MCAR

MUTHAYAMMAL CENTRE FOR ADVANCED RESEARCH

Mcas Journal of Research

mcas Journal of Research Volume 5

MUTHAYAMMAL
Publishing House

DEC 2019

MCAS JOURNAL OF RESEARCH

MCAS POLICY ON PLAGIARISM

There have been tendencies to misuse the system and vitiate the process of science communication for personal benefits. One of the ills, afflicting science communication, is plagiarism. Attempts at plagiarism may range from verbatim copying of extensive material of other authors, misappropriating results/data of others with minor changes in languages/presentation without giving credit to original source, and to publishing essentially the same information more than once.

As the premier institution of publishing primary scientific journals in various disciplines of sciences and technology, MCAS strongly reiterates its policy of discouraging of plagiarism of all kinds. All efforts are made to detect and frustrate attempts at plagiarism through editorial screening and rigorous peer review in respect of communications received for publication in the MCAS publications. Cooperation community is sought in our efforts to frustrate all attempts at plagiarism.

In case, an attempts of plagiarism is brought to our attention accompanied with convincing evidence following steps would be taken:

i. After consulting the respective Editorial Board Members, authors guilty of plagiarism will be debarred from publishing their papers in MCAS journals.
ii. Heads of the Departments/Institutions of the offending authors will be intimated of such incidences of plagiarism.

CONTENTS

S. NO.	CONTENTS	PAGE NO.
1	ACCESS PRIVILEGE BASED DATA RETRIEVAL AND SECURE SHARING IN DECENTRALIZED MILITARY NETWORKS K. Renuka and M. Sudha	01
2	ACCURATE DETECTION OF SPAM MAIL TO SECURE USER INFORMATION THROUGH MACHINE LEARNING S. Umamaheswari and A. M. Nirmala	04
3	A DYNAMIC WEB CONTENT READER S. Saranya and A. Anusha Priya	07
4	DATA RECOVERY IN MULTI THREAD A. Manikandan and P. Subramaniam	09
5	EFFICIENT MATHOD OF SECURING PERSONAL HEALTH RECORD AND SHARING IN THE CLOUD S. Meignana Prakash and M. Sudha	12
6	ENHANCED PRIVACY AND ACCESS CONTROL DISTRIBUTED DATA IN CLOUD THROUGH BLOCK CHAIN TECHNOLOGY V. Menaka and M. Sudha	15
7	HYPOGLYCEMIC AND HYPOLIPIDEMIC ACTIVITY OF *SHOREA ROBUSTA* BARK EXTRACT ON ALLOXAN INDUCED DIABETIC RAT P. Shobana Devi, Dr. M. Shabana Begum and Dr. M. Devi	19
8	MOLECULAR DOCKING STUDIES OF HIV- REVERSE TRANSCRIPTASE WITH *ENICOSTEMMA AXILLARE* S. Anbalagan and M. Sankareswaran	26
9	OPTIMIZING INFORMATION LEAKGAE IN MULTICLOUD STORAGE SERVICES A. Soundararajan and A. AnushaPriya	40
10	PHYTOCHEMICAL SCREENING AND ANTIDIABETIC ACTIVITY OF AQUEOUS EXTRACT OF *BLEPHARIS MADERASPATENSIS (*STEM) R. Banupriya and P. Dhivya	43
11	SECURE AND EFFICIENT DE-DUPLICATION OF ENCRYPTED DATA IN CLOUD USING E-ABE S. Keerthana and P. Subramaniam	49
12	SECURE IMAGE STORING AND SHARING IN CLOUD THROUGH DOUBLE STEP VERIFICATION B. Deepa and P. Subramaniam	52

ACCESS PRIVILEGE BASED DATA RETRIEVAL AND SECURE SHARING IN DECENTRALIZED MILITARY NETWORKS

Renuka. K & Sudha. M
Department of Computer Science,
Muthayammal College of Arts & Science, Rasipuram, Namakkal (Dt)-637408
Email:renukamark25@gmail.com

ABSTRACT

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-Tolerant Network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Cipher text-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

KEY WORDS - Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multi-authority, secure data retrieval.

INTRODUCTION

Mobile in many military network cases wireless device connections which is followed by soldier may be disconnected temporarily by connection jam, some environment factors and mobility, mainly when they operate in hostile environments. To communicate each other in these extreme networking environments DTN technologies are solution to allow the nodes. When there is no any end to end connection in between source and destination pair and massage from source node may wait on intermediate node for a substantial amount of time until the connection would be eventually established. In author define storage nodes in DTNs where data is stored or examined that only such mobile node can access necessary information quickly and efficiently [1,2]. The military applications required increased protection of confidential data with access control method that is cryptographically enforced. In most of the cases, it is desirable to provide different access service like data accesses policies are define over the user's attributes and roles, which are managed by the key authorities. For example, in a disruption-tolerant military network, on the storage node commander may store confidential data which is access by "Battalion A" who are participating in "Region B." We studied DNA architecture for handle multiple issues and independently manage own attribute keys as DTN [3]. The attributes based encryption is promising approach which is fulfill the requirement of secure data in DTNs. ABE features is a mechanism of enable access control over the encrypted data and ascribed attributes among private keys and cipher texts. One of the important things is cipher texts-policy ABE (CP-ABE) provided easier way of encryptor data such that the encryptor can describe the attribute keys that need to be process by descriptor and convert into cipher text [4]. However, the user can decrypt the data in

different way for security purpose. Hence, the problem of applying the ABE to DTNs introduces several security and privacy challenges.

MODULES

KEY AUTHORITIES

There are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users based on the users' attributes. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system, however they would like to learn information of encrypted contents as much as possible.

SENDER

This is an entity who owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

STORAGE NODE (Decentralized Server)

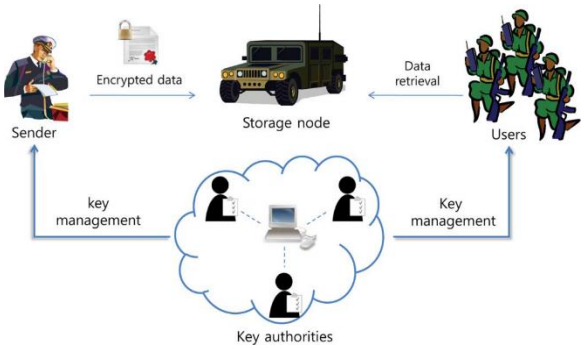
This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static. Similar to the previous schemes, we also assume the storage node to be semi-trusted.

SOLIDER (USER)

This is a node or user who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the cipher text and obtain the data.

CP-ABE METHOD

In Cipher text Policy Attribute based encryption scheme, the encryptor can fix the policy that who can decrypt the encrypted message?. The policy can be formed with the help of attributes. In CP-ABE, access policy is sent along with the cipher text [5]. We propose a method in which the access policy need not be sent along with the ciphertext, by which we are able to preserve the privacy of the encryptor. This techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.



CONCLUSION

DTN technologies are becoming successful solutions in military applications that allow wireless devices to correspond with one another and access the secret data dependably by abusing outside storage nodes. CP-ABE is an adaptable cryptographic answer for access control and to secure data recovery issues. In this task, an effective and secure data recovery strategy utilizing CP-ABE for decentralized DTNs where various key powers deal with their attributes independently has been executed. The intrinsic key escrow issue is determined such

that the secrecy of the stored data is ensured even under the antagonistic environment where key powers may be traded off or not completely trusted. In addition, the fine-grained key revocation should be possible for every attribute group data.

REFERENCES

[1] Roy, S., Chuah, M. (2009). Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs. Lehigh CSE Tech. Rep., 1–11.

[2] Chuah. M., Yang, P. (2007). Performance evaluation of content-based information retrieval schemes for DTNs. Proc. IEEE MILCOM, 1–7.

[3] Kallahalla, M., Riedel, E., Swaminathan, R., Wang, Q. & Fu, K. (2003). Plutus: Scalable secure file sharing on untrusted storage. Proc. Conf. File Storage Technol., 29–42.

[4] Harrinton, A. & Jensen, C. (2003). Cryptographic access control in a distributed file system. Proceedings of ACM SACMAT, 158–165.

[5] Ibraimi, L., Petkovic, M., Nikova, S., Hartel, P & Jonker, W. (2009). Mediated ciphertext-policy attribute-based encryption and its application. *Proc. WISA, LNCS* 5932: 309–323.

ACCURATE DETECTION OF SPAM MAIL TO SECURE USER INFORMATION THROUGH MACHINE LEARNING

Umamaheswari .S And Nirmala .A. M
Department of Computer Science,
Muthayammal College of Arts & Science, Rasipuram, Namakkal. (Dt)-637 408,
Email: uma74963@gmail.com

ABSTRACT

An industrial mobile network is crucial for industrial production in the Internet of Things. It guarantees the normal function of machines and the normalization of industrial production. However, this characteristic can be utilized by spammers to attack others and influence industrial production. Users who only share spams, such as links to viruses and advertisements, are called spammers. With the growth of mobile network membership, spammers have organized into groups for the purpose of benefit maximization, which has caused confusion and heavy losses to industrial production. It is difficult to distinguish spammers from normal users owing to the characteristics of multidimensional data. To address this problem, existing proposes a Spammer Identification scheme based on Gaussian Mixture Model (SIGMM) that utilizes machine learning for industrial mobile networks. It provides intelligent identification of spammers without relying on flexible and unreliable relationships. However already registered fake mail id has been stored in our database and new mail has been verified with the database through SIGMM in exact way.

The drawback is if new spam mail is generated detecting it is a difficult process. Therefore, in our proposed method through machine learning new spam mails are detected through stop word identification technique. In our proposed efficient and accurate detection of spam mail is done compared to existing methods.

KEY WORDS: SVM, NLP, SIGMM.

INTRODUCTION

Email is inclined to spam messages in view of its wide utilization and the majority of its advantages as a certified mechanism of correspondence. Spam mail has been identified through blacklist and already recognized spam mail ID that were stored in our database. By utilizing these approaches, we can identify spam mails that were available already in our database. In case of new spam mail has been arrived from a fresh mail ID it is difficult to detect. Hence in our proposed method we use NLP based stop word identification. In this system, based on datasets spam mail words are identified and stored in our database as stop words [1,2]. Then efficient classification has been done through SVM classifier which detect the words that are available in new mail. The identified words are checked with stop words list in database in accurate way through SVM classifier. The percentage level of words available in new mail is checked with database if it is maximum then it will be identified as spam mail and blocked otherwise it will be sent to the destination mail.

DATA PRE-PROCESSING STEPS

In filtering of spam, the pre-processing of the textual information is very critical and important. Main objective of text data pre-processing is to remove data which do not give useful information regarding the class of the document. Furthermore, we also want to remove data that is redundant. Most widely used data cleaning steps in the textual retrieval tasks are removing of stop words and performing stemming to reduce the vocabulary [3]. In addition to these two steps we also removed the words that have length lesser than or equal to two. The main pre-processing tasks applied in textual information retrieval tasks is the stemming. Stemming is a process of reducing words to its basic form by stripping the plural from nouns (e.g. “apples” to “apple”), the suffixes from verbs (e.g. “measuring” to “measure”) or other affixes. For example, applies, applying & applied matches apply.

STOP WORD REMOVAL

Sentence segmentation is boundary detection and separating source text into sentence. Tokenization is separating the input query into individual words.

Stop word removal: In any document narration the conjunction words do not play much role in the meaning of the document, so by discarding these words (like: is, the, for, an) from the documents which greatly reduces the overhead of processing

SVM

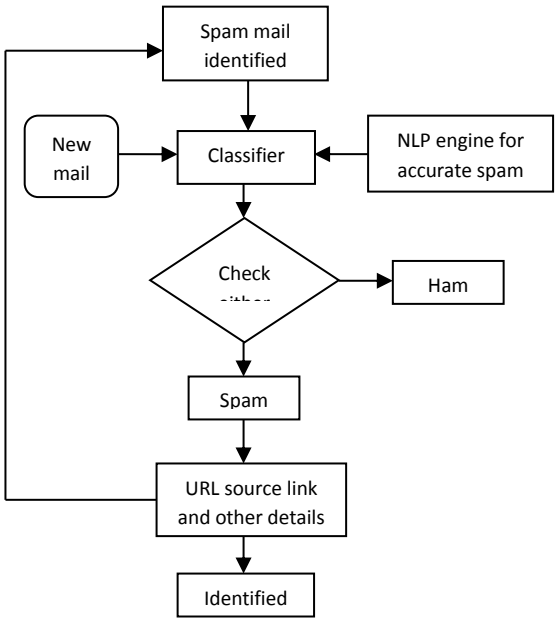
Support vector machine (SVM) is a supervised approach for machine learning. The main idea used in SVM is constructing a hyper plane that is optimal for the classification of patterns that can be linearly separated. In email spam detection the aim is to divide the email into two categories spam or ham email by using an optimal hyper plane. The idea is to distinguish the two classes to achieve maximum marginal difference between two classes, viz. spam and ham. SVM represents the information points in the workspace, mapped so that the information points of the other categories are partitioned by a maximum marginal difference. New information points are labeled to that same workspace and predictions are conducted to analyze the category of the new information point.

CONTENT BASED FILTERING

Content-based mail filtering (the system mainly discusses text format), you need to decrypt the message subject, body, and attachments. Then use natural language processing technology to express the message content (including attachments) by the semantic characterization. In this process, first, it need pre-treating the message content, including segmentation, feature extraction etc. Then, it need expand the characteristics items combining with knowledge database, form the vector and match the corresponding categories of the vector database to calculate the similarity of two vectors according to the weight vector, in order to judge the credibility of the message. Furthermore, the system analyses trust-email and non-trust email by self-learning feature, and adjust intelligent the weight of key words related topics, making higher accuracy of spam filters.

