International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Security Algorithms for Privacy Protection and Security in Aadhaar

Arpana Chaturvedi[*1], Dr. Meenu Dave[2], Dr. Vinay Kumar[3]
[*1]Assistant Professor, Jagannath International Management School, JIMS, GGSIPU, New Delhi, India
[2]Professor, Jagannath University, Jaipur, Rajasthan, India
[3]Professor, Vivekananda School of IT, VIPS, GGSIPU, New Delhi, India

ABSTRACT

Government is enforcing the citizens to link Aadhaar details with various government services to provide services to right beneficiaries. At the same time resident of India are worried about their privacy and security. In recent months, many cases of fraudulent increased the worry of all citizens. The Aadhaar project is the largest biometric identity project, a great initiative taken by the Planning Commission of India in 2009.The project has taken care of all aspects of privacy protection and security issues. Then after the fraudulent and theft of identity related issues keep on taking place. In this paper, various security measures are discussed which can be implemented to be safe from insider's attacks. Authentication, Authorization, Data Encryption, Security against various attacks are the key levels of data and information security in the Hadoop environment. In recent years, various efforts made to manage more effectively each and every level of security. Kerberos is one such effort in order to attain Authentication and Authorization and it succeeded in doing so, but with the attackers having new technologies and hacking tools attackers can easily bypass the security provided by Hadoop's Kerberos Authentication system and then the data at storage level is unencrypted can easily be stolen or damaged which is a big concern. A new encryption technique to secure data in HDFS environment is the combination of AES and Map Reduce. It performs encryption in parallel using AES-MR (an Advanced Encryption standard based encryption using Map Reduce) technique in Map Reduce paradigm. To provide network security Quantum Cryptography and Biometric based Security solution using BB84 protocol is suggested protocol. This paper also explained the various suggested algorithms and security measure to implement on the Network level security Layer, Database level Security Layer and Application Level security Layer.
Keywords: UIDAI, CIDR, QKD, BB84, AES-MR, HDFS, Cryptography, Kerberos.

I. INTRODUCTION

The central government under the leadership of Mr. Nandan Nilekani, Minister of State, created the Unique Identification Authority of India (UIDAI). It is an agency responsible for implementing the Multipurpose National Identity Card or Unique Identification card (UID Card) project in India. UIDAI will be responsible for issuing the numbers to the citizen of India. Individual government ministries and agencies will be responsible for integrating the numbers with their respective databases. The implementation of a biometric based Unique Identification project faces many social, ethical, cultural, technical, and legal challenges. One of the major challenges is issuing each and every resident of the country a Unique Identification Number (UID). The idea behind this India's largest biometric project is to ensure that residents could have a singular universal identification card. It is also a portable form of identification. It can eliminate duplicate and fake identities. It will save identity verification costs for businesses. The systems having facility of online verification of authentication of identity is very cost and time effective. To enable this fast verification at global level through any device is only possible through central database. To enable the fast and cost effective verification it is required that UIDAI system stores all the details of every Indian resident including demographic and biometric information in the centralized Database. At the same time such a centralized system invites the worry about single point of failure and potential abuse from

insiders. As UIDAI aims to make verification easier for both organizations in both private and public sector through a central database, it is important to understand potential loopholes that include breach of privacy and various technological and legal issues in India. In this paper we suggested various security measures to be taken against Insider attacks.

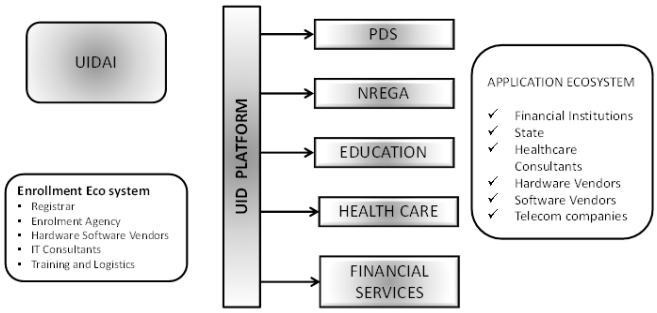

Figure 1. Linking of Aadhaar number with various services

Different tools and techniques are proposed to protect the system from runtime attacks. The section 2 contains these ideas and proposals. In Section 3 Proposed algorithm for Network security and Data Security control is discussed. Application Level Security and Reactive Level Security control is discussed in section 4. In section 5, the work is concluded with future work to be done further.

