Indian Census Counting and Securing Using AES Encryption Algorithm: A Review Paper

Balaji Puri[1], Harshal Shelare[2], Lalit Tepale[3], Khan Kalimulla[4], Prof. Jagdish Kapadnis[5]
[1,2,3,4] *Student, PVGCOE, Nashik*
[5]*Assistant Professor, PVGCOE, Nashik*

***Abstract*- With the rapid development of information technologies, data became a need for everyday activities of an individual that demands fast and secure access to it. Cloud storage, therefore, emerged as a suitable solution to address these challenges of accessing and processing data anytime, anywhere and, to some extent, in any quantity. Different approaches to implementing cloud storage systems have declined or increased users trust in these systems. In this paper, we propose a client based encryption storage system in which users control the cryptographic keys lifecycle and are allowed to select different encryption methods, according to their requirements. We also make an analysis of our proposed solution compared to some features of other similar solutions.**

Index Terms- AES algorithm, Cloud Security, census, Performance.

I. INTRODUCTION

Security is one of the most difficult tasks to implement in cloud computing. The proposed system basically deals with the security issues that are experienced during the storage of data on the cloud. The cloud vendors generally store the client's data and information in the cloud without following any security measures. Cloud computing is a large-scale distributed computing paradigm in which a pool of computing resources is available to cloud consumers via the Internet. Cloud storage is a data storage model in which files are stored in logical partitions whereas the physical storage spans multiple servers in multiple locations and the physical environment is owned and managed by a hosting company. These cloud storage providers are responsible for providing the availability and security of user files. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. When the file is distributed then data is also segregated into many servers. So here the need for data security arises. Every block of the file contains its own hash code, using hash code which will enhance user authentication process; an only authorized person can access the data. Here, the data is encrypted using advanced encryption standard, so data is successfully and securely stored on the cloud. The third-party auditor is used for public auditing. The proposed design allows users to audit the data with lightweight communication and computation cost. The analysis shows that the proposed system is highly efficient against malicious data modification attack and server colluding attack. Performance and extensive security analysis shows that proposed systems are provably secure and highly efficient. Cloud storage services may be accessed through a co-located cloud computer service, web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems. Files are stored in cloud storage systems in plain text format. Again multiple copies of the files are maintained in multiple locations for faster access and availability. If proper security measures are not taken, malicious users can gain access to the files and misuse it.

II. LITERATURE SURVEY

Literature Survey is the most important step in the software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satires, then next step is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmer need a lot of external support. this support can be obtained from senior programmers, from a book or from websites.

