CONSTITUENCY LEVEL DEVELOPMENT MONITORING SYSTEM (CLDMS) WITH SECURE AUTHENTICATION IN CLOUD

[1] Roopa Priyanka Konaru, [2] G.V.Hindhumati, [3] Srinivasa Subbarao Akella
[1] M.Tech,Final year student, [2] Assistant Professor, [3] Technical Director(NIC)
[1] Department of Computer Science and Engineering (CSE)
[1] Gayatri Vidya Parishad College of Engineering, Visakhapatnam, India

Abstract : Data security has become a major concern in the virtual world today .User authentication, data security and data maintenance are the major issues which needs to be handled thoroughly. Earlier authentication is done based on passwords, there after many algorithms came into existence for securing these passwords and data. With the emerging technologies and increase in computational power, algorithms are being broken easily. Recent algorithms like Rivest, Shamir, and Adelman (RSA) are getting diluted. To yield a high level security with smaller key sizes, this paper underlines a double authentication method using One Time Password (OTP) and Elliptic curve cryptography (ECC) encryption where ECC is used for both authentication and confidentiality. Maintaining large amounts of data on traditional servers requires high investments and maintenance costs due to which most of the data is being migrated from traditional servers to cloud storage services. The main objective of this paper is to handle security threats during authentication using ECC and deploy the entire application in cloud server.

Keywords - Double Authentication, Elliptic Curve Cryptography, Cloud Storage

I.INTRODUCTION

CLDMS service aims to cover elected representatives like Members of Legislative Assembly and Members of Legislative Council representing Telangana state.Each user will login with their respective identities, and update their fund status, work proposals etc according to the tasks given by the government. Tasks are periodically monitored by the Executive Agencies. In addition it facilitates the user to get various sorts of reports needed by the District Administration, for conducting review meetings at District level and to generate the reports instantly to send progress reports to the Government. The CLDMS project helps the target groups to login through front end and enter the work status periodically given by the government. The data entered is stored in the back end server which is monitored by the Executive Agencies and retrieved whenever required. The work proposals can be edited, updated etc. As the application consists of sensitive and larger chunks of data it has to secured and maintained with at most accuracy. This is achieved by using various parameters like strong encryption algorithm like ECC, Dual authentication mechanism, cloud services.

II.LITERATURE REVIEW

Web applications in general secures the data using conventional RSA algorithm and maintains the data in servers which requires high capital investment ,leads to high maintenance costs when dealing with large set of data, which may be susceptible to data loss during disastrous situations. The CLDMS application mainly aims at auditing the money transactions of the target groups(MP's, MLA's), as the transactions contain sensitive information it has to be handled carefully in order to know whether the funds are used accurately. We need a high level security algorithm to handle the transactions accurately.

2.1 Cloud- Aware Web Service Security

Cloud services consume large amounts of data, many of them personal. Yet, the topics like data security, privacy are not satisfying covered. In this regard, Data security is of vital concern. Personal data has to be managed according to user's requirements and free from privacy violations Predominantly usage control and data leakage prevention are open problems. Trusted Platform as a Service Cloud architecture which address all the data security and privacy threats is needed. Services that consume personal data are to be hosted where it guarantees to handle data according to user's requirements, while inspecting and instrumenting services before uploading data to a cloud node to ensuring appropriate access control enforcement at runtime is required. Moreover, it will also ensures the trustworthiness of the node the services are deployed to. Last but not least, a security analysis attests the coverage of all threats and a prototype shows the feasibility of the implementations.