II. TOOLS AND TECHNIQUES FOR PROTECTION FROM INSIDER AND RUNTIME ATTACKS

A. Proposed Security measures against insider attacks

UIDAI System and its database cannot be trusted against insider leaks, possibilities of system hacks, tampering of authentication records and audit trails. Most dangerous threat is the involvement or possibility of insiders attacks. The other party's attacks are only possible or more likely due to involvement of insiders. Insiders have the access to various components of the Aadhaar System. To provide security against insiders proper authorized investigation are required. The investigation process should be through pre-approved, audited and tamper proof computer programs which must be further maintained by digitally signed authorization. The enrolment agencies, enrolment devices, Point of Sale devices and various AUAs whether government or private cannot be trusted from data privacy, protection and security point of view.

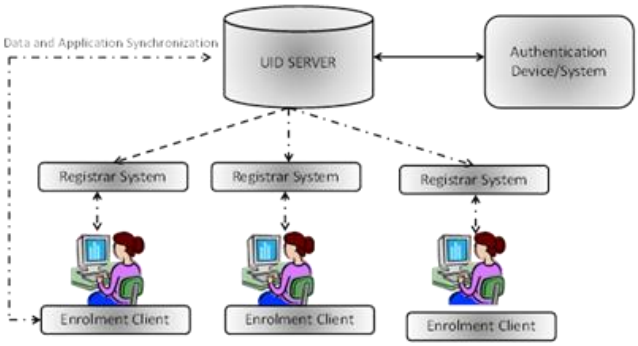

Figure 2. UIDAI MODEL

The biometric, demographic data, sensitive and private user data related to its medical and immunization records cannot be compromised at any cost. A very strong legal and policy frameworks are required to ensure the trust and reliability. Keeping all the above mentioned issues in view the strict security measure must be taken against insider attacks.

The proposed security measures are:

A) Legal provision: A legal provision is required to set up a third party audit and key management protocol. The steps to be taken are:

- ✓ The working of the system should be based on Distributed Key Management.
- ✓ A part of decryption key should be kept with third party.
- ✓ The program stored in CIDR should be requested and accessed by following steps.

a. A third party can only share the key with the computer program residing in CIDR. The share of key is only allowed after getting authenticated and approved by auditor using cryptographic certificate. It verifies that the program has not been tampered.

b. Auditor should inspect the data thoroughly and approve it digitally for further use. It is must that auditor should examine, approve and cryptographically sign the program that may run in the CIDR. These programs should be cryptographically approved by the auditors program that they are genuine and have not got tampered.

c. At the time of execution, key must be shared only with audited and approved UIDAI program.

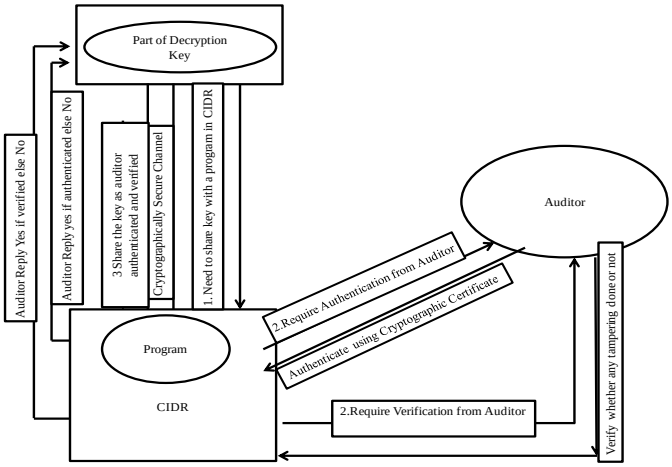

Figure 3. Working of Security Measures against Insider attacks.