PERFORMANCE COMPARISSION

SYSTEM ARCHITECTURE



CONCLUSION

In this paper we review some of the most popular machine learning methods and of them applicability to the problem of spam e-mail classification. Descriptions of the algorithms are presented, and the comparison of their performance on the Spam Assassin spam corpus is presented, the experiment showing a very promising results specially in the algorithms that is not popular in the commercial e-mail filtering packages, spam recall percentage in the six methods has the less value among the precision and the

accuracy values, while in term of accuracy we can find that the Naïve bays and rough sets methods has a very satisfying performance among the other methods, more research has to be done to escalate the performance of the Naïve bays and Artificial immune system either by hybrid system or by resolve the feature dependence issue in the naïve bays classifier, or hybrid the Immune by rough sets. Finally, hybrid systems look to be the most efficient way to generate a successful anti-spam filter nowadays

REFERENCES

[1] Marsono, M. N., El-Kharashi, M. W. and Gebali F. (2008). Binary LNS-based naïve Bayes inference engine for spam control: Noise analysis and FPGA synthesis, IET Computers & Digital Techniques, 56-62.

[2] Muhammad, N. M., El-Kharashi, W. and Gebali F. (2009). Targeting spam control on middleboxes: Spam detection based on layer-3 e-mail content classification. Elsevier Computer Networks, 53(6), 835-848.

[3] Tang, Y., Krasser, S., He, Y. and Yang, W. (2008). Support Vector Machines and Random Forests Modeling for Spam Senders Behavior Analysis, IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference, New Orleans, LO, 1-5.

A DYNAMIC WEB CONTENT READER

Saranya. S & Anusha Priya. A
Department of Computer Science,
Muthayammal College of Arts & Science,Rasipuram,Namakkal(Dt)-637408
Email: 18pcs008@gmail.Com

ABSTRACT

With six meters highest visibility and 20 degrees maximum wide view, people who suffer from low vision are unable to see words and letters in ordinary newsprint. This fact makes the reading process becomes difficult that can disturb the learning process and slow the patient's intellectual development. Therefore, an application is needed to help them read easier. The challenges faced by visually impaired people in reading printed text in their day-to-day life are often not well understood. This project is based on a prototype which helps the user to listen to the contents of the live websites in Tamil, English, and Hindi etc. It involves the extraction of content from the websites and translates audio output in the languages mentioned above. This is done using python libraries with the concept of Natural Language Processing, Web Mining and Text-to-Speech. It is portable and easy to use thus providing a better reading experience to the visually challenged people as enjoyed by their sighted peers.

KEY WORDS: Tamil, English, Hindi, Natural Language Processing, Web Mining, Text-to-Speech.

INTRODUCTION

The complexity of the existing Braille system for the visually impaired people is that it requires the text to be translated to Braille literature. Translating a book or a document into Braille literature is a complex, time consuming and more expensive process. Day-to-day information cannot be translated into Braille literature [1]. To ease this process of reading for the visually impaired people, this prototype has been proposed. Using this prototype, text information can be converted into its equivalent audio format. This is done using python libraries with the concept of Natural Language Processing, Web Mining and Text-to-Speech [2]. It is portable and easy to use thus providing a better reading experience to the visually challenged people as enjoyed by their sighted peers. Remaining section describe about Existing System and Proposed System.

RESEARCH METHODOLOGY

EXISTING SYSTEM

The Existing system done by integrating camera module and speakers to Raspberry Pi 3 model B which is a credit card sized single board computer. Also, two other software called Tesseract and TTS engine (Text to Speech synthesizer) is installed to the Raspbian OS. Principally, the camera captures the image and stores it as an image file with a .jpg extension. The OCR engine converts it from image file to text file by extracting the numbers and characters of the language. The file is given as an input to a python program which gives a translated speech output using Google text to speech engine.

Text-to speech device consisted of three main modules, the image processing module, word correction module, and voice processing modules. Image processing module sets the object position, focus and illumination camera, taking pictures, and converting the image into text. Word correction module makes corrections to the output image processing module to improve accuracy by matching with Indonesian

dictionary. Voice processing module changes the writing into sound and process it with specific physical characteristics so that the sound can be understood.

The input image captured by the camera has a size of 5 MPI (2592 x 1944 pixels) or 215 ppi (pixels per inch). Based on the specifications of the Tesseract OCR engine, the minimum character size that can be read is 20 pixels uppercase letters. Tesseract OCR accuracy will decrease with the font size of 10pt. The image is taken by the user via GPIO pin that are connected to the tactile key using interrupt function. Furthermore, the picture is taken by using raspistill program with sharpness mode to sharpen the image. The resulting image has a .jpg format.
With a resolution of 2592 x 1944 pixels. Word correction module gets input from the image processing module in the form of text from the image processing module. Image processing module can't define truth or falsity of the word output, so that the correction module of this word, correction for whole words output from the image processing requires module. In order to improve the accuracy of the output image processing module, to design the word correction module.

PROPOSED SYSTEM

The complexity of the existing Braille system for the visually impaired people is that it requires, the text to be translated to Braille literature. Translating a book or a document into Braille literature is a complex, time consuming and more expensive process. Day-to-day information cannot be translated into Braille literature. To ease this process of reading for the visually impaired people, this prototype has been proposed. Benefits of the visually impaired are not necessary to learn any new language. The visually impaired can easily understand because different languages converted into native languages and hearable audio output. In the Proposed system, all external devices are avoided. In the Existing System, only can convert specific languages like Tamil and English. But, in the proposed system, establish multiple conversions of languages like English, Arab, Japanese and French etc. In the Proposed System, convert the dynamic web content using web mining and Natural language processing concepts. It is easy to use and portable. All kind of people can use this application. And content can easily understand by the visually impaired persons also other language peoples are able to understand the different languages in our native languages.

CONCLUSION

In this paper we present prototype system to assist the visually handicapped in writing compositions. The system can be seen as information probing and gathering environment.

REFERENCES

[1] Alvisi, L. and Marzullo, K. (1998). Message Logging: Pessimistic, Optimistic, Causal and Optimal. IEEE Transactions on Software Engineering, 24(2), 149–159.

[2] Anstreicher, K., Brixius, N., Goux, J.P. and Linderoth, J. (2002). Solving Large Quadratic Assignment Problems on Computational Grids. Mathematical Programming, 91, 563–588.

DATA RECOVERY IN MULTI THREAD

Manikandan. A and Subramaniam. P
Department of Computer Science,
Muthayammal College of Arts & Science, Rasipuram, Namakkal (DT)-637408
Email: manikd459@gmail.Com

ABSTRACT

Large applications executing on Grid or cluster architectures consisting of hundreds or thousands of computational nodes create problems with respect to reliability. The source of the problems is node failures and the need for dynamic configuration over extensive run-time. This paper presents two fault-tolerance mechanisms called theft induced check pointing and systematic event logging. These are transparent protocols capable of overcoming problems associated with both, benign faults, i.e., crash faults, and node or subnet volatility. Specifically, the protocols base the state of the execution on a dataflow graph, allowing for efficient recovery in dynamic heterogeneous systems as well as multi-threaded applications. By allowing recovery even under different numbers of processors, the approaches are especially suitable for applications with need for adaptive or reactionary configuration control. The low-cost protocols offer the capability of controlling or bounding the overhead. A formal cost model is presented, followed by an experimental evaluation. It is shown that the overhead of the protocol is very small and the maximum work lost by a crashed process is small and bounded.

KEY WORDS: Bank Manager, Account id and secret pin number, bank server, transaction server

INTRODUCTION

GRID and cluster architectures have gained popularity for computationally intensive parallel applications. However, the complexity of the infrastructure, consisting of computational nodes, mass storage, and interconnection networks, poses great challenges with respect to overall system reliability. Simple tools of reliability analysis increases complexity of the system, its reliability, and thus, Mean Time to Failure (MTTF), decreases [1,2]. If one models the system as a series reliability block diagram the reliability of the entire system is computed as the product of the reliabilities of all system components. For applications executing on large clusters or a Grid, the long execution times may exceed the MTTF of the infrastructure and, thus, render the execution infeasible [3]. As an example, let us consider an execution lasting 10 days in a system that does not consider fault tolerance. Under the optimistic assumption that the MTTF of a single node is 2,000 days, the probability of failure of this long execution using 100, 200, or 500 nodes is 0.39, 0.63, or 0.91, respectively, approaching fast certain failure. The high failure probabilities are due to the fact that, in the absence of fault-tolerance mechanisms, the failure of a single node will cause the entire execution to fail. Note that this simple example does not even consider network failures, which are typically more likely than computer failure. Fault tolerance is, thus, a necessity to avoid failure in large applications, such as found in scientific computing, executing on a Grid, or large cluster.

MODULE

CLIENT MODULE

Bank Manager can create Account for user via using their bank id. When Authenticated Bank manager can process and create account. After creating an account manager can activate their Account. After Activation only the user can processed using that Account id. After Activation user or banker can withdraw their amount through using their Account id and secret pin number [4]. After Activation user or banker can deposit their amount through using their Account id and secret pin number. Here bank transaction to other bank is to been processed. The transaction Account id checked to access their other bank. If account id is valid. Checks the Amount enter via user. After finishing the procedure amount to be transfer to other bank server. After transaction Process, Admin can view transaction from other server db. if transaction server gets failed (or) problem in maintenance. Client can be divert to grid Environment.

GRID MODULE

Grid is dynamic storage device. It must change their environment. Check pointing relies on periodically saving the state of the computation to stable storage. If a fault occurs, the computation is restarted from one of the previously saved states [5]. Since the computation is distributed, one has to consider the tradeoff space of local and global check pointing strategies and their resulting recovery cost. Thus, checks pointing based methods differ in the way processes are coordinated and in the derivation of a consistent global state. The consistent global state can be achieved either at the time of check pointing or at the time of rollback recovery.

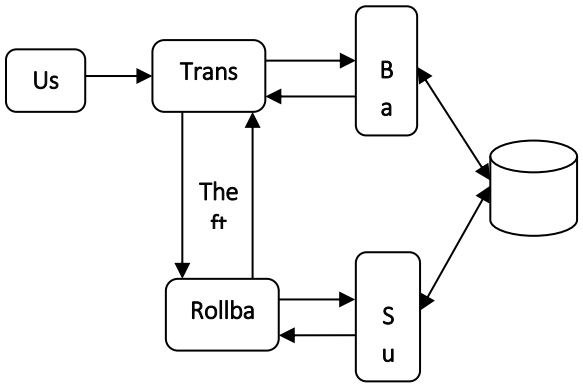
SERVER MODULE

Server can maintain db. If db gets failure. Server can choose dynamic grid server in network configuration. If system are active form ip list. They choose active system from dynamic setting. Here using semantic event logging backups are sending to other systems for timely updating. If server problem. Server can collect request from multiple client. If check for personal db. If problem found in server. it will divert to selected grid server from client request. But client can't get particular ip for grid. Because it will grid server to be changed.

RESEARCH METHODOLOGY

EXISTING SYSTEM

They depend on the prefigure configuration and consider 1) node and cluster failures as Well as operation-induced unavailability of resources and 2) dynamic topology reconfiguration in heterogeneous systems. Each fault in a system, may it be centralized or largely distributed, has the potential for loss of information, which then has to be re established. Recovery is, thus, based on redundancy. Several redundancy principles exit, i.e., time, spatial, and information redundancy.



PROPOSED SYSTEM

This paper presents two fault-tolerance mechanisms called Theft-Induced Check pointing and Systematic Event Logging. These are transparent protocols capable of overcoming problems associated with both benign faults, i.e., crash faults, and Node or subnet volatility. By allowing recovery even under different numbers of Processors, the approaches are especially

suitable for applications with a need for adaptive or reactionary configuration control

CONCLUSION

To overcome the problem of applications executing in large systems where the MTTF approaches or sinks below the execution time of the application, two fault-tolerant proto- cols, *TIC* and *SEL*, were introduced. The two protocols take under consideration the heterogeneous and dynamic characteristics of Grid or cluster applications that pose limitations on the effective exploitation of the underlying infrastructure. The flexibility of dataflow graphs has been exploited to allow for a platform-independent description of the execution state. This description resulted in flexible and portable rollback recovery strategies.

REFERENCES

[1] Alvisi L. and Marzullo, .K (1998). Message Logging: Pessimistic, Optimistic, Causal and Optimal. IEEE Trans. Software
Eng. 24(2), 149-159.

[2] Anstreicher, K., Brixius N, Goux, J-P & Linderoth, J. (2002). Solving Large Quadratic Assignment Problems on Computational. Grids. Math. Programming, 91, 563–588.

[3] Baldoni, R. (1997). A Communication-Induced Check pointing Protocol That Ensures Rollback-Dependency Trackability. *Proc. 27th Int'l Symp. Fault-Tolerant Computing (FTCS '97).*

[4] Baude, F. Caromel, D. Delb, .C. & Henrio, L. (2005). "A Hybrid Message Logging-CIC Protocol for Constrained Check pointability," Proc. European Conf. Parallel Processing *(EuroPar '05),* pp. 644-653.

[5] Bosilca G, Bouteiller A, Cappello F, Djilali S, Fedak G, Germain C, Herault T, Lemarinier P, Lodygensky O, Magniette F, Neri. V, Selikhov A. (2002). MPICH-V: Toward a Scalable Fault Tolerant MPI for Volatile Nodes. *Proc. ACM/IEEE Conf. Supercomputing (SC '02),* 29–29.