III.RELATED WORK

Cloud computing technology is seen because the assortment of web primarily based services for higher utilization of the resources and services. It's the new utility that provides virtualization, parallel and distributed computing into single unit. It implies the sharing of resources to handle applications which reduces capital and low maintenance price. It offers magnified quantifiable and easy access feature with low quality. There can be three main ways in which cloud services are utilized; they are Software as a Service (SaaS), Platform as a Service(PaaS) and Infrastructure as a Service (IaaS). These services can be deployed by Private, Public, Hybrid or Community cloud. The data present in the cloud is easily susceptible to many kind of attacks. The data which is present in the cloud should not get served to any user without knowing the user details, the user is eligible to access this data or not has to be known primarily, hence this gives rise to the strong authentication requirement for cloud based resource. Even if the authentication requirement is matched then there should be some mechanism which should take care access rights of the users, hence this gives rise to develop the access control mechanism which should take care whether the resource is being accessed to proper

user or not, or in short we can say "Who can access what". In order to highly secure the data RSA algorithm is used for encryption to make complete communication secure and encrypted by converting all the plain text information into cipher text information by using 2048-bit size key and MD5 algorithm is basically used for authentication purpose.

3.1 Drawbacks of Existing system:

- Traditional servers requires a capital investment in hardware and infrastructure.
- Servers are more susceptible to data loss during disaster situations.
- Servers will not have guaranteed uptime or recovery time.
- RSA algorithm requires more computer power supply compared to single key encryption.
- In this cryptosystem, if the private key is lost then all received message cannot be decrypted.
- RSA key sizes are too large and calculation time is long.
- Very slow key generation.

IV.DESIGN AND IMPLEMENTATION

4.1Design:

The figure 4.1 represents user's interaction with the system and depicts the specifications of the application. The figure portrays different types of users (MLA's, MP's) and their various ways of interaction with the system for

- User Registration(Using ECC user password is secured)-
  User has to register first by giving their personal details like member code, to which constituency they belong, password, contact number, mail id, address, their designation.
- Login(User Verification, OTP Generation)-
  User has to login with the registered username, password, generated captcha. On submission OTP is sent to mail for authentication purpose.
- Admin granting Funds-
  Admin will allocate funds from the government, total works to be done for each and every user.
- Services like uploading data-
  The users will update the status of their works like scheme fund, progress amount, not started work amount, completed works amount, balance
- Viewing reports-
  Users can view all the reports based on the access permissions and know the status of the works periodically
- Logout-
  After all the actions, finally user will successfully logs out of the application.

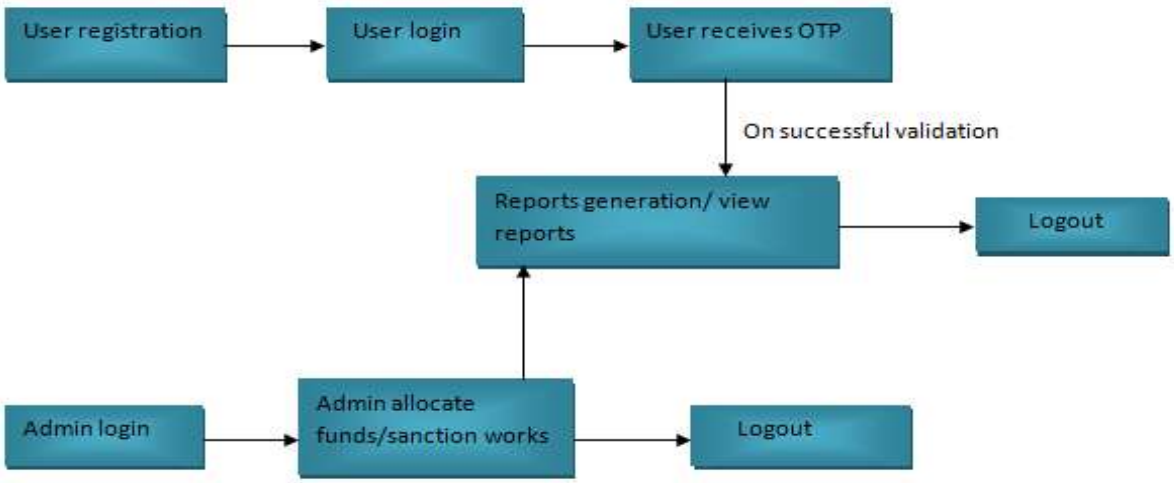


Figure 4.1: Overview of CLDMS Application

Table 4.1 : List of user roles and assigned privileges

User role	**Privileged services**
User(MLA,MP)	Login
	Upload data
	View data
	Update password
	Logout