B) Tools and Techniques to protect the system from run time attacks: Every decryption key should reside in the memory of the UIDAI systems during the time of execution of programs or processes. An experienced and smart System administrator, will access to hardware and the operating system, will be easily able to access these decryption keys from the system's memory. The variety of tools proposed which could be used to protect system against such run-time attacks are:

i) Use of Fuzzy Extractor and Symmetric Hashing Techniques: It is used to Store Hash of biometric data. Fuzzy extractors and symmetric hashing techniques are basically used to store non-invertible hash of biometrics which converts it into a string representing biometric data. It should be used to protect biometric data stored in Aadhaar database. It converts a string representing biometric data to a uniform random string which does not leak any information about the individuals.

ii) Proposed Tools used for Tamper proof code: There are so many numbers of tools which are used for Tamper proof code. It protects code from tampering of information by insiders. There are so many techniques which can be used to maintain security and integrity of code without any code transformations. These techniques are used to examine the code without executing the program.

a) Static Code Analysis: Static Code Analysis reveals the errors and uncovers the subtle defects and vulnerabilities. The process is also termed as glass-box testing. Veracode is one of the best static analysis tools. It uses binary code or byte code. It is one of the best tools to write secure code. It is also used to verify the server code that whether it is working according to intended specifications or the behaviours of the server code got changed due to tampering. End to end static code analysis or model checking on server code is used to address malicious activity if taken place with server code to modify it.

b) Executable Languages: Executable languages are used to code behavioural specifications into industry adopted known format. Few examples of such language are TLA+, Simulink and State flow Message Sequence chats.

- ✓ **TLA** stands for the Temporal Logic of Actions used for writing high-level specifications of concurrent and distributed systems. It describes the things using simple mathematics.
- ✓ **Simulink** is a visual tool used for doing computational simulations. It uses a drag and drop system for simulation components that can then be connected between them with lines. In past, people use it for engineering, where you can represent your system as a set of variables and model it mathematically. E.g. Electrical circuits, Mechanical systems that need to control are cars, airplanes and Robotics etc.
- ✓ **Message Sequence Chart (MSC)** used to provide a trace language for the specification and description of the communication behavior of system components and their environment by means of message interchange.
- ✓ **Control flow integrity** performs runtime check on the code by installing an additional monitor. It is the best solution to perform the activity. It checks the execution behaviour of the code and warns of any activity is against the admissible behaviour of the program. Third party is required to set up the processes accordingly so that can ensure the availability of tamper proof code.

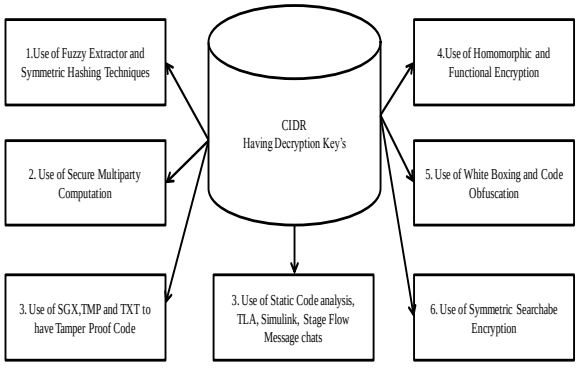

Figure 4. Tools and Techniques to protect the system from run time attacks

iii) Tamper proof hardware: Intel's Software Guard Extension (SGX) and its forerunners TPM and TXT are the solutions to protect cryptographic keys or data reside in memory. Data lying in non-volatile memory can be leaked during reboot or through side channel attacks. It protects the areas of hardware's where execution of application can take place without compromising BIOS, drivers, memory buses and application security.SGX provide solutions for remote attestation challenges to ensure hardware integrity. Trusted hardware leveraged to provide integrity and confidentiality. Third party has to carefully set up the system and keep the hardware trusted to ensure tamper proof storage.

iv) Secure multiparty computation: In Digital India, many services are interlinked with UID number and help to get the services available to right beneficiaries. In this process, many organization need to communicate with each other. This communication arise the chances of leakage of secret information, which can be further misused. Secure multiparty computation, a field of cryptography can be one of the solutions to secure keys and private inputs. It provides security to several mutually distrustful parties. In this process, two parties frequently need to perform some computation on their joint data like verifying identity of a person. It helps to maintain privacy of the input data of both the parties. Secret-sharing scheme can also be used which can help split the database across two servers belonging to different entities, ensuring that the two servers have disjoint set of system administrators , different operating systems and hardware's. This scheme is beneficial as if in case at any point of time one server is hacked, the data will remain protected. This proposed scheme can results as efficient and reliable technique which can be used to answer queries on the data distributed across servers.

v) Homomorphism and Functional Encryption: Homomorphic and functional encryption are the advanced technique that can be used to prevent a server breach from leaking viable user data. Critical and sensitive data stored by or generated by user needs to be stored on the server in encrypted form. Homomorphic systems allow sensitive data to be encrypted in a way that allow sophisticated computation on the data in its encrypted form. These forms of encryption techniques may be very relevant and much applicable to ensure privacy of data in the UIDAI database. To implement Homomorphic and functional encryption, third party is required to set up the computation in the encryption domain.