EFFICIENT MATHOD OF SECURING PERSONAL HEALTH RECORD AND SHARING IN THE CLOUD

Meignana Prakash. S & Sudha. M
Department of Computer Science,
Muthayammal College of Arts & Science,Rasipuram,Namakkal(Dt)-637408
Email: meignanaprakashselvam@gmail.com

ABSTRACT

The widespread acceptance of cloud based services in the healthcare sector has resulted in cost effective and convenient exchange of Personal Health Records (PHRs) among several participating entities of the e-Health systems. Nevertheless, storing the confidential health information to cloud servers is susceptible to revelation or theft and calls for the development of methodologies that ensure the privacy of the PHRs. Therefore, a methodology called SeSPHR for secure sharing of the PHRs in the cloud has been implemented. The SeSPHR scheme ensures patient-centric control on the PHRs and preserves the confidentiality of the PHRs. The patients store the encrypted PHRs on the un-trusted cloud servers and selectively grant access to different types of users on different portions of the PHRs. A semi-trusted proxy called Setup and Re-encryption Server (SRS) is introduced to set up the public/private key pairs and to produce the re-encryption keys. In our proposed RC4 algorithm is used to encrypt data and random key generator is used for every request. Moreover, the methodology is secure against insider threats and also enforces a forward and backward access control.

KEY WORDS: Personal Health Records (PHRs), SeSPHR, encrypted PHRs, semi-trusted proxy, Re-encryption Server (SRS)

INTRODUCTION

Today, personal health record (PHR) has risen as a standard of health report exchange. A PHR model allows a user (patient) to create, manage, and control health data at one central place through the technology of web, which has thus made storing, retrieval, and sharing of the information more efficient. Here each patient is allowed to take the full control of medical records and can share health information with a variety of users, including medical report providers, family members and friends. But while it is easier to have PHR services for everyone, but there can be many security and privacy risks which could slow down its acceptance. The main reason to worry about is whether the patients could control the sharing of their health information (PHI), specifically when they are stored on external servers where users may not fully assurance. On the other side, due to the susceptible health information (PHI), the external cloud storage servers are often at risk of various attacks which may lead to vulnerability of the PHI. To ensure users (patient) confidential control on their own PHRs, it is fundamental to have fine data access control model that works with non-trusted servers [1–3]. A basic idea would be to encrypt the data before storing on cloud. Here basically, the PHR owner should be able to decide how to encrypt files and to allow or not which users to retrieve access to each file. A PHR record file must only be accessible to the users who are given the decryption key, while it remains confidential to the other users [4]. Next would be that the patient shall always have the right to not only allow, but also be able to access authorization when they feel it is necessary. However, the patient-centric privacy is often in danger with amount of scalability in a PHR system. The certified users may either need to retrieve the PHR for own use

or authoritative use [5,6]. On the other side, different from the single data owner type which is often considered in most of the previous works, in a PHR system, there are numerous users who may encrypt according to their own possible ways, by using different sets of cryptographic keys. Here a concern would be, allowing each user acquire keys from every owner whose PHR wants to be read would limit the access since patients are not always online. So an alternative way would be to employ a central authority to do all the key management for all PHR owners, but this again requires too much trust on an authority.

MODULES

PATIENT LOGIN

First the patient/user needs to login the account. If he doesn't have account he has to register. During registration the random key is set in order to enhance more security. Once username and password matches with the database then particular patient can login to next form. Here he/she enters his/her complete biomedical data. These data are encrypted using the encrypt key. Later it is aggregated and that data is sent to cloud.

PATIENT DESCRIPTION

The patient will enter the details of his/her in the storage area. Using the file key the patient will encrypt the data and send to the cloud. The required file will be transferred to the doctor. RC4 algorithm is also known as symmetric cryptography, refers to cryptographic systems that require a pair of keys to operate: one key (the public key) is used to encrypt messages and, the other key (the private key) is used to decrypt them.

RANDOM KEY GENERATION

The doctor can download particular report of patient by satisfying attributes of owner of report. The patient will give the file to the doctor using the file key of decrypted data. So that the data will be fully secured and no one can able to access the file without the authentication key and the file key. After the patient sent the file, the doctor will receive the file. The doctor must open the file by sending the key request to the patient. After the patient viewed it, he/she can update the random key and the patient will send the original key to the doctor. With the authentication key and file key the doctor will process the file.

FILE ACCESSING BY DOCTORS

Here the data received from the client are accessed by the doctor by login to his account. The process is further preceded by requesting a random key to the patient. When the patient receives the message he sends the key to the doctor. The doctor accesses his required patient's details on successful matching of the key. Then the decrypted data is loaded initially. Then particular report is analyzed and prescription has been given by doctor and submitted to cloud. Once document is uploaded again accessing it using same accessing key is not possible. Therefore for every time accessing the file random key is generated and it should be matched to view the document.

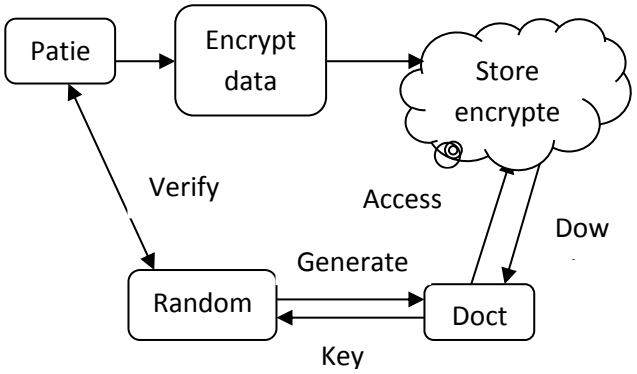


Figure – 1: Schematic representation of the proposed file accessing process

CONCLUSION

A structure of securely sharing of personal health records has been proposed in this paper. Considering partially trustworthy cloud servers, we know that to fully deploy the patient-status

concept, the patient's complete control over their own privacy. Attribute Based Encryption is a good technique to securing the Health records. It is efficient in the Conjunctive Property. The attribute-based encryption model is enhanced to support operations with MAABE. We utilize Attribute Based Encryption to encrypt the Health record data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications and affiliations. The system is improved to support dynamic policy management model. Thus, Personal Health Records are maintained with security and privacy.

REFERENCE

[1] Ming Li, Shucheng Yu, and Wenjing Lou, (2012). Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute based Encryption. IEEE Transactions on Parallel And Distributed Systems, 131–143

[2] Vida, M., Lupse O., & Stoicu-Tivadar, L. (2012). Improving the interoperability of healthcare information system through HL7 CDA and CCD standards. *7th IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI)*, Timisoara, 157-161.

[3] Vishal Jagdale, Dinesh Kekan, Ishwar Baride. (2015) Secure Sharing of Personal Health Records in Cloud using Attribute-based Encryption. , International Journal of Computer Science and Mobile Computing, Vol.4, 309-312.

[4] Ibraimi, L., Petkovic, M., Nikova, S., Hartel, P. & Jonker, W. (2009). Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes, Centre for Telematics and Information Technology (CTIT), 1–21.

[5] Zheng Y. (2011). Privacy-preserving personal health record system using attribute-based encryption. Master's thesis, Worcester Polytechnic Institute.

[6] Li, M., Yu, S., Cao, N. & Lou, W. (2011). Authorized private keyword search over encrypted personal health records in cloud computing. *31st International Conference on Distributed Computing Systems*, Minneapolis, MN, 383–392.

ENHANCED PRIVACY AND ACCESS CONTROL DISTRIBUTED DATA IN CLOUD THROUGH BLOCK CHAIN TECHNOLOGY

Menaka. V & Sudha. M
Department of Computer Science,
Muthayammal College of Arts & Science, Rasipuram, Namakkal (Dt) - 637408
Email: menakavks1998@gmail.com

ABSTRACT

Now more and more data are being outsourced to cloud services. In order to ensure data security and privacy, data are usually stored on the cloud server in the form of cipher text. When a user requests access to the encrypted data, an access key distributed by a third party is needed. However, if the third party is dishonest, the security of the system is threatened. To overcome this problem, we propose a new secured cloud storage framework with access control by using the block chain technology in this article. Our new scheme is a combination of block chain and cipher text-policy attribute-based encryption (CP-ABE). The proposed cloud storage framework is decentralized, so there is no trusted third party in the system. Our scheme has three main features. Firstly, using block chain technology the data owner can store cipher text of data through smart contracts in a block chain network. Secondly, the data owner can set valid access periods for the data usage, so that the cipher text can only be decrypted during valid access periods. Finally, as the creation and invocation of each smart contract can be stored in the block chain, the function of the trace is achieved. The analysis of the security and experiment shows that our scheme is feasible.

Keywords: *access control; encryption; blockchain; cloud; CP- ABE.*

INTRODUCTION

Nowadays, the increase and proliferation of large amounts of heterogeneous data (also known as Big Data) is generated in many fields, such as agriculture, business, finance/banking, education, medicine and healthcare [1]. This provides us with opportunities in the field of technology for another era of innovation and production. However, these heterogeneous data are continuously increasing and pose evident challenges, which necessitate more flexible data processing tools and platforms, in order to find useful information in data [2].

Blockchain technology makes use of cryptography in multiple different ways, for wallets, transactions, security, and privacy-preserving protocols [3]. It is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree). In addition, it is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way [4] [5] [6]. The blockchain is a simple yet ingenious way of passing information from A to B in a fully automated and safe manner. The transmitted information or transactions are grouped in blocks. Each block is verified by thousands, perhaps millions of computers distributed around the net. The verified block is added to a chain, which is stored across the net, creating not just a unique record, but a unique record with a unique history. Falsifying a single record would mean falsifying the entire chain in millions of instances. That is virtually impossible. Bitcoin uses this model for

monetary transactions, but it can be deployed in many others ways.

MODULE

CLOUD SERVER

Responsible for storing encrypted files uploaded by data owners. In this module, we allocate identity numbers to each and every user during registration. Using that we can collect information regarding the users present in the group. We can also send and receive files from the user in our group or individual. An individual or group entity, which owns its data stored in the cloud for online data storage and computing. Different users may be affiliated with a common organization, and are assigned with independent authorities on certain data fields.

BLOCK CHAIN

Deploy smart contracts on Block chain, the smart contracts is of interfaces to store data and get data. The file ID hash is used as an index of file information, and is recorded as Hash Field. DU's Ethereum account address is used as an index of user information, recorded as user Address. The Smart Contract defines two structures: file information named File and user information named User. File is used to store file related information, such as Hash Field. User is used to store user related information, such as user Address.

Since the code of the smart contract is stored in the block chain, the operation of the smart contract is also in the container provided by the block chain system. Combined with the cryptographic principles used by block chain technology, smart contracts are naturally tamper-proof and anti-counter-fitting. The results produced by the smart contract are also stored in the block, so that the execution from the source, the execution process and the result are all executed in the block chain, which ensures the authenticity and uniqueness of the release, execution and record of smart contract.

DATA OWNER (DO)

Responsible for creating and deploying smart contracts, uploading encrypted les, defining access control policies, assigning attribute sets and appending valid access periods to data users. The DO is the creator of the contract, and its Ethereum account address is recorded as owner. After the DO uploads the encrypted file to the cloud server, the setup algorithm is executed to obtain the public key and the master key. Through the execution of the smart contract, the relevant information of the file, such as cipher text, is stored in the block chain network, so that the data cannot be tampered with and all of operations are transparent. In addition, the data owner adds a valid access period while assigning attributes set to each data user.

DATA USER

Accessing an encrypted file stored in the cloud server. When its attribute set satisfies the access structure embedded in a given cipher text, it can decrypt the received cipher text to obtain the content key to decrypt the encrypted file. The effective access period for each data and user's access is stored in the block chain network through smart contract, making it impossible to tamper. The decryption can be successful only if the data consumer is within the valid access period and its set of attributes meets the access policy established by the data owner.

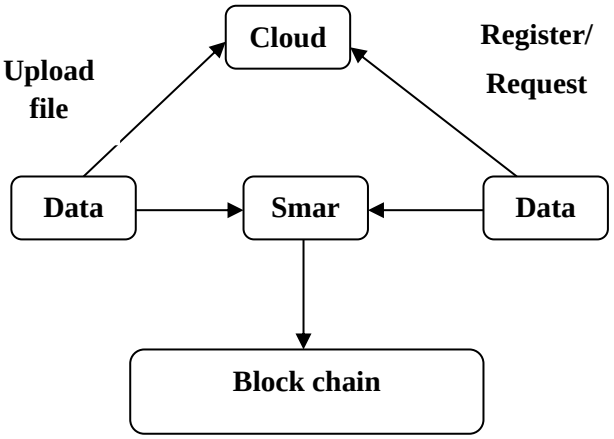


Figure – 1: Schematic representation of the proposed cloud storage framework

RESEARCH METHODOLOGY

EXISTING SYSTEM

Cloud is an emerging technology utilized widely by everywhere. In order to ensure the security of data and the privacy of users, data is usually stored on the cloud server in the form of cipher text. In order to achieve access control of the data, encryption technology can be regarded as a security guarantee. But achieving access control for encrypted data is a big challenge. In CP-ABE mode, a cipher text is associated with an access policy, and a user's private key is associated with an attribute set. The user can decrypt the given cipher text only if his attribute set satisfies the access policy established by the data owner. The data user obtains the corresponding key from the attribute authority centre according to the attribute set he owns. The data owner can control the access of the data according to access policy. In the CP-ABE scheme, one or more fully trusted attribute authorities or center authority are required. If the center authority is corrupted, it will endanger the entire system. Therefore, in the field of access control technology, decentralized system is necessary to get rid of the potential threat of trusted center authority.

PROPOSED SYSTEM

Block chain technology to a cipher text-policy attribute-based encryption algorithm is used, and use of smart contract technology to store the publically available information into the block chain network. At the same time to achieve the role of supervision and to track the behavior of the data access. All access records are recorded in the block chain network. A secure cloud storage framework with access control based on block chain is proposed, which is a combination of block chain and cipher text-policy attribute based encryption (CP-ABE) algorithm, the aim is to realize fine-grained access control for cloud storage. No trusted attribute authority is required in our scheme. The key information is stored in the block chain network by smart contract technology. Thus, decentralization is achieved in our cloud storage framework. When an attribute set is assigned to the data user, the data owner can append an effective access period for the data user, and store an access period time of information on the block chain. Only when the valid access period time and the attributes of data user satisfy the access control policy, the data user can perform data decryption algorithm correctly.