Admin	Admin login
	Allocate funds to user
	Sanction works to user
	Admin logout

4.2 IMPLEMENTATION:

4.2.1 An Innovative Approach for Dynamic Authentication in Public Cloud: Using ECC Improved OTP

The cloud computing stage gives populace the chance for sharing information resources and services along with the people through internet. In the cloud computing system, both application software and databases are moved to the large data centers, where the data is not secure in the hands of providers. IT organizations have exhibited concerns about the various security aspects that exist with the widespread implementation of cloud computing. These type of concerns come from the fact that data which is stored remotely on the customer's location.

In general, for the customers the major concern which acts as a roadblock for adoption of cloud services was privacy protection and data security in cloud computing This paper gives the magnification for the already existing data security model in cloud environment. The proposed data security model advances user authentication and data protection. This makes secure communication system by hiding information from others. This model also includes onetime password (OTP) system for user authentication process.

Though cloud computing has vivid anticipations for both researchers and business, there are some demanding issues like performance, scalability, security, reliability, virtualization , interoperability etc needs to be addressed in particular. We describe the security issues related to the cloud computing; help to better understand the protocols and the principles behind it thus make better integrity and authentication. In this paper we have projected a novel security formation for cloud computing environment which comprises ECC and OTP. The ECC is used for file encryption system and authentication , ECC system is used for secure communication, Onetime password (OTP) along with ECC i.e; *Double Authentication* is used to validate users in cloud environment. This proposed model ensures authentication and security for the application by using algorithms like ECC and OTP makes the model highly secured. Unlike our Existing system RSA encryption is used which is obsolescence, the system uses ECC for both authentication purpose and encryption of data. In future we want to work with certifying protected communication system among users and systems and user to user.

Table 4.2: Algorithms used

Confidentiality	ECC
Authentication	1. User Id-Password Mechanism 2. Captcha Mechanism 3. OTP + ECC Based Authentication
Access Control Mechanism	Role Based Access Control

V.OUTPUT

5.1 Creating Azure account- In order to deploy the application into the cloud we need to first create an account in the cloud.