Homomorphic term is known as same structure and the data in a Homomorphic encryption scheme keeps the same structure, identical mathematical operations no matter whether they are performed on encrypted data or decrypted data.

Working of Homomorphic Encryption:

- We know that the UID store in CIDR is private data of residents. It contains information all biometric and demographic details along with UID Number. Let say this uid number s linked with Bank. Bank has account details of a resident like UID number-Uno, Account number Acno. Some amount a resident want to deposit let say amt. This amt will get added with balance and new amt in bank will appear as balance to encrypt this data set, Bank ABC multiplies each element in the set by 2, creating a new set of members.
- Bank ABC sends the encrypted data set to the storage server for safe storage. A few months back, the government contacts Bank ABC and request the total balance of customer having UID number uno.
- Bank ABC is very busy in various transactional activities, hence asked server storage i.e. cloud provider to perform operation. The cloud provider, who only access to the encrypted data sets, find the total balance appeared after summation and returns the current balance. Let say 10+20=30 in case of actual digits 5 and 10.
- Bank ABC decrypts the cloud providers reply and provide the government with the decrypted answer, 15.

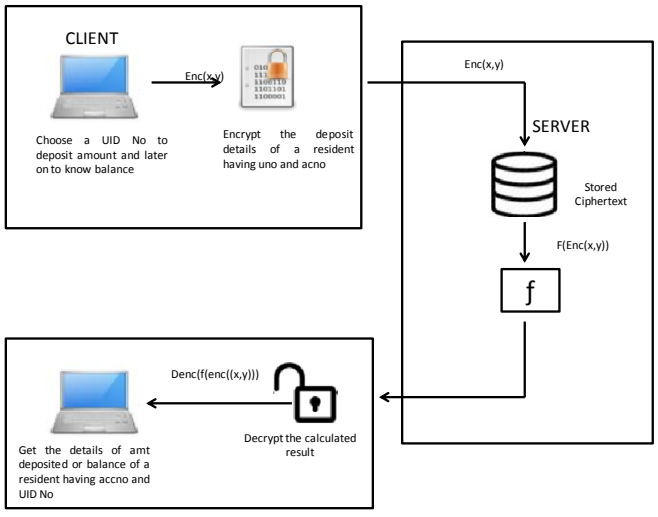

Figure 5. Working of Homomorphic Encryption

A cryptosystem that supports arbitrary computation on cipher texts is known as fully Homomorphic encryption (FHE) and is far more powerful. Such a scheme enables the construction of programs for any desirable functionality, which can be run on encrypted inputs to produce an encryption of the result. Since such a program need never decrypt its inputs, it can be run by a non trustable party without revealing its inputs and internal state. Fully Homomorphic cryptosystems have great practical implications in the outsourcing of private computations.

The application scenario is one of outsourcing computation, whilst preserving privacy of inputs. The standard way to achieve this in a single user setting is with FHE. However, when faced with a large pool of users who wish to compute a function on all their private inputs, FHE cannot be applied so easily.

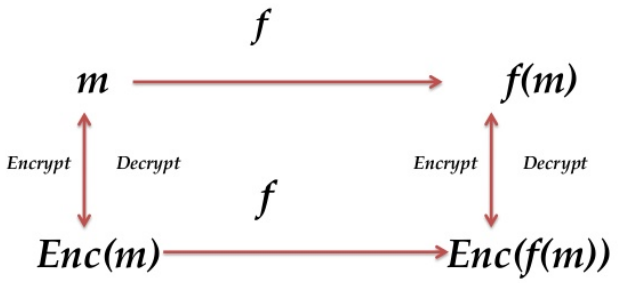

Figure 6. Fully Homomorphic Encryption

They create a new primitive, called Multi-key Fully Homomorphic Encryption, to deal with this situation. Each client has a key pair (ski, pki), and there is a single high-powered server used to evaluate the desired function, f. When given some cipher texts c1 = Enc (pk1, x1), cn = Enc (pkn, xn), the server can compute y = Eval (f, c1, cn). The clients then perform an interactive decryption protocol to jointly recover f(x1, xn) = Dec (sk1, skn, y). It is stressed that this decryption phase is the only part of the process requiring interactivity. The number of clients and the function to be evaluated is completely dynamic and can be chosen on-the-fly.