CONCLUSION

We created an efficient access control system in a big data environment using blockchain. Our system allows granular access control based on the blockchain scheme. The latter uses transactions to guarantee authentication, non-repudiation and integrity. We have demonstrated the feasibility of using blockchain technology to manage access control process for big data through the description of our proposed framework. The latter leverages the salient features of blockchain that are, distribution, full-fledged and append-only ledger to make a promising solution for addressing the access control challenges in big data. However adopting the blockchain technology to handle

access control functions is not straightforward. Additional critical issues emerge that are: The public aspect of the blockchain versus the private aspect of some access control policies and the inherent traceability problem. To address these issues, the encryption was used to encrypt attributes in the data owner's security policy and access requester's attributes to mask the transparency and visibility of the attributes to the public. Regarding the problem of traceability, we planned to ensure it in our next work.

We also used the ciphertext-policy Attribute Based Encryption (CP-ABE) scheme in order to add another security layer in our framework. This technology is a promising cryptographic primitive for the security of cloud storage system, which can bring fine-grained access control. In the future, we envision implementing our model using access control tools and Multichain for the blockchain. The results of this implementation would help us to evaluate the security level and performance of our proposed infrastructure.

REFERENCES

[1] Xia, D., Rong, Z., Zhou, Y., Wang, B., Li, Y. and Zhang, Z. (2013). "Discovery and analysis of usage data based on hadoop for personalized information access," in Proceedings - 16th IEEE International Conference on Computational Science and Engineering, CSE pp.917–924.

[2] Gudivada, V. N., Baeza-Yates, R. and Raghavan, V. (2015). "Big data: Promises and problems," Computer, 48: 20–23.

[3] Meng, W., Tischhauser, E., Wang, Q., Wang, Y. and Han, J. (2018) "When Intrusion Detection Meets Blockchain Technology: A Review," IEEE Access. 6: 10179-10188.

HYPOGLYCEMIC AND HYPOLIPIDEMIC ACTIVITY OF *SHOREA ROBUSTA* BARK EXTRACT ON ALLOXAN INDUCED DIABETIC RAT

Shobana Devi. P*, Dr. M. Shabana Begum and Dr. M. Devi
Department of Biochemistry
Muthayammal College of Arts and Science,
Rasipuram - 637408, Namakkal Dist, Tamil Nadu, India.
E-mail: shobirose2013@gmail.com

ABSTRACT
The present investigation was aimed at evaluating the hypoglycemic and hypolipidemic properties of the *Shorea robusta* bark extract have been screened for their protective effect against reactive Alloxan induced diabetes rats. They have been found to be effective antioxidant when administered in combination. The purpose of the study was to investigate the effect of administration (500mg/kgb.wts) for 15 days of the ethanol extract of *Shorea robusta*. The increase in Alloxan induced diabetes Group II LPO, GSH, Glucose, Hb, GlyHb & lipid profile (mg/dl) comparing to Group I & Group III. It is suggested to changes initially contract the oxidative stress in diabetes however; a gradual decrease in the antioxidative process may be one of the factors with result in chronic diabetes. These results indicate that the plant extract have shown antidiabetic activity & also reduced oxidative stress in diabetes. The results were statistically analyzed & indicate *Shorea robusta* bark extract showed better efficiency.

KEYWORDS: *Shorea robusta*, Alloxan, Diabetes, Hypoglycemic, Hypolipidemic.

INTRODUCTION
Type 2 diabetes is caused by the failure of beta cells to compensate for insulin resistance. This leads to hyperglycemia, which can in turn exert deleterious effects on β cells. A diabetic is a major health problem approximately 15% of the world's population suffering from diabetes. Independent forecasters however suggested that the global prevalence of the disease would increase from 150 million in 2000 to 220 million in 2010 and to 300 million by 2030. Diabetes is a disease where the body produces little insulin/ceases to produce insulin or becomes progressively resistance to its action [1].

There are estimated 143 million people worlds wide suffering from diabetics [2] almost five more than the estimates ten years ago. This number may probably double by the year 2030. Reports from the WHO indicate that mellitus is one of the major killers of our time, with people in South – East Asia & Western pacific begin most at risk [2]. There are two main categories of this disease Type 1 diabetes mellitus also called Insulin dependent & Type 2 diabetes mellitus also called non-insulin dependent.

In folk -tribal medicinal practice many plant are used to treat diabetic's mellitus in South India. Most of these medicinal plants are not scientifically validated for their therapeutically efficient & safety. Scientific studies on these plants are likely to provide invaluable anti – diabetic's drugs. The objective of the present study was to evaluate the hypoglycemic and hypolipidemic activity of an ethanol extract of the *Shorea robusta* bark in normal and alloxan-induced diabetic rats.

Shorea robusta is a large deciduous tree 18-30m in height with smooth or longitudinally fissured reddish brown or grey bark. Base cordate, 12-14 pans of lateral veins; stalks 2-2.5 cm long. Flowers yellow, in large showy branched clusters. Fruit ovoid, with five wings,

three long and two short the longer up to 7.5 cm long. The bark used as astringent, acrid, cooling, anthelmintic, alexeteric and tonic [4].

MATERIALS AND METHODS

PREPARATION OF EXTRACT

The bark of *Shorea robusta* was purchased from local Traditional medical shop at Thanjavur, Tamil Nadu. The bark was dried & soaked with ethanol (70%) for 48 hours. A semisolid extract was obtained after complete elimination of alcohol under reduced pressure. The extract was stored in refrigerator until used. The extract contained polar & non – polar phytocomponents of the plant medical used. The *Shorea robusta* bark extract was dissolved in distilled water just before oral administration.

ANIMALS

Male albino rats weighing about 120 – 180g were obtained from the Indian Institute of Bangalore. The animals were housed in polypropylene cages & maintained in controlled temperature with 12 hours period of light or dark & fed with standard rat feed & water were provided *ad libitum.*

DRUG ADMINISTRATION

Diabetic was induced by the intra peritoneal injection of Alloxan monohydrate (120mg/kg) dissolved in distilled water for 3 consecutive days. Diabetics was confirmed 2 days after the blood glucose concentration, treatments were started after confirmation of diabetic in rats.

EXPERIMENTAL DESIGNS

Body weight of animals was recorded & they were dividing into 3 groups of 6 animals each as follows.

Group I : Normal animal received normal diet & water *ad libitum*

Group II: Alloxan induced diabetic rats.

Group III: *Shorea robusta* treated with (500mg/kgb.wts) to diabetic rats for 15 days.

On completion of the experimental period, animals were anaesthetized with thiopentone sodium (50mg/kg). The blood was collected with & without EDTA as anticoagulant, Serum was separated by centrifuge.

BIOCHEMICAL ESTIMATIONS

S. No	Experiment	Methods
1	Estimation of Glucose	Trinder (1969) [5]
2	Estimation of Malondialdehyde	Nichans & samulson (1968) [6]
3	Estimation of Glutathione.	Ellman's (1959) [7]
4	Estimation of Triglycerides.	Werner *et al* (1981) [8]
5	Estimation of HDL Cholesterol.	Allain *et al* (1974) [9]
6	Estimation of Serum Cholesterol.	Allain et al (1974) [9]
7	Estimation of Haemoglobin.	Dacie & Lewis(1968) [10]
8	Estimation of Glycosylated Haemoglobin	Trivelli *et al* (1971) [11]

Statistical analysis

The results were presented at the mean ± SD. Data were statistically analyzed using student "t" test. P values lower than were considered as statistically significant.

Result

The Present study was carried out to evaluate the modulatory effect of *Shorea robusta bark* on alloxan induced diabetic mellitus. The observations made on different

groups of experimental animals and control animals were compared as follows.

EFFECT OF *SHOREA ROBUSTA* ON LPO & GSH IN NORMAL & EXPERIMENTAL RATS

Group II Alloxan intoxication rats showed a significant increase in the level of LPO when compare to Group I rats. Group III rats treated with *Shorea robusta* significantly decreased the level of LPO when compared to Group II. Group II Alloxan intoxicate rats showed the significant decrease in the level of GSH when compared to Group I rats. Group III rats treated with *Shorea robusta* significantly increases the level of Glutathione as compare to Group II.

Table I: Effect of *Shorea robusta* on LPO & GSH in normal & experimental Rats

Parameters	*Group I*	*Group II*	*Group III*
LPO(mg/dl)	49.32±2.41	85.41±3.71*	53.41±2.91
GSH(mg/dl)	37.9±6.4	26.9±4.5*	37.9±3.2

Values were expressed as Mean ± SD

*significantly different from Group I & Group II rats (P <0.05)

EFFECT OF *SHOREA ROBUSTA* ON GLUCOSE, HB & GLYHB IN NORMAL & EXPERIMENTAL RATS

Group II Alloxan intoxicated rats showed a significant increase in the level of glucose when compared to Group I rats. Group III rats treated with *Shorea robusta* significant decrease the level of glucose when compared to Group II. Group II Alloxan intoxicated rats showed a significant decrease in the level of Hb when compared to Group I rats. Group III rats treated with *Shorea robusta* significantly increase the level of Hb compared to Group II. Group II Alloxan intoxicated rats showed a significant decrease in the level of GlyHb when compared to Group I rats. Group III rats treated with *Shorea robusta* significantly decrease the level of GlyHb compared to Group II.

Table – II : Effect of *Shorea robusta* on Glucose, Hb & GlyHb in normal & experimental Rats

Parameters	*Group – I*	*Group –II*	*Group –III*
Glucose (mg/dl)	78.6±9.6	295.6±10.3*	87.8±15.5
Hb(mg/dl)	12.65±0.55	9.2±0.40*	12.25±0.59
GlyHb(mg/dl)	0.22±0.02	0.87±0.06*	0.25±0.04

Values were expressed as Mean ± SD

*significantly different from Group I & Group II rats (P< 0.05)

EFFECT OF *SHOREA ROBUSTA* ON BARKS EXTRACTS ON LIPID PROFILE IN EXPERIMENTAL RATS

Group II Alloxan intoxicated rats showed a significant increase in the level of Cholesterol, Triglyceride, VLDL & LDL-C when compare to Group I rats. Group III rats treated with *Shorea robusta* significantly decrease the level of Cholesterol, Triglyceride, VLDL & LDL- C when compare to Group II. Group II Alloxan intoxicated rats showed a significant decrease in the level of HDL – Cholesterol when compare to Group I rats. Group III rats treated with *Shorea robusta* significantly increase in the level of HDL when compare to Group II.

Table – III: Effect of *Shorea robusta* on barks extracts on lipid profile in experimental Rats

Parameters	Group I	Group II	Group III
Cholesterol (mg/dl)	79.32±15	159.55±15.68*	104.47±13.87
Triglycerides (mg/dl)	131.78±11.45	272.45±15.45*	144.85±12.45
HDL C (mg/dl)	29.52±2.72	19.12±1.5*	24.55±1.94
LDL (mg/dl)	44.68±4.64	144.13±4.88*	50.32±4.18
VLDL (mg/dl)	53.77±1.72	78.34±1.23*	52.31±1.14

Values are expressed as Mean ± SD for six rats

*significantly different from Group I & Group II rats (P<0.001)

Discussion

Diabetes mellitus is a growing health concern worldwide. The latest WHO publication estimates diabetes in adults to be around 173 million [12] and around two thirds of these live in developing countries. Diabetes mellitus is a metabolic disorder of the endocrine system. The disease occurs worldwide, and its incidence is increasing rapidly in most parts of the world. People suffering from diabetes are not able to produce or properly use insulin in the body, so they have a high level of blood glucose. Diabetes is becoming the third 'Killer' of mankind, after cancer and cardiovascular diseases, because of its high prevalence, morbidity and mortality [13].

Oxidation stress is increased in Diabetics because of multiple factors. Dominant among these factors is glucose antioxidation leading to the production of free radicals' glycation of protein alters protein & cellular function & binding of AGEs to their receptors can lead to modification in cell signaling & further production of free radicals [14].

Oxidation Stress Marker

LPO

Alloxan has been shown to induce free radicals' production and has tissues injury [15] free radicals damage to the cell membranes lipid peroxidation is one of the characteristic features of chronic diabetics. It has been observed that insulin secretion is closely associate with lipoxygenase derived peroxide the reduction of two electrons from alloxan gives dialuric acid, which undergoes oxidation & leads to generation of O_2, H_2O_2 & OH . Dialuric tied has been observed to stimulate lipid per oxidation in vitro. In this context a marked increase in the concentration of MDA was observed in diabetic's rats. But at the same time administration of *Shorea robusta* significantly decreased the levels of MDA diabetic rats. Thus it has anti lipid peroxidative effect.

GSH

Glutathione a tripeptide present in all the cells is an important antioxidant. Decreased glutathione levels in diabetics have been considered to be an indicator of increased oxidative stress. GSH also function as free radicals scavenger & in the repair of radicals caused biological damage of decrease level of GSH was observed in diabetic rats. The decreased in GSH level represents increased utilization, due to oxidative stress administration of *Shorea robusta* increased the content of GSH in diabetic rats.

Diabetic's markers of as Glucose

Diabetes mellitus is a disorder characterized by hyperglycemic at due to an absolute or relative deficiency of insulin & of insulin resistance. It affects 1-2% of the population worldwide hyperglycemia person important role in the pathogenesis of long – term complication. All

action induced diabetics has been observed to cause a massive reduction of the β – cells of the islet of the pancreases lading to hyperglycemia [16].

In our study we have found that decrease blood glucose in alloxan diabetic rats treated with the possible mechanism by which *Shorea robusta* bring about its hypoglycemic action may be potentiating the insulin effect of serum by increasing either the pancreatic secretion of Insulin from the β – cells of islet of Langerhans or its release from bound insulin. In this content a number of other plants have also observed to have hypoglycemic effects [17].