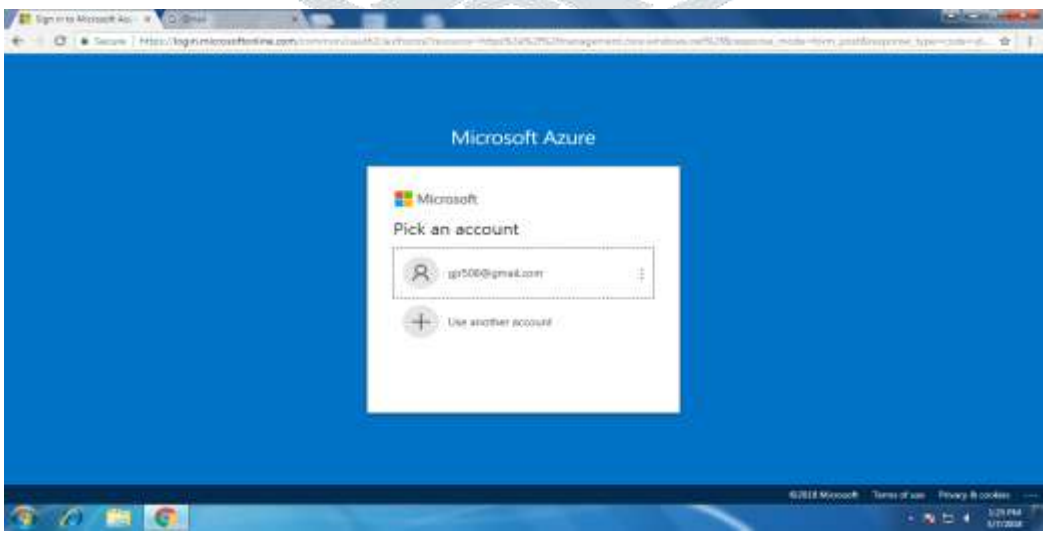


Figure 5.1: Creating Azure account

5.2 Creating instance- On successful login in to cloud account, we can see this page. To create a virtual instance, we need to click on the CREATE INSTANCE in the left menu.

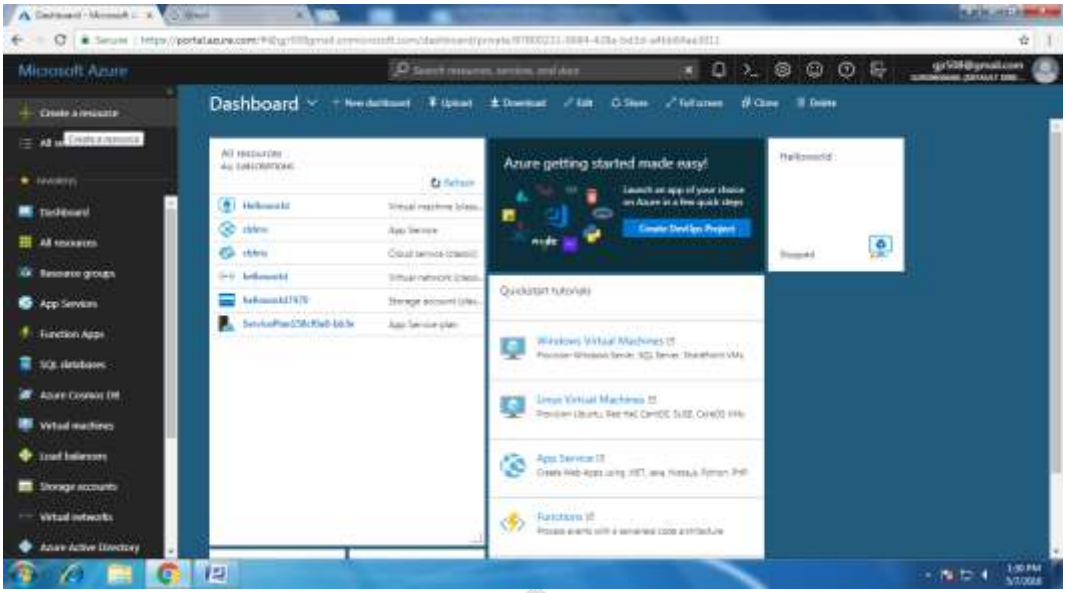


Figure 5.2: Creating instance

5.3 On successful deployment of application - After installation of Java, Tomcat, etc. applications is ready to run.

Figure 5.3: Application ready to Run

5.4 User registration - User has to register first by giving their personal details ,the password is secured using ECC and is stored in cloud .

