms are not much suitable for providing security over the untrusted communications and data exchange.

ECC is more and more considered as an attractive public-key cryptosystem for mobile/wireless environments. One of the other recent public key cryptosystems is Elliptic Curves Cryptography use for security. In recent times, the majority of e-commerce applications are designed using asymmetric cryptography to assure the authentication of the concerned parties. Compared to traditional public-key cryptosystems like RSA or Diffie-Hellman, ECC propose equivalent security with smaller key sizes; these results in faster calculation, lower power expenditure, as well as memory and bandwidth savings. ECC is peculiarly useful for mobile devices, which are typically particular in terms of their CPU, power and network connectivity.

Therefore, a new encryption standard is required that can fulfil the current need of security meanwhile that is extendable according to the need. The proposed work includes the development of new hybrid algorithm using ECC, ECDH and AES algorithms along with encryption techniques.

**Solution Domain**

A hybrid model is proposed which is a mixture of elliptical curve cryptography and symmetric key algorithm. ECC is used to achieve the process of user's verification and to keep the private data secure. AES algorithm is used which allow the user to store and access their data securely to the cloud by encrypting the data in the client side and decrypting the data after downloading from the cloud. Since the private key is owned by the user of the data, no one can decrypt the data, even though the hacker can get the data through some approaches. Moreover, user will securely authenticate itself by using different input parameters at the time of login to the cloud server. This scheme can make users assure about the security of data stored in the cloud. Here, we will apply an ECC and ECDH algorithm that provide same level of security as of other public key crypto systems with less key size and strengthens the security of the algorithm.

Benefits are:

* Proper access mechanism to avoid unauthorized access to the information system.
* Secure storage and access of data over the cloud.

**System Domain**

**3.1 User Interface**

* Platform – Desktop or Mobile browser
* Display – 1024x768 or higher, 1366x768 recommended
* Latest Video and supported graphics drivers.

These are the basic UI requirements and nowadays almost every system has. So, there is not much of a problem for any user.

**3.2 Hardware Interface**

* Processor – i3/i5/i7 x64 Bit Minimum 2 Ghz.
* Hard Disk – 8 GB + at least 2 GB for Relational Database System
* Memory – 2 GB RAM minimum, 4 GB RAM recommended
* High Speed Internet Access
* LAN Connection with Ethernet.

Again these requirements are basic ones but LAN connectivity should be there for better user experience.

**3.3 Software Interface**

* Linux / Windows OS
* JDK 7 or above
* NetBeans IDE
* Relational Database Server, MYSQL Preferred
* Apache Tomcat Server

**APPLICATION DOMAIN**

The Project simulates a model that is already quite common for consumer apps like email and photo sharing, and for certain business applications. But in this project, we used different compression and encryption algorithms to secure the data. We also hide its whereabouts from the users that stores and retrieves it. As with the Internet, on-demand applications have grown so ordinary that most of the business user interacts with at least one, whether it's an email service, a Web conferencing application, or a file hosting system. The data is kept at multiple places over the data house (over the Internet). It sounds almost like file hosting websites that stores the info that's being uploaded by completely different users and may be retrieved using correct authentication. The only difference is that the system for which project is targeted is an application based system like which will run on the clients own system. This application will allow users to upload file of different formats with security features including Encryption and Compression over the cloud securely.

The uploaded files are accessed from anyplace using the application that is provided. we tend to believe this method is a foundation for future work in integrating and securing data sources across the world Wide web.

**EXPECTED OUTCOME**

* Proper access mechanism to avoid unauthorised access to the information system.
* Secure storage and access of data over the cloud.
* The uploaded files can be accessed from anywhere using the application which is provided.
* Form validation so that only real users access the system. An error message should be displayed in case of improper working of the application.
* The application can take any number of users provided the database size is large enough.

**REFERENCES**

1. Qin Liu, Guojun Wang, and Jie Wu “Efficient Sharing of Secure Cloud Storage Services” 2010 .10th IEEE International Conference on Computer and Information Technology (CIT - 2010).
2. Uma Somani, Kanika Lakhani, Manish Mundra “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing” 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).
3. Ashutosh Kumar Dubey 1, Animesh Kumar Dubey 2, Mayank Namdev3, Shiv Shakti Shrivastava4 “Cloud-User Security Based on R SA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment “in 2011.
4. Xiang Tana, Bo Aib “The Issues of Cloud Computing Security in High-speed Railway “in 2011.
5. Arthur Rahumed, Henry C. H. Chen, Yang Tang, Patrick P. C. Lee, and John C. S. Lui “A Secure Cloud Backup System with Assured Deletion and Version Control” 2011 International Conference on Parallel Processing Workshops.
6. Eman M. Mohamed and Sherif EI-Etriby “Randomness Testing of Modem Encryption Techniques in Cloud Environment” in year 2008.