Cardiovascular risk in diabetic

We have noticed elevated serum in alloxan diabetic rats lipids play an important role in the pathogenesis of diabetic mellitus the level of serum lipids is usually raised in diabetics & such elevation represent a risk factor for coronary heart disease [18] the abnormal high concentration of serum lipids in diabetics is mainly due to the increase in the mobilization of free fatty acid from the peripheral departs , science insulin inhibits the hormone sensitive lipase, on the other hand. Glucagon's, Catecholamine's, & other hormones enhance lipolysis. The marked hyperlipidemic that characterized the diabetic state may be regarded as a consequence of the uninhibited actions of biolytic hormones on the deports [19].

In our study, we have also observed an increase in the concentration of Triglyceride, Cholesterol, VLDL, LDL – C & decrease in the HDL – Cholesterol in alloxan diabetic rats. Hyperlipidemia is a recognized consequence of diabetes mellitus [20]. Administration of *Shorea robusta* normalizes serum lipids. Diabetes induced Hyperlipidemia is attributable to excess mobilization of fats from adipose due to the under-utilization glucose.

Hemoglobin & GlyHb

In uncontrolled or poorly controlled diabetes is an increased glycosylation of a number of proteins including hemoglobin & α–crystalline of lens [21]. Glycosylated hemoglobin HbA_1 C was found to be increase in patients with the diabetic mellitus to approximately 16% [22] & the amount of increase is directly proportional to the fasting blood glucose level [23]. Amongst the various markers of glycemic control, glycated hemoglobin (GlyHb) has now been established as he most reliable, through many other proteins are also glycated in the diabetic [21]. In the present study, the lower of Hb & increase GlyHb content were observed in alloxan diabetics rats. During diabetics, the excess glucose present in the blood reacts with hemoglobin to form glycosylated Hemoglobin. Therefore, the total hemoglobin level is lowered & increased GlyHb in alloxan diabetic rats [24]. Administration of *Shorea robusta* reversed the total Hb & GlyHb content in alloxan diabetic rats.

CONCLUSION

Diabetes mellitus is the common endocrine disorder that affects more than 100 million people worldwide and in the next 10 years it may affect about five times more than it does now. In India the prevalence rate of diabetes estimated to be 1-5% complications are the major cause of morbidity and mortality in diabetic mellitus. There is an increasing demand by the use of natural products due to side effects associated with use of Insulin and oral hypoglycemic agents. Oral administration of *Shorea robusta bark* extract on alloxan induced diabetic rats exerts the following results. Restored the level of glycogen in experimental rats, improved the status of GSH and Heamoglobin content, Normalized the lipid profile in experimental rats, Reduced Gly Hb. Administration of *Shorea robusta to* alloxanized rats, restore the level of glucose, Hb, lipids, and reduce Gly Hb. Administration of *Shorea robusta* to alloxanized rats, restore the level of glucose, Hb, lipids and reduce Gly

Hb. Oxidative stress markers as MDA and GSH also reduced. These confirm the hypoglycemic and hypolipidemic activity of *Shorea robusta* in alloxan rats.

REFERENCES

[1] Wild, S., Roglic, G., Green, A., Sicree, R. and King, H. (2004). Golbal prevalence of diabetics: estimate for the year 2000 & projection for 2030. Diabetic care, 27, 1047 – 53.

[2] King, H., Rubert, R. E. and Herman, W. H. (1998). Diabetics care, 21, 1414 – 1431.

[3] Firshein, R. (2001). BioMed 8: 67–69.

[4] Prajapati, N. D., Purohit. S. Sharma, S. and Kumar T. (2006). A hand book of Medicinal Plants. A complete source book 3rd edition. Published by Agrobios (India) Jodhpur.

[5] Trinder P. (1969). Analytical Clinical Biochemistry, 6, 24.

[6] Nichaus, W. G. and sammuelson. B. (1968). Formation of malondialdehyde from phospholipids arachidonate during microsomal lipid peroxidation. European Journal of Biochemistry, 6(1), 126 – 130.

[7] Ellman-Arch, G. L. (1959). Tissue sulphydryl groups, Biochemical and Biophysical Research. 82, 70 – 77.

[8] Werner, M., Gabrielson, D. G. and Eastman G. (1981). Ultra-micro determination of serum triglycerides by bioluminescent assay. Clinical chemistry, 27, 268 – 271.

[9] Allain, C. C., Poon, L. S., Chan, C. S. G., Richmond, W. and Fu, P. C. (1974). Enzymatics determination of total serum cholesterol. Clinical chemistry, 20, 470-475.

[10] Dacie, J. V. and Lewis, S. M. (1968). Practical Heamo-tology, 4th Edition, J & A , Churchill, UK., 174.

[11] Trivelli, L. A., Ranney, H. M. and Lai, H.T. (1971). Hemoglobin components in patients with Diabetics mellitus. New England Journal of Medicine, 248, 353 – 357.

[12] Wild, S., Roglic, G, Sicree, Green A. and King, H. (2003). Global burden of diabetes mellitus in the year 2000, Global burden of Disease, Geneva.

[13] Li, W. L., Zheng, H. C., Bukuru, J. and De Kimpe N. (2004). Natural medicines used in the traditional Chinese medical system for therapy of diabetes mellitus. Journal of Ethanopharmacology. 92, 1-21.

[14] Penckofer, S., Schwertz, D. and Florczak, K. (2002). Oxidation stress & cardiovascular disease in type 2 diabetes: the role of antioxidants & prooxidants. Journal of Cardiovascular Nursing, 16(2), 68 – 85.

[15] Halliwell, B. and Gutteridge, J. M. C. (1992). Free radicals, antioxidants & human disease: where are we now? The Journal of Laboratory, 119, 598 – 620.

[16] Chattopathyay, R. R., Medd, C., Das, S., Balu, T. K, and Podder, G. (1993). Hypoglecimic and antihyperglycemic effect of *gymnema syivestre* leaf extract in rats. Fitoterapia, 64, 450 – 454.

[17] Chattopathyay, R. R., Chattopadhyay, R. N., Nandasy, A. K., Poddar, G. and Maitra, S. K. (1987). A preliminary report on anti–hyperlipidimic effects of an fraction of fresh leaves of *Azadichta indica* (Beng Neem), Bulletin of the Calcutta school of tropical medicine, 35, 29 – 33.

[18] Shanmugasundaram, K. R., Panneerselvam, C., Samudram, P. and Shanumugasundram, R. (1983). Enzyme changes & glucose utilization in diabetic rabbits. The effects of gymnema Sylvester, Journal of Enthnopharmacology, 7, 205 – 234.

[19] Al – Shamon, L. A., Al – Khazraji, S. M. and Twaij, H. A. (1994). Hypoglycemic effects of *Artemisia herba alba.* II. Effect of a valuable extract on some blood parameters in

diabetics animals. Journal of Ethnopharmacology, 43, 167- 171.

[20] Sharma, S. R., Dwivedi, S. K, and Swarup, D. (1997). Hypoglycemic, antihyperglycemic and hypolipidemic activity of *Caesalpinia bonducella* seeds in rats. Journal of Ethnopharmacology, 58, 39 – 44.

[21] Chandalia, H. B. and Krishnaswamy, P. R. (2002). Glycated heamoglobin. Current science, 83(12) 1522 – 1533.

[22] Koenig, R. J., Peterson, C. M., Jones, R. L., Saudek, C., Lehrman, M. and Cerami, A. (1976). Correlation of glucose regulation & heamoglobin A_1C in diabetes mellitus. The New England Journal of Medicine: Research and Review, 295, 417 – 420.

[23] Jackson, R. L., Hess, R. L. and England, J. D. (1979). Heamoglobin A_1C values in children with over diabetes maintained in varying degree of control. Diabetes Care, 2(5), 391 – 395.

[24] Sheela, C. G., and Augusti, K. T. (1992). Antidiabetic effects of S-allyl cysteine sulphoxide isolated from garlic Allium sativum Linn. Indian Journal of Experimental Biology, 30, 523 – 526.

Molecular Docking Studies of HIV- Reverse Transcriptase with *Enicostemma axillare*

Anbalagan S and Sankareswaran M
Department of Microbiology,
Muthayammal College of Arts and Science,
Rasipuram - 637408, Tamil Nadu, India

Abstract

Current research in drug discovery from medicinal plants involves a multifaceted approach combining botanical, phytochemical, biological, and molecular techniques. Medicinal plants drug discovery continues to provide new and important leads against various pharmacological targets including Cancer, HIV/AIDS, Alzheimer's, Malaria, etc. Several natural products drugs of plant origin have either recently been introduced to the United States markets, including art ether, galantamine, nitisinone, and tiotropium or currently involved in late-phase clinical trials. Realizing the importance of HIV/AIDS, knowing the immense value of Indian medicinal plants and attempt was made to study the antiviral properties of these plants, to investigate the antiviral, phytochemical screening and molecular docking of *Enicostemma axillare-Leaves* against HIV. The phytochemical analysis, antiviral, GC-MS analysis and molecular docking studies. Molecular docking studies of *Enicostemma axillare-Leaves* against HIV. The phytochemical study was done, the anti-HIV property of the plants was evaluated based on its ability to inhibit the HIV reverse transcriptase enzyme and several plants have shown potential HIV inhibitory activity *in-vitro*. The high-intensity signals obtained by GC-MS against methanolic extract of *Enicostemma axillare* contain fifteen spectra of compounds. The compound 2-chloroethyl linoleate was docked with HIV receptor (1W5V) and the dock score was 75.567. The results in the present study suggest that *Enicostemma axillare* leaf can be used in treating HIV. From the results obtained, it could be concluded that the herb exhibited excellent antiviral activity. Hence the objective of antiviral activity was satisfied. Such type of plant extract can find wide application in the pharmaceutical industries.

Keywords: Anti-viral activity, Anti-HIV inhibitory assay, phytochemicals, bioactive compounds, Molecular docking.

Introduction

Human immunodeficiency virus (HIV), the causative agent for acquired immunodeficiency syndrome (AIDS) belongs to family of Retroviridae. There is no satisfactory or curative treatment for this disease Acquired immunodeficiency syndrome caused by the human immunodeficiency virus (HIV), results in life-threatening opportunistic infections and malignancies. HIV leads to the destruction and functional impairment of the immune system, subsequently destroying the body's ability to fight against infections [1]. In 1981, the first patient diagnosed with acquired immunodeficiency syndrome (AIDS) in the USA was reported. The growing number of people living with HIV has constantly been detected the world over and in particular from the three main continents, Asia, South America and sub-Saharan Africa [2]. HIV infection is not a cause for termination of employment. As with many other illnesses, persons with HIV-related illnesses should be allowed to work for as long as they are medically fit for available, appropriate work.

Sexual behaviour is central to the epidemic spread of HIV and acquired immunodeficiency syndrome (AIDS). As of January 1992, an estimated 71% of HIV infection around the world was due to heterosexual behaviour and 15% was due to homosexual behaviour; only a

relatively small proportion was due to intravenous drug use [3]. The symptoms of AIDS are primarily the result of conditions that do not normally develop in individuals with healthy immune systems. Most of these conditions are opportunistic infections caused by bacteria, viruses, fungi and parasites that are normally controlled by the elements of the immune system that HIV damages [4].

People with AIDS also have an increased risk of developing various cancers such as Kaposi's sarcoma, cervical cancer and cancers of the immune system known as lymphomas. Additionally, people with AIDS often have systemic symptoms of infection like fevers, sweats (particularly at night), swollen glands, chills, weakness, and weight loss. The specific opportunistic infections that AIDS patients develop depend in part on the prevalence of these infections in the geographic area in which the patient live [5].

Antiretroviral drugs used in the treatment of HIV infection includes lamivudine, abacavir, zalcitabine, dideoxycytidine, tenofovir disoproxil fumarate, emtricitabine and stavudine. However, many different side effects are associated with the use of anti-HIV drugs. The occurrence of side effects plays a large role in adherence to drug regimens, which in turn can impact the development of drug resistance. Side effects such as nausea and diarrhea which affect drug absorption can also contribute to drug resistance.

Current anti-retroviral therapies available for symptomatic treatment of AIDS are quite expensive or unaffordable by common men and are associated with rapid emergence of drug resistance. Therefore, urgent need for new anti-HIV/AIDS drug is a global concern. Nature has been a source of medicinal agents for thousands of years and an impressive number of modern drugs have been isolated from natural sources. Anti-HIV inhibitory activity is widely distributed in nature in the form of medicinal plants. In this present study, the phytochemical evaluation and antiviral potentiality and molecular docking of predominant hit compounds with receptors of selected medicinal plants.

Current research in drug discovery from medicinal plants involves a multifaceted approach combining botanic phytochemica, biological and molecular techniques. Medicinal plant drug discovery continues to provide new and important leads against various pharmacological targets including cancer, HIV/AIDS, Alzheimer's, malaria and pain. Several natural product drugs of plant origin have either recently been introduced to the United States market, including ether, galantamine nitisinone and tiotropium, or are currently involved in late-phase clinical trials [6].

Medicinal plants are widely studied looking for new compounds possessing anti-HIV activity. Medicinal plants produce bioactive compounds used mainly for medicinal purposes. These compounds either act on different systems of animals including man, and/or act through interfering in the metabolism of microbes infecting them. A variety of natural products have been found to inhibit unique enzymes and proteins crucial to the life cycle of HIV including efficient intervention with the reverse transcription process, virus binding, and the integrase [7,8,9]. Till date, numerous papers have been published on the activity of various medicinal plants against the human immunodeficiency virus. Scientists from the developed and developing countries are in the quest for a natural product that will prove to be a therapeutic option against this deadly virus.