Symmetric Searchable encryption and Extensions: Symmetric Searchable encryption enables searching on encrypted data. This searchable encryption is highly efficient and appropriate for voluminous and ever growing UIDAI data. The proposed solution delegates searching on encrypted data to cloud service provider CSP but with privacy preserved.

It is possible to search for specific keywords within an encrypted content, i.e., without requiring the user to download the database and decrypt its contents before searching can be performed.

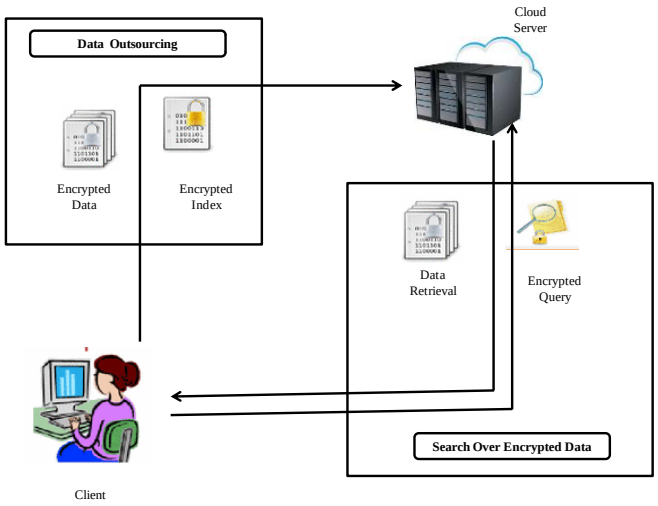

Figure 7. Searchable Symmetric Encryption

The Adaptively Secure Searchable Symmetric encryption scheme provides a simple and is proposed by Curtmola. It uses the index based approach where user has to pre-process the contents to generate a keyword index to provide for the search capability. This is why it is an efficient method and it enables searching over encrypted data. It preserves the data privacy more efficiently. A private / symmetric key implementation in this scheme is better than public/asymmetric key implementation. The reason behind is its computational overhead which is comparatively very less in case of private symmetric key.

vi) White boxing and code obfuscation: White Box cryptography technique can be used to protect attacks from insiders. It can be used to implement cryptographic procedures in the software that transform and obfuscate code. The data in this way remain secure as cryptographic even in case of white box attacks also. It protects the code from insiders who have full access of source code, binary files running on the system, its corresponding memory pages during execution. It also protects debuggers, emulators, intercept system calls, and possibilities of tamper with the binary and its execution etc. attacks by insiders. A cryptography algorithm gets the key and plaintext (encryption mode)/cipher text (decryption mode) as input and outputs the cipher text/plaintext. A white box implementation of the cryptography algorithm gets just plaintext/cipher text as input and outputs the cipher text/plaintext. The key embedded in the algorithm is

merged on S-boxes. White-Box Cryptography and an AES Implementation is a way to implement a white-box implementation of AES. In code obfuscation we should protect some parts of the code. Code obfuscation is NOT a way to achieve white-box cryptography whereas White-box cryptography is used in code obfuscation. White-box cryptography techniques are aimed at protecting software implementations of cryptographic algorithms against key recovery. Code obfuscation is aimed at protecting against the reverse engineering of a cryptographic algorithm.

III. PROPOSED ALGORITHM TO PROTECT NETWORK SECURITY AND DATA SECURITY

A) Quantum Cryptography based Encryption for Network Security: in this process, the key distributes over the quantum channel in spite of encrypted message. To establish communication between John and Michal, two channels are required. First one is Public Communication Channel responsible for transmission of encrypted message or cryptogram and the second one is quantum channel responsible for key distribution. Such establishment or process is known as Quantum Key distribution (QKD).In QKD it is impossible to tap single quantum signals in the conventional sense. The eavesdroppers' activities produce an irreversible change in the quantum states due to collapse of the wave function, before they are retransmitted to the envisioned recipient. These changes produces high error rate in the transmissions between the sender and projected acknowledgements, allowing them to detect the attempted eavesdropper. The most effective is the use of private key with quantum key distribution, as it helps to detect monitoring channel. Measuring is an integral part of quantum technique and it should not be done passively. To implement this Protocol used is BB84.

Main idea behind this model is to use quantum cryptography for securing key distribution thus providing our data another layer of security. This way we can provide perfect security to data over the internet.