Figure 5.4: User registration

5.5 User login - User has to login with the registered username, password, generated captcha.

Figure 5.5: User login

5.6 OTP Generation -. On submission OTP is sent to mail for authentication purpose.

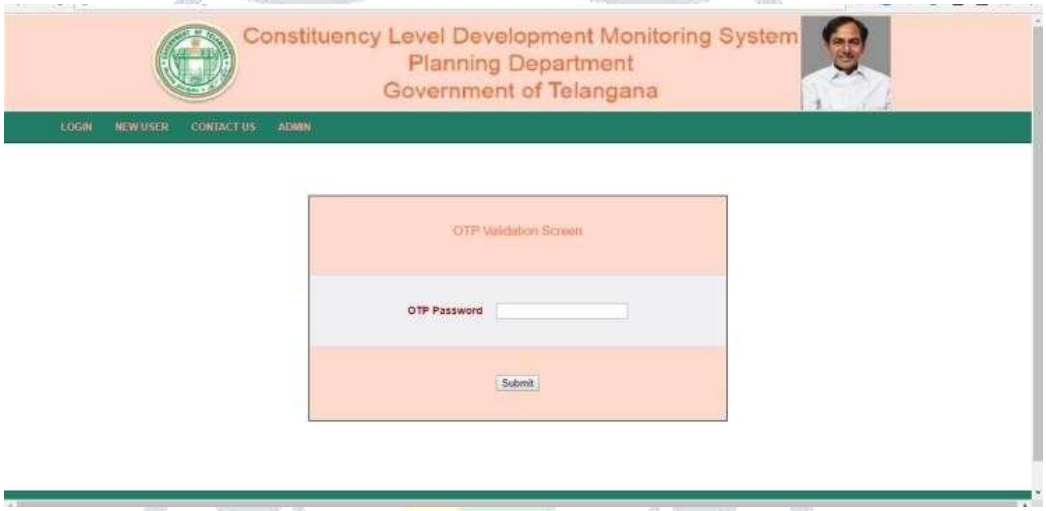


Figure 5.6: OTP Generation

5.7 Admin allocating funds - Admin will allocate funds from the government, total works to be done for each and every user.