Enicostemma axillare is a perennial herb with sessile lanceolate leaves. The white flowers are arranged in clusters. This tropical genus is widely distributed in South America, Africa, and Asia. The plant is bitter, acrid, thermogenic, digestive, carminative, stomachic, laxative, anthelmintic, anti-

inflammatory, liver tonic, urinary astringent, depurative, revulsive, antiperiodic and is useful in dyspepsia, flatulence, colic, helminthiasis, abdominal ulcers, hernia, constipation, dropsy, swellings, vitiated conditions of kapha and vata, hepatopathy, glycosuria, leprosy, skin diseases, pruritus, intermittent fever and malaise. The plant is locally applied in snake bites [10-12]. Based on the importance of HIV/AIDS and knowing the immense value of Indian medicinal plants the present study was carried out to study the antiviral properties of certain Indian Medicinal plants against HIV virus.

Materials and Methods

Preparation of plant Extracts

The plant sample *Enicostemma axillare*- (Leaves*)* were washed, shade-dried, powdered and extracted in Hexane, Methanol, Ethanol, Chloroform, Petroleum ether and stored at 4°C until they were processed for biological evaluation. The solvent from the extract was removed under reduced pressure at 40 ºC. The solid was used in anti-viral assay after dissolving in Dimethyl-Sulphoxide (DMSO) considered that the maximum concentration of DMSO in the test solution should not exceed one percent.

Preliminary Phytochemical Screening

Various extracts collected from the shade-dried powdered leaves and seeds of all three plants were tested for identification of its active chemical constituents [13,14].

Test for alkaloids

To the small quantity of test solution, a few drops of diluted HCl was added and filtered. The filtrate may be tested carefully with various alkaloidal reagents such as,

a. Mayor's reagent – Creamy precipitate

b. Dragondroff's reagent – Orange-brown precipitate

c. Hager's reagent – Yellow precipitate

d. Wager's reagent – Reddish brown precipitate

Test for proteins and free amino acids

Dissolve small quantities of test solution in a few ml of water and treated with

1. ***Millon's reagent*** – appearance of red colour shows the presence of proteins and free amino acids.
2. ***Ninhydrin reagent*** – appearance of purple colour shows the presence of proteins and free amino acids.
3. ***Biuret test*** – Equal volume of 5% of sodium hydroxide and 1% solution of copper sulphate were added. Appearance of pink colour shows the presence of proteins and free amino acids.

Tests for anthraquinone glycosides

Borntrager's test: The small quantity of test solution was boiled with dil. Sulphuric acid and filtered. Benzene or ether is added to the filtrate and shaken well. An organic layer separates. To this ammonia is added. The layer becomes pink to red. It indicates the presence of anthraquinone glycosides.

Test for flavonoids

Shimoda's test**:** The small quantity of test solution is dissolved in alcohol, to that piece of magnesium followed by conc. HCl drop was added and heated. Appearance of magenta colour shows the presence of flavonoids.

Test for tannin and phenolic compounds

The small quantity of test solution was taken separately in water and tested for the presence of phenolic compounds and tannins with

1. Diluted ferric chloride solution (5%) – violet colour
2. 1% solution of gelatin containing 10% NaCl – white precipitate
3. 10 % lead acetate solution – white precipitate.

Test for carbohydrates

The small quantity of test solution was dissolved in 5 ml of distilled water and filtered.

The filtrate was subjected to test for carbohydrates.

a. Molisch' test: The filtrate was treated with 2-3 drops of 1% alcoholic alpha naphthol and 2 ml of concentrated sulphuric acid was added along the sides of the test tube.

b. Fehling's test: The filtrate was treated with 1 ml of Fehling's solution and heated. Orange precipitate was obtained shows the presence of carbohydrates.

Test for saponins

The small quantity of test solution was diluted with 20ml of distilled water and it was agitated on a graduated cylinder for 15 minutes. The presence of saponin was indicated by the formation of 1 cm layer of foam.

Test for phytosterol

Liebermann Burchard test

The small quantity of test solution was dissolved in few drops of dry acetic acid; 3 ml of acetic anhydride was added followed by few drops of conc. Sulphuric acid. Appearance of bluish green colour indicates the presence of Phytosterols.

Test for triterpenes

To the small quantity of test solution, add few Tin pieces and 3 drops of Thionyl chloride and appearance of violet or purple colour indicates the presence of triterpenes.

HIV-RT Inhibition assay: (www.roche-applied-science.com)

General recommendations for the quantification of the inhibitory effect of reverse transcriptase inhibitors, a reverse transcriptase (e.g. reverse transcriptase, HIV-1, recombinant) used in conjunction with the colorimetric Reverse Transcriptase Assay. For the quantification of the inhibitory effect of reverse transcriptase inhibitors in the current procedure, all steps of the Reverse Transcriptase Assay, including the RT reaction, can be performed directly in the MP modules supplied with the kit. Inhibitory activity of reverse transcriptase inhibitors is calculated as percentage inhibition as compared to a sample that does not contain an inhibitor. Therefore, an HIV-1-RT calibration curve is not required.

Additional reagents required:

Reverse Transcriptase, HIV-1, recombinant
Reverse Transcriptase inhibitors

Assay procedure

- 4–6 ng recombinants HIV-1-RT, diluted in lysis buffer (20 µl/well) was added in a separate reaction tube. Lysis buffer with no HIV-1-RT should be used as a negative control.
- 20 µl of RT inhibitors diluted in lysis buffer was added to 20 µl reaction mixture (solution 3a or 3b) per reaction tube and incubate for 1 hour at 37°C.
- Enough foil bags were opened for the number of MP modules to be used. Put them into the frame in the correct orientation. (The correct fitting ensures a tight support of the MP modules). MP modules are ready to use and need not be rehydrated prior to addition of the samples.
- 60 µl samples were transferred into the wells of the MP modules. The MP modules were covered with a cover foil and incubated for 1 hour at 37°C.
- Remove the solution completely. Rinse 5 times with 250 µl of washing buffer per well (solution 6) for 30 seconds each and remove washing buffer carefully.
- Add 200 µl of anti-DIG-POD working dilution (200 mU/ml, solution 5a) per well, cover the MP modules with a cover foil and incubate for 1 hour at 37°C.
- Remove the solution completely. Rinse 5 times with 250 µl of washing buffer (solution 6) for 30 seconds per well each and remove washing buffer carefully.

- Add 200 µl of ABTS substrate solution (solution 7) per well and incubate at +15 to +25°C until colour development (green colour) is sufficient for photometric detection (10–30 minutes).
- Using a microplate (ELISA) reader, the absorbance of the samples was measured at 405 nm (reference wavelength: approx. 490 nm).

Note: Shaking of microplates at 250 rpm during incubation with substrate solution can be employed to shorten the incubation period, but is not essential. If shaking is not carried out, gently tap on the side of the microplate was done before measuring absorbance to ensure a homogeneous distribution of the colored reaction product.

Gas Chromatography-Mass Spectroscopy (GC-MS)

The value of the technique is that it requires only microgram amount of material, that it can provide an accurate molecular weight and that it may yield a complex fragmentation pattern which is often characteristic of (and may identify) hat particular compound.

Mass spectroscopy, in essence, consists of degrading trace amounts of an organic compound and regarding the fragmentation pattern according to mass. The ample vapors diffuse into the low-pressure system of the mass spectrometer here it is ionized with sufficient energy to cause fragmentation of the chemical bonds. The resulting positively charged ions are accelerated in a magnetic field which disperses and permits relative abundance measurements of ions of given mass-to-charge ratio. The resulting record of ion abundance versus mass constituents, the mass spectral graph, which thus consists of a series of lines of various intensity at different mass units. In many cases, some of the parent compound will survive. The vaporization process will be recorded as a parent ion.

Those compounds which are too involatile to vaporize in the MS instrument converted to trimethyl silyl ethers, methyl esters, or similar derivatives [15]. Mass spectroscopy is frequently used in conjunction with GLC and the combined operation provides to go for a qualitative and quantitative identification of the many structurally complex components that may be present together in a particular plant extract.

Instrument Description

GC-Fisons instruments (Automated)
Modal : GC 8000 Series
Column : DBSMS size 0.25u ID X 0.25u X 30 m
Injection temperature - 25°C

Temperature programming:

Time	Rate / Min	**Temp (ºC)**
0	6	50
45	0	250

MS: Fisons instruments

Molecular docking

Retrieval of 3d structure for HIV

Step 1: Visited the website www.Google.com and in the search column entered RCSB and clicked the search button.

Step 2: The RCSB homepage was displayed.

Step 3: In the search column entered as HIV, then a list of receptors was displayed.

Step 4: From the list, structure of HIV was selected and then 3D structure of receptor was saved as 1w5v.pdb file format.

Selection of Ligand:

Step 1: Enter into google and type PubChem compound.

Step 2: Pubchem home page was displayed.

Step 3: In search box enter into a compound name.

Step 4: Select the structure for the compounds in .mol file format

Step 5: Load the structure into Discovery studio 2.1

Docking Process:
Before beginning the docking, it is necessary to specify a binding site of the receptor. LigandFit uses a method based on protein shape searching for cavities. Often the largest cavity is part of the ligand-binding site.

Step 1: In the Tools Explorer, selected the "protein report and utilities" by expanding it,

Step 2: Clicked the protein report. So that a text window was displayed with all the information about the PDB file.

Step 3: Clicked the "Split all" under the "protein report and utilities" to split the receptor into protein and non-protein parts. Non-protein parts were deleted.

Step 4: Under the "Binding site" from Tools Explorer, "Define protein molecule as Receptor" was selected.

Step 5: Selected the "Find sites from Receptor cavities" under the Binding site.

Step 6: A list of binding sites was opened in the hierarchy view.

Step 7: Load the 3-D Structure of Ligand
Step 8: Select the Receptor – Ligand interaction Protocol

Step 9: Set the Parameters

Step 10: Click RUN Button for docking process.

Step 11: Analysis the Results.

Step 12: From the results choose least Dock Score Value.

Result and Discussion
In the present study, the Antiviral activity, Phytochemical studies, GC-MS and Molecular docking of selected plant extracts have been investigated and the results were documented under various segments. Traditional medicines are used by about 60 percent of the world's population. Many medicinal plants produce a variety of compounds of known therapeutic properties

All the Extracts obtained from the medicinal plants were evaluated for their antiviral activity against HIV-reverse transcriptase enzyme, and the following results were obtained. The Hexane extract of *Enicostemma axillare* inhibited HIV-RT Table:1

A study with nineteen Chinese medicinal herbs was conducted [15] to evaluate their anti -HIV activity by virtue of their inhibition of the interaction of the HIV-1 gp120 and CD4 receptors and inhibition of the HIV RT activity. Similarly, Shuwen Liu et al [16] found that the extracts of two herbs, *Prunella vulgaris* and *Rhizoma cibotte*, showed potent HIV inhibitory activity. Veljko Veljkovic *et al.,* [17] stated that Flavonoid compounds represent an important natural source of antiretrovirals for AIDS therapy due to their significant anti-HIV-1 activity and low toxicity.
Petroleum ether extract of *Enicostemma axillare* found to possess steriods, sugars, alkaloids, and Phenolic groups, flavones, saponins, tannins and flavonones. ethanol extract had all the secondary metabolites except catechin, Saponins, and anthroquinone glycosides. Methanol extract did not show the presence of anthroquinone glycosides and amino acids. Hexane extract consists of

steriods, Sugars, and Phenolic groups, flavones, tannins and flavanones. In chloroform extract most of the components were absent except triterpenes, sugars, alkaloids, catechin, anthroquinone glycosides and amino acids Table:2

Retnam and John [18] investigated that the phytochemical analysis of a medicinal plant *Enicostemma axillare (Lam.)* for the identification of alkaloids, steroids, terpenoids, and flavonols by Gas Chromatography. Their study threw light on various alkaloids, steroids, terpenoids, and flavonols present in this medicinal plant which was proven by the present phytochemical studies which reveals the presence of Steroids, flavones, tannins and flavonones. The detected plant compounds were the bioactive molecules which exhibit antiviral property against HIV and HBV.

The predominant components present in all the extracts of *Enicostemma axillare* are steroid, Phenolic groups, flavones, tannins and flavonones. It is well known that many pharmacologically active components in herbal medicines are volatile chemical compounds and therefore Gas chromatography is very important in the analysis of herbal medicines**.** In the present study the plant extracts were subjected to GC-MS for the identification of spectrum of compounds. Only Hexane extracts of *Enicostema axillare* was subjected for this analysis.

The high intensity signals obtained by GC-MS against methanolic extract of *Teprosia uniflora* pronounced to contain spectrum of compounds such as -Propyl-Cis-Bicyclo(3,2,0)Hept-6-En-2-One,6-Octen-1-Ol,3,7-Dimethyl, Ethanoe,1(2,4,6-TrimethylPhenyl), 1(2H)Naphthalenone,3,4 Dihydro-6-Methoxy, 2-Propenoic Acid,3(3-Hydroxy Phenyl),Methyl Est, 2-FuranCarboxaldehyde,5(2-Furanyl Methyl), CycloDoDecane Methanol, 2-Chloro Ethyl Linoleate, 5,8,11-HeptaDecatrien-1-Ol, 1-Decanol.2-Hexyl, 3-Methyl-2(2-Oxopropyl) Furan, Z,Z-6,28-HeptatriactonTadien-2-One, CycloHexanol,4 Ethyl-4-Methyl-3(1-Methylethyl), CycloPentanone,2-(Methylpropyl), CycloHepta Decanol. The previous investigation carried out [19] and found to be correlated with the present GC MS analysis of *Enicostemma axillare* plant extracts. Table :3

Similar studies by Proestos *et al,* [19] on *Enicostemma axillare* explained that GC–MS can be used for characterization of different phenolics as trimethylsilyl derivatives. The antioxidant capacity was determined, in dried plants and in their methanol extracts, with the Rancimat test using sunflower oil as substrate. Both pulverized plants and extracts showed antioxidant capacity. Total phenolic content in the extracts was determined spectrometrically applying the Folin- Ciocalteu assay. It ranged from 2.9 to 28.2 mg gallic acid/100 g dry sample.