B) Proposal for Database level security: Data security is an important issue as far as storage of sensitive data is concerned. Hadoop is usually utilized for storage, large amount of data using its storage technology, namely Hadoop Distributed file System HDFS. Hadoop by default does not contain any security mechanism but as it has grown very much and it is the first choice of the business analyst and industries to store and manage data it is necessary to introduce security solutions to Hadoop in order to secure the important data in the Hadoop environment. Authentication, Authorization, Data Encryption, Security against various attacks are the key levels of data and information security in the Hadoop environment. Efforts have been made in order to attain each and every level of security over the period of recent years. Kerberos is one such effort in order to attain Authentication and Authorization and it succeeded in doing so, but with the attackers having new technologies and hacking tools attackers can easily bypass the security provided by Hadoop's Kerberos Authentication system and then the data at storage level is unencrypted can easily be stolen or damaged which is a big concern. Encryption of large data stored in HDFS is actually a process which takes a lot of time and this time consuming nature of encryption should be controlled by encrypting the data using a parallel method. Following Points which are to be taken care of to provide better data level security features in the UIDAI System are:

- ✓ Access to data to authorized users in office hours only.
- ✓ Authorization should be multifactor.
- ✓ Resident Data should only to be stored in encrypted in database as well as in backup tapes.
- ✓ Audit trail of data should be fine grained.
- ✓ AES-MR is an algorithm, which when used in XTX mode can provide better data level security.

a) The proposed encryption scheme is the combination of AES and Map Reduce. It performs encryption in parallel using AES-MR (an Advanced Encryption standard based encryption using Map Reduce) technique in Map Reduce paradigm. The time taken for performing the encryption and decryption process is relatively less for user generated content. AES-MR encryption process is found to be faster with mapper function alone in comparison with running the encryption process under mapper function and reducer function.

Map Reduce can be used to encode the huge data volumes and vital data utilizing the AES encryption algorithm as a part of XTX mode. The broadly utilized IEEE 1619-2007 standard is XEX-TCB-CTS (XTS)

mode in which key material for XTS-AES comprises of an encryption key and in addition a change key that is utilized to consolidate the coherent position of the data hinder into the encryption. XTS yields tend to deliver autonomous yields which prompt the parallelization of such procedure. XTS is a solid instantiation of the class of change capable square figures. The XTS mode permits parallelization and pipelining in figure executions. It empowers the encryption of the last deficient piece of data while different modes are not having this office. Guide Reduce is by all accounts an alluring, financially savvy answer for substantial scaling data, preparing administrations like securing data in the cloud through piece encryption.

Overall, this approach will give the data security a new height along with the use of Kerberos. It helps to attain all the levels of security in a faster speed.

IV. PROPOSED ALGORITHM TO PROVIDE APPLICATION LEVEL AND REACTIVE SECURITY CONTROL

A) Proposal for Application server level security:

- **a)** Centralized Access and identity management service for the entire system.
- **b)** LDAP data for individual states to authenticate in case of network failure between state and central systems.
- **c)** Consolidated LDAP for storing details of all users of UID system at all levels.
- **d)** Implementation of Identity Management software to implement Granular access policies to define different levels of access granted or denied to a user in the enterprise applications.
- **e)** Tools to implement preventive controls so that can ensuring that right people is entrusted with appropriate types of approvals and authorizations. This tool should have the flexibility to handle very complex, real-world scenarios for evaluating that which users have the ability to grant approval for various types of transactions.
- **f)** Use of Service-oriented architecture to secure web services. It is better to have a Common Web Services Security Manager, which is responsible for providing policy-driven security and management capabilities to existing or new Web services. It must have the ability to add policy-driven best practices to use Web services and should ensure uniform enforcement of policy across all portal services.

B) Proposal for Reactive security controls:

- **a)** This UID Project will produce vast amounts of audit log data which has to be effectively captured, managed and analyzed. Security auditors have to analyze the audit log of all heterogeneous system of an enterprise. It is suggested to consolidate the audit log data of an enterprise into a single data warehouse to have secure and scalable storage and access. Suitable compliance are required to know who accessed, altered, updated, deleted, or viewed sensitive data and accordingly can take further steps to protect data.
- **b)** Audit management infrastructure is required from the web so that Common audit records enables to know which users or applications have accessed any Web Services and what actions have been performed.