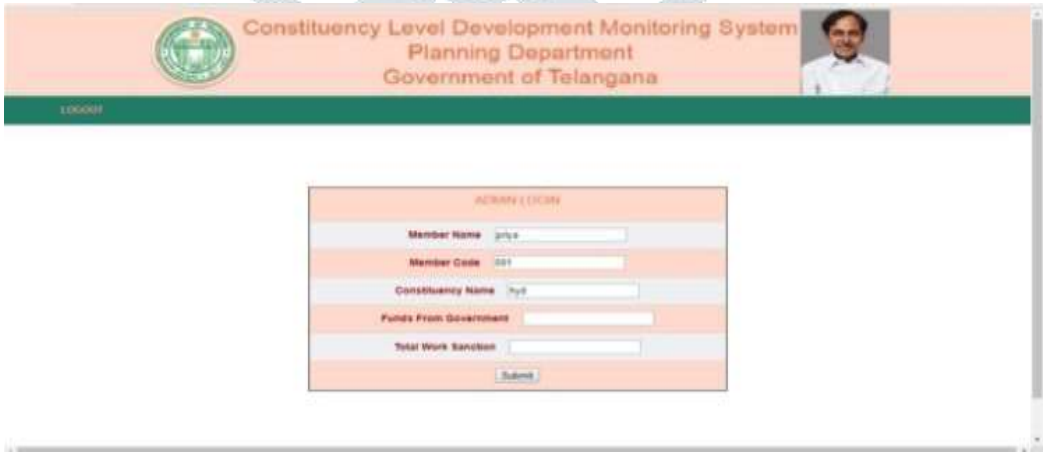


Figure 5.7: Admin allocating funds

5.8 Uploading Data – Users will update the work details time to time based on the funds allocated by the government.

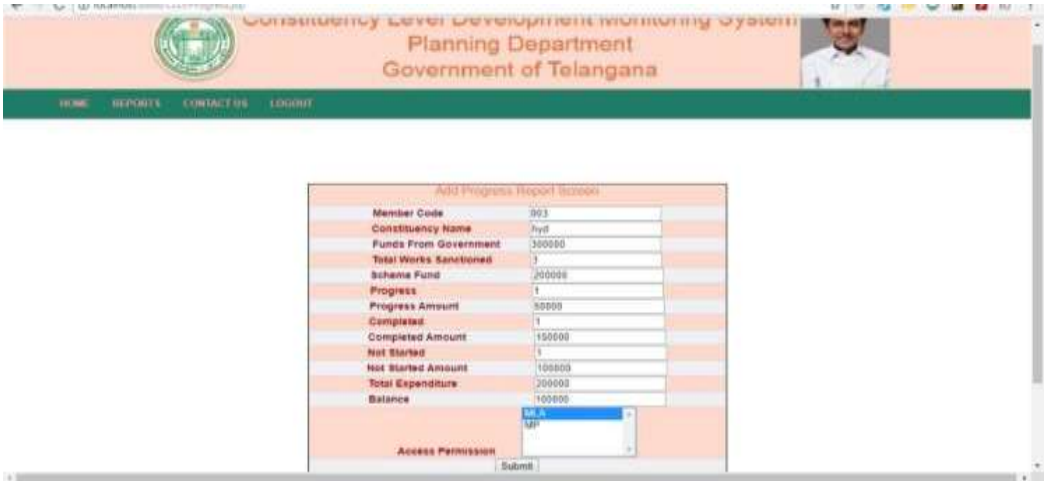


Figure 5.8: Uploading Data

5.9 Viewing reports – Based on access permissions data is shown to the authorized users.

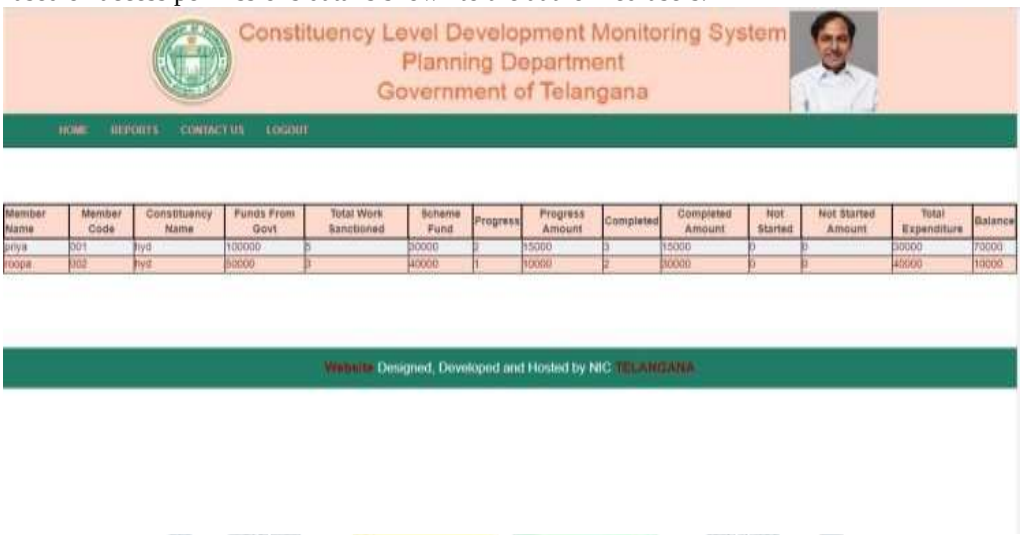
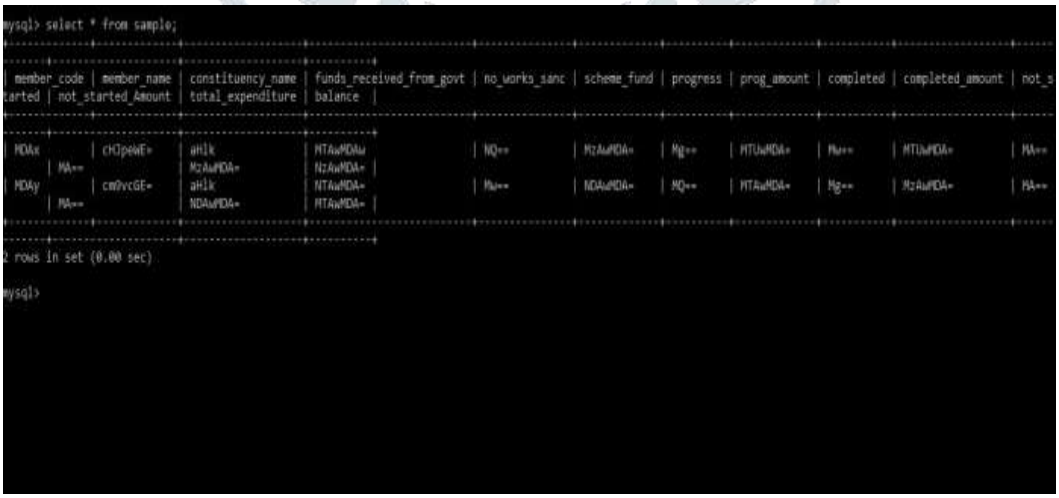