From the present investigation, *Enicostemma axillare*, was observed to have anti-HIV activity. The compounds therefore were isolated from the plant extracts and specific hit compounds (ligands), docked against the receptors of respective viruses to check their antiviral binding activity. The compound 2-chloro ethyl linoleate (CEL) from *Enicostemma axillare* was docked with HIV receptor (1W5V) and the dock score was 75.567. The hit compound cycloheptodecanol from *Enicostemma axillare* was docked with HIV receptor (1W5V) and the dock score was 53.288. (Fig 1,2,2a, 3,3a)

Singh *et al* [20] studied the chemokine receptor CXCR4 which is the receptor for several chemokines and major co-receptor for X4 Human Immunodeficiency Virus type-1 strains entry into cell. Subsequently, Harnett *et al* [21] screened the extracts made from *Sutherlandia frutescens* (L.) R. Br (Fabaceae) and *Lobostemon trigonus* (Boraginaceae) as identified by the Botany Department,

University of Port Elizabeth to detect if any of the extracts inhibited the human immunodeficiency virus (HIV)

CONCLUSION:

Viral diseases, such as acquired immunodeficiency syndrome (AIDS), respiratory viral diseases and hepatitis, are the leading causes of death in humans worldwide, despite the tremendous progress in human health care and medicine. The lack of effective therapies and/or vaccines for several viral infections and the rapid emergence of new drug-resistant viruses have urged a growing need for developing new and effective chemotherapeutic agents to treat viral diseases. Recent advances in the understanding of both the cellular and molecular mechanisms of virus replication have provided the basis for novel therapeutic strategies. Several hundred natural products have been isolated for screening and identifying antiviral activity and some have been shown to have great medicinal value in preventing and/or ameliorating viral diseases in preclinical and clinical trials. There are innumerable potentially useful medicinal plants and herbs waiting to be evaluated and exploited for therapeutic applications against genetically and functionally diverse virus families.

These natural active compounds, which contain more characteristics of high chemical diversity and biochemical specificity than standard combinatorial chemistry, offer major opportunities for finding novel lead structures that are active against a wide range of assay targets. In addition, natural products that are biologically active in assays are generally small molecules with drug-like properties capable of being absorbed and metabolized by the body. Hence, the development costs of producing orally active medicines are likely to be much lower than that of biotechnological products or most compounds produced to date from combinatorial chemistry. Therefore, natural products, including traditional medicinal plants (herbs), offer great promise as potentially effective new antiviral drugs

Tables and Figures

Table. No-1-Antiviral activity of *Enicostemma axillare*

S. No	**SOLVENT**	**HIV-RT Inhibition Assay**
1	*Hexane extract*	**Pos**
2	Methanol extract	Neg
3	Ethanol extract	Neg
4	Chloroform extract	Neg
5	Petroleum ether extract	Neg

Table. No-2: Preliminary Phytochemical screening of various extracts of the leaves of *Enicostemma axillare*

Constituents	**Petroleum ether**	**Ethanol**	**Methanol**	**Hexane**	**Chloroform**
Steroids	+	+	+	+	+
Triterpenes	-	+	+	-	-
Sugars	+	+	+	+	-
Alkaloids	+	+	+	-	-
Phenolic groups	+	+	+	+	+
Flavones	+	+	+	+	+
Catachin	-	-	-	-	-
Saponins	+	-	+	-	+
Tannins	+	+	+	+	+
Anthroquinone glycosides	-	-	-	-	-
Amino acids	-	+	-	-	-
Flavonones	+	+	+	+	+

Table. No-3: Gas Chromatographic Analysis of Methanolic extracts of Plant

S. No.	R.time	Compound name	Molecular Formula
1	7.10	Propyl-Cis-Bicyclo(3,2,0)Hept-6-En-2-One,	$C_{10}H_{14}O$
2	30.28	6-Octen-1-Ol,3,7-Dimethyl	$C_{10}H_{20}O$
3	30.69	Ethanoe,1(2,4,6-TrimethylPhenyl)	$C_{11}H_{14}O$
4	31.03	1(2H) Naphthalenone, 3,4 Dihydro-6-Methoxy	$C_{11}H_{12}O_2$
5	31.43	2-Propenoic Acid,3(3-Hydroxy Phenyl),Methyl Est	$C_{10}H_{10}O_3$
6	31.64	2-Furan Carboxaldehyde,5(2-Furanyl Methyl)	$C_{10}H_8O_3$
7	32.22	CycloDoDecane Methanol	$C_{13}H_26_O$
8	33.05	2-Chloro Ethyl Linoleate	$C_{20}H_{35}O_2Cl$
9	33.32	5,8,11-HeptaDecatrien-1-OL	$C_{17}H_{30}O$
10	33.60	1-Decanol.2-Hexyl	$C_{16}H_{34}O$
11	33.78	3-Methyl-2(2-Oxopropyl) Furan	$C_8H_{10}O_2$
12	34.41	Z,Z-6,28-HeptatriactonTadien-2-One	$C_{37}H_{70}O$
13	34.98	CycloHexanol,4 Ethyl-4-Methyl-3(1-Methylethyl)	$C_{12}H_{24}O$
14	35.17	CyclePentanone,2-(Methylpropyl)	$C_9H_{16}O$
15	35.69	CycloHepta Decanol	$C_{17}H_{34}O$

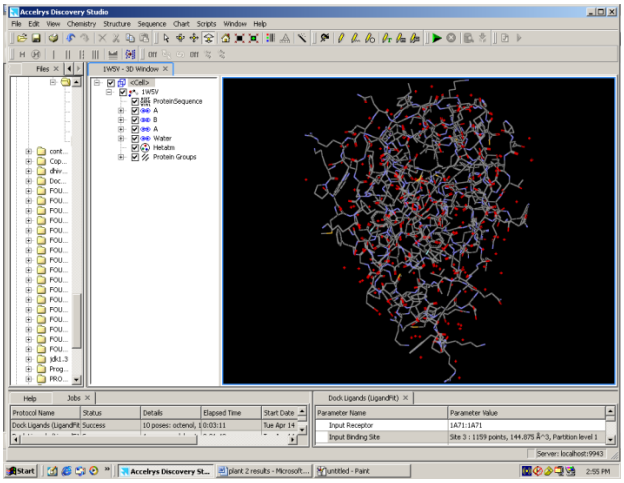


Figure (1): Structure of HIV (1W5V) receptor

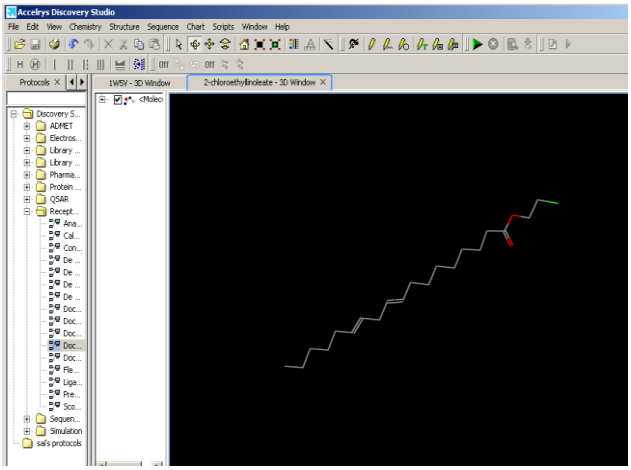
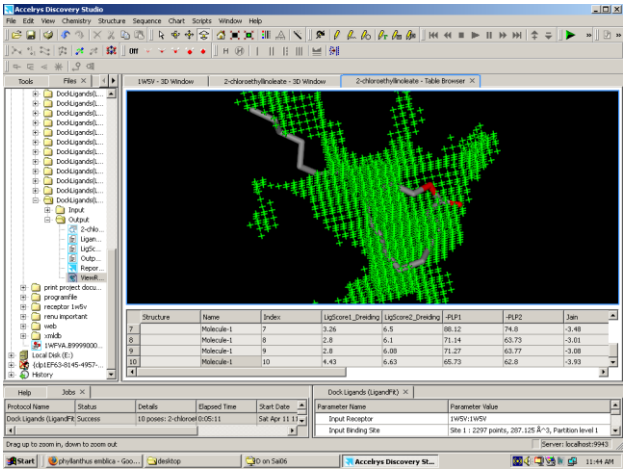


Figure (2): Structure of chloro ethyl linoleate first hit compound from *Enicostemma axillare*



	LigScore1_Dreiding	LigScore2_Dreiding	-PLP1	-PLP2	Jain	-PMF	LigScore Warning	DOCK_SCORE
1	3.57	6.37	79.19	74.03	-3.84	84.98	unfilled valencies:...	79.116
2	3.2	6.64	92.12	86.83	-4.01	81.67	unfilled valencies:...	77.911
3	3.34	6.24	81.93	74.09	-4.29	86.15	unfilled valencies:...	76.87
4	3.34	6.24	81.83	74.03	-4.3	86.09	unfilled valencies:...	76.865
5	3.89	6.89	83.55	72.52	-3.95	84.36	unfilled valencies:...	76.043
6	3.22	6.5	88.67	74.85	-3.47	80.76	unfilled valencies:...	75.783
7	2.8	6.1	71.35	64.04	-3.04	76.06	unfilled valencies:...	75.648
8	2.82	6.11	71.49	64.17	-3.08	76.38	unfilled valencies:...	75.644
9	3.13	6.18	79.69	74.36	-4.04	78.18	unfilled valencies:...	75.574
10	4.4	6.62	65.69	62.53	-3.96	92.65	unfilled valencies:...	75.567

Figure (2.a): Docked view of chloro ethyl linoleate from Enicostemma axillare with HIV (1W5V) receptor

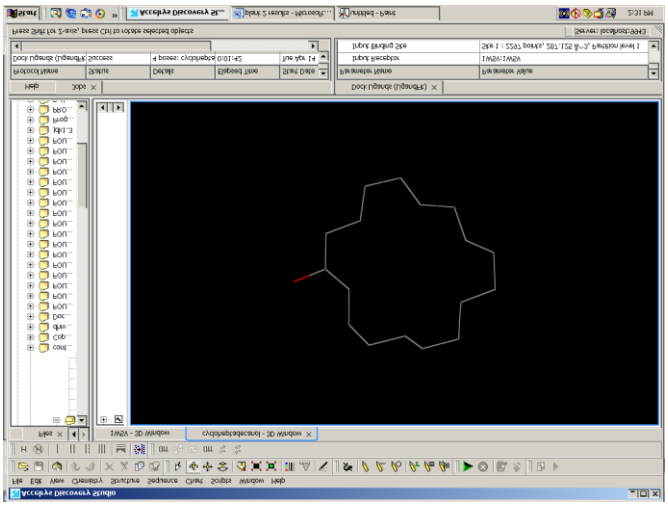
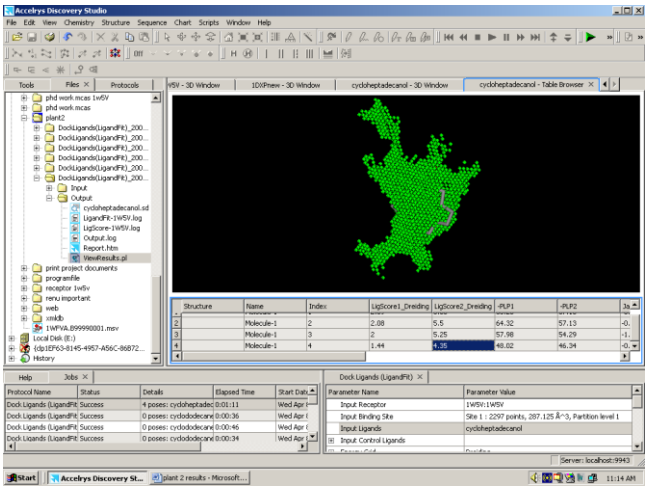


Figure (3): Structure of Cycloheptadecanol (second hit compound from *Enicostemma axillare)*



	^_Dreiding	-PLP1	-PLP2	Jain	-PMF	LigScore Warning	DOCK_SCORE	LF
1		63.81	59.91	-0.69	60.88	unfilled valencies:...	59.106	0
2		47.14	45.56	-1.2	75.2	unfilled valencies:...	58.496	0
3		60.66	54.68	-0.56	59.01	unfilled valencies:...	56.833	0
4		51.7	51.52	-1.09	68.1	unfilled valencies:...	53.288	0

Figure (3 a): Docked view of cyclo hepta decanol (second hit compound from *Enicostemma axillare)* with HIV receptor (1w5v)