V. ACKNOWLEDGMENT

This research was supported by various research work done by researchers and published papers. I thank all of them as their research work has provided the insight and expertise to me and their work has greatly assisted my research. I would like to thank and show my gratitude to Dr. Vinay Kumar and Dr Meenu Dave for sharing their pearls of wisdom with me during the course writing this research paper. I am immensely grateful to the reviewers for their comments on an earlier version of the manuscript, although any errors are my own and should not tarnish the reputations of these esteemed persons.

VI. REFERENCES

[1]. Kadre V.,Chaturvedi S., "AES-MR: A Novel Encryption Scheme for securing Data in HDFS Environment using Map Reduce" , www.ijcaonline.org/ research/ volume129/ number12/kadre-2015-ijca-906994.pdf

[2]. Mehak, Gagan, "Improving Data Storage Security in Cloud using Hadoop ",ISSN : 2248-9622, Vol. 4, Issue 9(Version 3), September 2014, pp.133-138 , http://

www.ijera.com/papers/Vol4_issue9/Version%203/U4903133138.pdf

[3]. Weeks B.,Bean M.,Rozylowicz T., Ficke C. ,"Hardware Performance Simulations of Round 2 Advanced Encryption Standard Algorithms ,National Security", https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Standards-and-Guidelines/documents/aes-development/NSA-AESfinalreport.pdf doi=10.1.1.35.6941

[4]. Clunie D.,Public Comments on the XTS-AES Mode," https://csrc.nist.gov/csrc/media/projects/.../comments/xts/collected_xts_comments.pdf

[5]. Public Comments-Modes Development - Block Cipher Techniques,"https://csrc.nist.gov/Projects/Block-Cipher-Techniques/BCM/Public-Comments-Modes-Development ", Comments submitted to EncryptionModes nist.gov.

[6]. Dr. Hawthorne, NY, Computing Arbitrary Functions of Encrypted Data Craig Gentry IBM T.J. Watson Research Center 19 Skyline ,cbgentry us.ibm.com https://crypto.stanford.edu/craig/easy-fhe.pdf.

[7]. Desai S.,Park Y.,Gao J.,Sang-Yoon Chang,Chungsik Song, "Improving Encryption Performance Using Mapreduce", Published in: High Performance Computing and Communications (HPCC), IEEE 17th International Conference, ISBN: 978-1-4799-8937-9 , http:// ieeexplore. ieee.org / document/7336355/

[8]. G. Sujitha, M. Varadharajan, B. Raj Kumar and S. Mercy Shalinie ,"Provisioning Mapreduce for Improving Security of Cloud Data ",http:// scialert.net/ qredirect.php? doi = jai.2013.220.228&linkid=pdf, International Journal of Computer Science and Applications, Technomathematics Research Foundation Vol. 13, No. 2, pp. 89-105, 2016.

[9]. Alexander Uskov, Adam Byerly, Colleen Heinemann ,"Advanced Encryption Standard Analysis With Multimedia Data on Intel® AES-NI Architecture", Department of Computer Science and Information Systems, and interlabs Research Institute Bradley University, 1501 West Bradley Avenue Peoria, Illinois 61625, U.S.A. auskov bradley.edu http://www.tmrfindia.org/ijcsa/v13i26.pdf

[10]. Demir L.,Thiery M.,Roca V., Jean-Louis Roch, Jean-Michel Tenkes, "Improving dm-crypt performance for XTS-AES mode through extended requests ", Nov 21, 2016 The 4th International Symposium on Research in Grey-Hat Hacking - aka GreHack , Nov 2016, Grenoble, France https://hal.inria.fr/hal-01399967

[11]. Philip Derbeko, Shlomi Dolev, Ehud Gudes, Shantanu Sharma"Security and Privacy Aspects in mapreduce on Clouds: A Survey",www.https://arxiv.org/abs/1605.00677, (Submitted on 2 May 2016) 4. Network and Complex Systems www.iiste.org ISSN 2224-610X (Paper) ISSN 2225-0603 (Online) Vol 2, No.2, 2012

[12]. Liskov M., Minematsu K. , " Comments on XTS-AES" September 2, 2008 This is a comment in response to the request for comment on XTS-AES, as specified in IEEE Std. 1619-2007 September 2, 2008, https://csrc.nist.gov/ csrc /media/projects/block-cipher-techniques/ documents/ bcm/ comments / xts/xts_comments-liskov_minematsu.pdf..