Figure 5.9: Viewing reports

5.10 Data encrypted using ECC – The data is secured using Elliptic curve cryptography algorithm.

Figure 5.10: Data encrypted using ECC



VI.CONCLUSION

The implementation of this paper work is to enhance the authentication and access control process in cloud environment. By executing OTP along with ECC as an authentication parameter when one user wants to access cloud resource from external location or from public cloud the authentication system is enhanced. By practicing Role Based Access and Control (RBAC) we have provided different privileges to different users, in this way we have implemented a much secure access control mechanism.. The confidentiality of the message is maintained by using ECC algorithm. The database keeps all the information in encrypted form, hence it is very hard to intercept the data stored in database. The complete study concludes that, the existing model not only enhances the security to the public and private cloud but it also provides the same security in the hybrid cloud environment. By employing the security principle and algorithm we tried to enhance the security of the overall cloud based system.

VII.ACKNOWLEDMENT

I would also like to show my gratitude to the Organization, especially Mr.Srinivasa Subbarao Akella-Technical Director in National Informatic Center (NIC) for giving me this opportunity to work along with the esteemed employees of NIC.

VIII.REFERENCES

[1] Hsing-Chung (Jack) Chen, Marsha AnjanetteVioletta, Cheng-Ying Yang, Contract RBAC in cloud computing, The Journal of Supercomputing archive Volume 66 Issue 2, Nov 2013 Page 1111- 1131 Kluwer Academic Publisher Hingham,MA, USA

[2] TekinBicer,David Chiu, GaganAgrawal, Time and Cost Sensitive Data- Intensive Computing on Hybrid Clouds, 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Comlputing.

[3] Vijay Varadharajan, Department of Computing, Macquarie University, Sydney, Australia, Security, and trust in the web, Proceeding APWeb'12 Proceedings of the 14th Asia- Pacific international conference on Web Technologies and Applications.

[4] PriyankaNema, An Innovative Approach for Dynamic Authentication in Public Cloud: MD5, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2,Issue11, November 2014

[5] Primer, "An Elliptic Curve Cryptography Primer." *The Certicom 'Catch The Curve' White paper series*,June-2004

[6] D. R. L. Brown. "Standards for Efficient Cryptography 1(SEC-1)."*Standards for Efficient Cryptography*,2009.

[7] H. Darrel, A. J. Menezes and S. Vanstone. "Guide to Elliptic Curve Cryptography." *Springer Science & Business Media*,2006Hsing.

[8] P. V. G. D. Prasadreddy, T. SrinivasaRao, S. PhaniVenkat, A Threat Free for privacy Assurance in Cloud Computing, Proceeding SERVICES'11 Proceedings of the 2011 IEEE World Congress on Services Pages564-568.

[9] Parekh, T ;Gawshinde S ; Sharma M K " Token based authentication using mobile phone" published in proceddingof Communication Systems and Network Technologies (CSNT) 3-5 June 2011, Jammu,India.