Lattice-based cryptography is the use of conjectured hard problems on point lattices in Rn as the foundation for secure cryptographic systems. Attractive features of lattice cryptography include apparent resistance to quantum attacks (in contrast with most number-theoretic cryptography), high asymptotic efficiency and parallelism, security under worst-case intractability assumptions, and solution s to long-standing open problems in cryptography. This work surveys most of the major developments in lattice cryptography over the past ten years. The main focus is on the foundational short integer solution (SIS) and learning with errors (LWE) problems (and their more efficient ring-based variants), their provable hardness assuming the worst-case intractability of standard lattice problems and their many cryptographic applications. Dropbox is a cloud-based file storage service used by more than 100 million users. In spite of its widespread popularity, we believe that Dropbox as a platform hasn't been analyzed extensively enough from a security standpoint. Also, the previous work on the security analysis of Dropbox has been heavily censored. Moreover, the existing Python bytecode reversing techniques are not enough for reversing hardened applications like Dropbox. We describe a method to bypass Dropbox's two-factor authentication and hijack Dropbox accounts. Additionally, generic techniques to intercept SSL data using code injection techniques and monkey patching are presented. This system presents Hybrid (RSA and AES) encryption algorithm to safeguard data security in Cloud. Security is the most important factor in cloud computing has to be dealt with great precautions. Cloud computing model is a very exciting model, especially for business peoples. Many business peoples are getting attracted towards cloud computing model because of the features easy to manage, device independent, location independent. But these cloud models come with many security issues. A business person keeps crucial information on the cloud, so security of data is a crucial issue as the probability of hacking and unauthorized access is there. Also, availability is a major concern on the cloud. When a file is distributed then data is also segregated into many servers. So here the need for data security arises. Every block of the file contains its own hash code, using hash code which will enhance user authentication process; an only authorized person can access the data. Here, the data is encrypted using advanced encryption standard, so data is successfully and securely stored on the cloud. The third-party auditor is used for public auditing. This system discusses the handling of some security issues like Fast error localization, data integrity, data security. The proposed design allows users to audit the data with lightweight communication and security analysis shows that proposed systems are provably secure and computation cost. The analysis shows that the proposed system is highly efficient against malicious data modification attack and server colluding attack. Performance and extensive security analysis shows that proposed systems are provably secure and highly efficient. In cloud computing distributed resources are shared via the network in an open environment. Hence the user can their data easily accessible from anywhere. At the same time there exist privacy and security issues due to many reasons. First one is dramatic development in network technologies. Another is the increased demand for computing resources, which make many organizations to outsource their data storage. So there is a need for secure cloud storage service in the public cloud environment where the provider is not a trusted one. This system addresses different data security and privacy protection issues in a cloud computing environment and proposes a method for providing different security services like authentication, authorization, and confidentiality along with monitoring in delay. 128-bit Advanced Encryption Standard (AES) is used for increased data security and confidentiality. In this proposed approach data is encrypted using AES and then uploaded on a cloud. The proposed model uses Short Message Service (SMS) alert mechanism for avoiding unauthorized access to user data.

III. PROBLEM DEFINITION

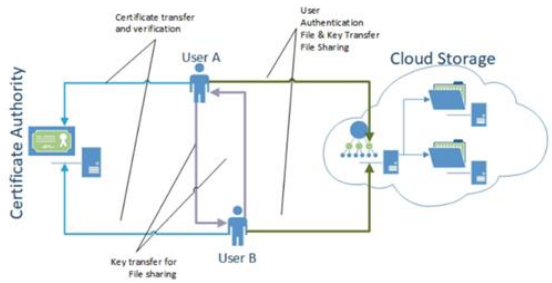
To design a system for the collection of real-time data regarding the Indian Census this changes per milliseconds. And storing that data on to the cloud by securing files using different cryptographic algorithms.

IV. SYSTEM ARCHITECTURE

The proposed model builds upon a general Cloud storage architecture with a client-side encryption

scheme and tries to enhance user control over the encryption mechanisms and to simplify the information flows that exist between the client application and other parties (in this case the Certification Authority and the Cloud storage). To address the second statement, four distinct components are comprised in our model:

1. Certificate Authority (CA) a 3rd party entity that is a valid and accredited organization to issue and manage public-key certificates for users;
2. Access Control Servers (ACS) the Cloud storage component through which access is permitted or denied to a user, based on its credentials. This module also enforces the filtering policies that are applied over the data storage servers, related to filing sharing functionalities;
3. Data Storage Servers (DSS) the Cloud component that provides only storage spaces allocated to individual users. Because it does not need any complex functionality, this component can be substituted with services from other Cloud storage providers, such as Google Drive or Dropbox.
4. Client Application (CApp) the main component of the architectures in which resides the key generating and file encryption logic. Also, it provides the means to ensure the sharing of keys when a file is shared with another user. All communications links between different components are secured using TLS or mutual TLS, such as the link for authenticating users by the ACS. We enable this type of authentication through the use of public key certificates, issued by a certified CA, thus separating this service from the Cloud storage domain. Therefore, we eliminate the possibility of the ACS to control any information flow, by having no knowledge or possibility to know the structure of data being transmitted through it, unless specifically demanded by the user.