[13]. Kirat Pal Singh, Shiwani ,"An Efficient Hardware design and Implementation of Advanced Encryption Standard (AES) Algorithm ", https :// eprint.iacr.org/ 2016/ 789.pdf.

[14]. Vaidyaa M. , Dr Shrinivas Deshpandeb ," Study of Performance Parameters on Distributed File Systems using mapreduce ",www.sciencedirect.com International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, https://ac.els-cdn.com/ S18770509 16000399/1-s2.0-S1877050916000399-main.pdf ?_tid=78c69a4a-e233-11e7-8cfd-00000aab0f01& acdnat=15134098 15_ d18af66cf2c2e5fa578411397b06ce28

[15]. Epuru Madhavarao,ChikkalaJayaRaju,Pedasanaganti Divya,A.S.K.Ratnam,"Data Security Using Cryptography And Stegnography", ISSN: 2278-1323 International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 5, July 2012, http://ijarcet.org/wp-content/uploads/IJARCET-VOL-1-ISSUE-5-319-325.pdf

[16]. Sahu S.,Bhadoria A.,"Survey on Cloud computing security using steganography",http://

ijsetr .org / wp-content/uploads/2015/08/IJSETR-VOL-4-ISSUE-8-2975-2978.pdf, Volume 4, Issue 8, August 2015 2975 ISSN: 2278-7798.

[17]. Vaikuntanathan V., University of Toronto ,"Computing Blindfolded: New Developments in Fully Homomorphic Encryption", http://www.cs.utoronto.ca/~vinodv/FHE-focs-survey.pdf

[18]. Seny Kamara ,Microsoft Research , Mariana Raykova , Columbia University, "Parallel Homomorphic Encryption", https://eprint.iacr.org/2011/596.pdf

[19]. Shai Halevi ,"Homomorphic Encryption ",(IBM Research) April 2017 ,https://shaih.github.io/pubs/he-chapter.pdf

[20]. Dr. E. Laxmi Lydia, Dr. M.Ben Swarup ,"Analysis of Big data through Hadoop Ecosystem Components like Flume, Mapreduce, Pig and Hive", www.ijcse.net/docs/IJCSE16-05-01-021.pdf.

[21]. Anju Rani ; Avanindra Kumar Lal ; Shalini Sharma ; Latha Banda ; Amit Kant Pandit. ,"Quantum Cryptography Based Biometric Encryption for Network Security ",IEEE XPlore: 09 October 2014, ISBN: 978-0-7695-5013-8, INSPEC Accession Number : 14651794 , DOI : 10.1109/ ICMIRA .2013.19 , http://ieeexplore.ieee.org /iel7/6917607 /6918774 / 06918796.pdf

[22]. G. Sujitha, M. Varadharajan, B. Raj Kumar and S. Mercy Shalinie ,"Provisioning Mapreduce for Improving Security of Cloud Data ", http:// scialert.net/ qredirect.php ?doi=jai.2013.220.228&linkid=pdf, International Journal of Computer Science and Applications, Technomathematics Research Foundation Vol. 13, No. 2, pp. 89-105, 2016.

[23]. Kumar M., Gupta A., Shah K.,Saurabh A.,Saxena P., Tiwari V., "Data Security Using Stegnography and Quantum Cryptography" , http://www .iiste.org/ Journals /i ndex.php / NCS/article/view/1672

[24]. Philip Derbeko, Shlomi Dolev, Ehud Gudes, Shantanu Sharma"Security and Privacy Aspects in mapreduce on Clouds: A Survey",www.https://arxiv.org/abs/1605.00677, (Submitted on 2 May 2016) 4. Network and Complex Systems www.iiste.org ISSN 2224-610X (Paper) ISSN 2225-0603 (Online) Vol 2, No.2, 2012

[25]. Liskov, Minematsu , " Comments on XTS-AES" September 2, 2008, A comment in response to the request for comment on XTS-AES, as specified in IEEE Std. 1619-2007, https://csrc.nist.gov/csrc/media/ projects/block-cipher-techniques/ documents/ bcm/comments/ xts/xts_comments-liskov_minematsu.pdf.

[26]. Morris Dworkin , Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices ,http://nvlpubs.nist. gov/ nistpubs/Legacy/SP/nistspecialpublication800-38e.pdf, NIST Special Publication 800-38E January, 2010