V. CONCLUSION

Through Cloud storage, an individual can isolate itself from problems such as the need for storage space or security issues that arise when allowing others to interact with personal files intended for public usage. Even with these major advantages, a severe drawback is a lack of controlling the security mechanisms that ensure the protection of one's data. Our solution tries to tackle this drawback, by empowering user's control over the encryption mechanisms. We propose a model in which the user application is the only entity that has any knowledge of the generated data encryption keys and what encryption algorithms have been chosen by the user for a specific file.

REFERENCES

[1] Rashminigoti and Dr. Shailendra singh, 2013. A survey of cryptographic algorithm for cloud computing, International journal of emerging trends and computer application systems.

[2] R.K Seth and Rimmy Chuchra March-April-2014.TBDSA A new data security algorithm in cloud computing, International journal of computer science and information technology.

[3] en.wikipedia.org/wiki/TinyEncryptionAlgorithm

[4] T.Sivasakthi and Dr.Prabakarn Feb-2014.Applying digital signature with encryption algorithm of user authentication for data security in cloud computing, International journal of innovative research in computer and communication engg.

[5] M.Vijayapriya Sept-2013, Security algorithm in cloud computing: Overview, International journal of computer science and emerging technology.

[6] N. Courtois. The HFE public key encryption and signature. http://www.minrank.org/hfe/. Accessed December 2004.

[7] N. Courtois. Is AES a Secure Cipher? http://www.cryptosystem.net/aes/. Accessed December 2004.

[8] N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdened systems of equations. IACR eprint server http://www.iacr.org, April 2002.

[9] N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdened systems of

equations,. In Asiacrypt 2002, Volume 2501 of Lecture Notes in Computer Science, pages 267-287, Springer-Verlag.

[10] N. Courtois, A. Klimov, J. Patarin, and A. Shamir. E - cient algorithms for solving overdened systems of multivariate polynomial equations. In B. Preneel, editor, Proceedings of Eurocrypt 2000, LNCS 1807, pages 392407, Springer-Verlag, 2000.

[11] A. Kipnis, A. Shamir. Cryptanalysis of the HFE public key cryptosystem. Proceedings of Crypto99, Springer-Verlag.

[12] S. Landau. Polynomials in the nations service: using algebra to design the Advanced Encryption Standard. American Mathematical Monthly, February 2004, pp. 89-117.

[13] S. Murphy and M.J.B. Robshaw. New observations on Rijndael. NIST AES website http://csrc.nist.gov/encryption/aes, August 2000.

[14] S. Murphy and M.J.B. Robshaw. Essential Algebraic Structure within the AES. In, M. Yung, editor, Advances in Cryptology CRYPTO 2002, volume 2442 of Lecture Notes in Computer Science, pages 116, Springer-Verlag. August 2002.

[15] S. Murphy and M.J.B. Robshaw. Comments on the Security of the AES and the XSL Technique. Note available at http://www.isg.rhul.ac.uk/mrobshaw/ rijndael/xslnote.pdf. 26 September 2002.

[16] National Institute of Standards and Technology. Advanced Encryption Standard. FIPS 197. 26 November 2001.

[17] B. Schneier. Crypto-Gram Newsletter, Counterpane Internet Security, available at http://www.counterpane.com/crypto-gram.htm September 15, 2002.

[18] B. Schneier. Crypto-Gram Newsletter, Counterpane Internet Security, available at http://www.counterpane.com/cryptgram.htm October 15,2002.

[19] EFF DES Cracker. Wikipedia. Available at http://en.wikipedia.org/wiki/DeepCrack. Accessed December 2004.

[20] http://ijaiem.org/volume3issue3/IJAIEM-2014-03-17-048.pdf

[21] https://en.wikipedia.org/wiki/Cloudcomputingarchitecture

[22] https://www.researchgate.net/publication/239732057CloudStorageArchitecture

[23] https://www.draw.io/

[24] https://www.entrust.com/wp-content/uploads/2015/08/HowSSLWorksChart.png

[25] http://mathworld.wolfram.com/RSAEncryption.html

[26] http://www.tutorialspoint.com/cryptography/tripledes.htm

[27] https://en.wikipedia.org/wiki/Randomnumbergeneration