Reference

1. Kanazawa, S. and Matija Peterlin, B. (2001). Repression of MHC determinants in HIV infection. Microbes and Infection 3: 467-73.
2. CDC. (1987). Revision of the CDC surveillance case definition for acquired immunodeficiency syndrome. MMWR Surveillance Summaries 36:1–15.
3. Judith Wasserheit. (1992). Epidemiological synergy; inter-relationship between Human Immunodeficiency Virus infection and other sexually Transmitted Diseases. Sexually transmitted diseases *19: 61-77*.
4. Holmes, C. B., Losina, E., Walensky, R. P., Yazdanpanah, Y., and Freedberg, K. A. (2003). Review of human immunodeficiency virus type 1-related opportunistic infections in sub-Saharan Africa. Clinical Infectious Diseases. 36: 652-62
5. Ng, T. B., Huang, B., Fong, W. P. and Yeung, H. W. (1997). Anti-human immunodeficiency virus (anti-HIV) natural products with special emphasis on HIV reverse transcriptase inhibitors. *Life Science*. 61: 933–949.
6. Balunas, M. J. and Kinghorn, A. D. (2005). Drug discovery from medicinal plants. Life Science. 78: 431-41.
7. Vlietinck, A. J., De Bruyne, T., Apers, S., and Pieters, L. A. (1998). Plant-derived leading compounds for chemotherapy of human immunodeficiency virus (HIV) infection. *Planta Medica*. 64: 97–109.
8. De Clercq E. (2000). Current lead natural products for the chemotherapy of Human Immunodeficiency Virus (HIV) infection. Medicinal Research Reviews. 20: 323-349.
9. Jung, M., Lee. S. and Kim, H. (2000). Recent studies on natural products as anti-HIV agents. Current Medicinal Chemistry. 7: 649–661.
10. Jaishree, V., Badami, S., Rupesh Kumar, M and Tamizhmani, T. (2009). Antinociceptive activity of swertiamarin isolated from *Enicostemma axillare*. *Phytomed*icine 16: 227-232.
11. Sharada-Deore, L., Khadabadi, S. S., Lalita, B., Ghorpade, D. S. (2008). In vitro antimicrobial and antioxidant studies on *Enicostemma axillare* (Lam.) Raynal. Leaves. Natural Product Radiance. 7: 409-412.
12. Pharmacognosy of Ayurvedic drug. Department of Pharmacognosy, University of Kerala; 1962, p.108-112.
13. Harborne, J. B. (1998). *Phytochemical Methods: A Guide to Modern Techniques of Plant Analysis*. (3rd edition). Chapman and Hall Co., New York. -302.
14. Kokate, C. K., Purohit, A. P. and Gokhale, S. B. (2003). *Pharmacognos*y. Nirali Prakashan, Pune 8: 1-624.
15. Collins, R. A., Ng, T. B., Fong, W. P., Wan. C. C and Yeung, H. W. (1997). A comparison of Human Immunodeficiency Virus type-1 inhibition by partially purified aqueous extracts of Chinese medical herbs. *Life Science*. 60: 345-351.
16. Liu, S., Jiang, S., Wu, Z., Lv, L., Zhang, J., Zhu, Z and Wu, S. (2002). Identification of inhibitors of the HIV-1 gp41 six-helix bundle formation from extracts of Chinese medicinal herbs *Prunella vulgaris* and *Rhizoma cibotte*. *Life Sciences*. 71: 1779–1791.
17. Veljkovic, V., Mouscadet, J.F., Veljkovic, N., Glisic, S and Debyser, Z. (2007). Simple criterion for selection of flavonoid compounds with anti-HIV

activity. Bioorganic & Medicinal Chemistry. 17: 1226–1232.

18. Retnam, K. R and John de britto, A (2003). Phytochemical analysis of a medicinal plant *Enicostemma axillare* (lam.) raynal, by gas chromatography. Journal of Economic and Taxonomic Botany.13: 172-179.
19. Proestos, C., Boziaris, I. S., Nychas, G. J. E and Komaitis, M. (2006). Analysis of flavonoids and phenolic acids in Greek aromatic plants: Investigation of their antioxidant capacity and antimicrobial activity. *Food Chemistry*. 95: 664–671.
20. Singh, S., Malik, B. K and Sharma, D. K. (2007). Targeting HIV-1 through molecular modeling and docking studies of CXCR4: Leads for Therapeutic Development. Chemical Biology & Drug Design. 69: 191–203.
21. Harnett, S. M., Oosthuizen, V and van de Venter, M. (2005). Anti-HIV activities of organic and aqueous extracts of *Sutherlandia frutescens* and *Lobostemon trigonus*. *Journal of Ethnopharmacology*. 96: 113–119.

OPTIMIZING INFORMATION LEAKGAE IN MULTICLOUD STORAGE SERVICES

Soundararajan, A. and Anusha Priya, A.
Department of Computer Science,
Muthayammal College of Arts & Science, Rasipuram, Namakkal (Dt) - 637408
Email: asoundar23@gmail.com

ABSTRACT

Many schemes have been recently advanced for storing data on multiple clouds. Distributing data over different cloud storage providers (CSPs) automatically provides users with a certain degree of information leakage control, for no single point of attack can leak all the information. However, unplanned distribution of data chunks can lead to high information disclosure even while using multiple clouds. In this article, we study the information leakage problem caused by unplanned data distribution in multi-cloud storage services. Then, we present an information leakage aware storage system in multi-cloud. To reduce duplicate while storing in multi-cloud efficient data detection is required therefore CP-ABE has been implemented. Similarly placing data in CSP is done through SJF algorithm which overcomes the issues faced in Round Robin (RR). To obtain result in efficient and effective way optimized query performance through indexing is implemented. Furthermore, our analysis on system attack ability demonstrates that our scheme makes attacks on information more complex.

Keywords: *Cloud storage provider (CSPs); multi-cloud storage services; unplanned data distribution; SJF algorithm; Round Robin (RR).*

INTRODUCTION

In general, all tasks that demand any type of parameter estimation from multiple sources can benefit from the use of data/information fusion methods. The term information fusion and data fusion are typically employed as synonyms; but in some scenarios, the term data fusion is used for raw data (obtained directly from the sensors) and the term information fusion is employed to define already processed data. In this sense, the term information fusion implies a higher semantic level than data fusion. Other terms associated with data fusion that typically appear in the literature include decision fusion, data combination, data aggregation, multi-sensor data fusion, and sensor fusion. Researchers in this field agree that the most accepted definition of data fusion was provided by the Joint Directors of Laboratories (JDL) workshop [1] [2]: “A multi-level process dealing with the association, correlation, combination of data and information from single and multiple sources to achieve refined position, identify estimates and complete and timely assessments of situations, threats and their significance.” Hall and Llinas [3] provided the following well-known definition of data fusion: “data fusion techniques combine data from multiple sensors and related information from associated databases to achieve improved accuracy and more specific inferences than could be achieved by the use of a single sensor alone.” Briefly, we can define data fusion as a combination of multiple sources to obtain improved information; in this context, improved information means less expensive, higher quality, or more relevant information. Data fusion techniques have been extensively employed on multi-sensor environments with the aim of fusing and aggregating data from different sensors; however, these techniques can also be applied to other domains, such as text processing. The goal of using data fusion in multi-sensor environments is to obtain a lower detection error probability and a higher reliability by using data from multiple distributed sources. The available data fusion techniques can be classified into three

nonexclusive categories: (i) data association, (ii) state estimation, and (iii) decision fusion. Because of the large number of published papers on data fusion, this article does not aim to provide an exhaustive review of all of the studies; instead, the objective is to highlight the main steps that are involved in the data fusion framework and to review the most common techniques for each step. This article also provides information on various classification categories available for data fusion techniques. Furthermore, we describe the most common methods for data association tasks and provide a review of techniques under the state estimation category. The most common techniques for decision fusion are enumerated followed by the conclusions obtained from reviewing the different methods.

MODULES

USER

In this module, the user has to create an account in the server for searching process. The user is allowed to register their detail for the server information surveillance. After the user has created their account, the user is allowed to search in records for the particular data to be retrieved. The query is given by the user to server.

SERVER

1. Assign the range: Server to perform the convert unsupervised data to supervised data operation based on some range. This module performs assigning the specified range for all websites.
2. Convert unsupervised data to supervised data: The problem of identifying duplicates has attracted much attention from many research fields, including Databases, Data Mining, Artificial Intelligence, and Natural Language Processing. In the Web database scenario, the records to match are highly query-dependent, since they can only be obtained through online queries. Moreover, they are only a partial and biased portion of all the data in the source Web databases.
3. Maintain the Data(s): After performing the conversion (unsupervised data to supervised data), the data will be maintained.

WEB SERVER

1. Data Collections: Web Server will collect all the data and maintain it.

2. Identifying a similarity function: Using training examples (i.e., manually labeled duplicate and non duplicate records) and a set of predefined basis similarity measures/functions over numeric and/or string fields, a single composite similarity function over one pair of records, which is a weighted combination (often linear) of the basis functions, is identified by domain experts or learned by a learning method, such as Expectation-Maximization, decision tree, Bayesian network or SVM

DUPLICATE RECORDS

The composite similarity function is used to calculate the similarity between the candidate pairs and highly similar pairs are matched and identified as referring to the same entity.

FUSION PROROGATION ALGORITHM

A framework of first and second order fusion functions has been developed and a distinction was made between backward and forward propagation. While back-ward propagation can be avoided with reasonable assumptions by intelligent design of the first order fusion function, forward propagation was shown to be more difficult. A propagation algorithm was proposed that relies on second order fusion functions to recursively fuse sets of linked tuples. Conflict resolution strategies are used to resolve conflicts in relationship attributes.

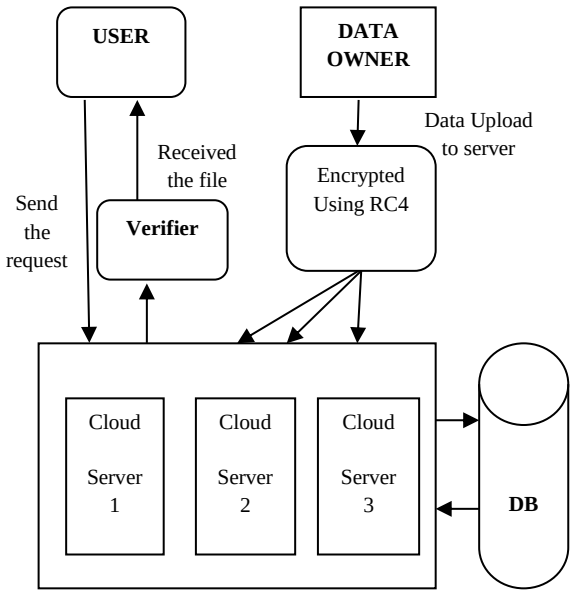


Figure – 1: Schematic representation of the proposed data fusion framework

CONCLUSION

In this study, a novel computational framework for power systems data fusion was proposed. Based on probabilistic graphical models, heterogeneous data sources and related measurement models (physical laws or data-driven machine learning models) can be combined such that a consistent and unified view of the system is obtained. An efficient and naturally distributed inference algorithm based on Gaussian belief propagation is also derived. In a set of numerical examples it was demonstrated how the traditional notion of state can be extended to provide visibility into the amount of solar generation at the buses of a network model. The fused information reduces the effect of noise in the various data sources and occurrences of missing or erroneous data are easily overcome and diagnosed. While fully known measurement functions were assumed, future work will investigate scenarios where they are partly unknown and need to be learned from the data. Further possibility for extensions of the state variable to include, for example, effects of temperature variation or of demand response programs on the active injections will also be investigated. Since the data consistency is one the key benefits of data fusion, extensions of traditional bad data analysis to the proposed framework is also of interest for future studies.

REFERENCE:

[1] Bleiholder, J. and Naumann, F. (2005). Declarative data fusion syntax semantics and implementation. *Proc. East Eur. Conf. Adv. Databases Inf. Syst.* 58-73.

[2] Naumann, F., Bilke, A., Bleiholder, J. and Weis, M. (2006). Data fusion in three steps: Resolving inconsistencies at schema- tuple- and value-level. The *Bulletin of Technical Committee on Data Engineering*, 21-31.

[3] Hall, D. L. and Llinas, J. (1997). "An introduction to multisensor data fusion," in *Proceedings of the IEEE*, 85: 6-23. doi:10.1109/5.554205.

PHYTOCHEMICAL SCREENING AND ANTIDIABETIC ACTIVITY OF AQUEOUS EXTRACT OF *BLEPHARIS MADERASPATENSIS (*Stem)

Banupriya.R * and Dhivya.P
Department of Biochemistry,
Muthayammal College of Arts and Science, Rasipuram, Namakkal, Tamilnadu.
Email: biobanupriya@gmail.com

ABSTRACT

In this study, phytochemical screening and antidiabetic activities of aqueous extract of *Blepharis maderaspatensis (stem)* was analyzed. The present findings showed the presence of phytochemicals such as carbohydrate, protein, aminoacids, sterols, flavonoids, alkaloids, saponins. The *in vitro* antidiabetic activity of *Blepharis maderaspatensis (stem)* was investigated by α-amylase inhibition assay. From this study it may be concluded that *Blepharis maderaspatensis (stem)* could have potential source of antidiabetic for pharmaceutical medicine preparations.

KEYWORDS: Phytochemical, antidiabetic, *Blepharis maderaspatensis.*

INTRODUCTION

In recent years, various medicines derived from medicinal plants are used to treat various diseases and this is not same in earlier times (Ghimeray *et al.*, 2009; Sultana *et al*., 2007). The significance of medicinal plant in drug development is known to us and humans have used them for separate diseases from the beginning of human history. (Fransworth .N, 2008). In plants any part of may contain active components such as leaves, stem, flowers, roots, fruits, bark and seeds (Gordon and David, 2001).

The phytochemical analysis of the plants is very important commercially and has great interest in pharmaceutical companies for the production of the new drugs for curing of various diseases. Phytochemicals are the chemicals that present naturally in plants. They are regarded as secondary metabolites because the plants that manufacture them may have little need for them (Tiwari .P, *et al*., 2011). Phytochemicals have been recognized as the basis for traditional herbal medicine practiced in the past and currently fashion in parts of the world (Lalitha T.P. *et al*., 2012). In the search for phytochemicals that may be of benefit to the pharmaceutical industry, researchers sometimes follow leads provided by local healers in a region (Das .K *et al*., 2010).

Diabetic mellitus (DM) is a condition arising due to abnormal metabolism of carbohydrate, promoted by factors, namely, insulin deficiency or insulin resistance. This disorder prevails worldwide with its occurrence increasing at an alarming rate globally. (Ashok K. T.*et al*., 2011). The effect of diabetes mellitus includes long term complications include heart disease, stroke, dysfunction and different diseases. (Keerthan.G, *et al*., 2013). Hence herbal remedies having high therapeutic efficacy with minimal side effects are favored. The antidiabetic agents from medicinal plants are very promising and traditionally acclaimed medicinal plants are being investigated for their antidiabetic potential (Babu V *et al.*, 2002; Parthasarathy .R *et al.*, 2009). Nearly 200 species of plant with hypoglycemic properties have been studied (Karthic .K *et al.*, 2008).

The plant *Blepharis maderaspatensis* is used to treat headache. Seeds are used as dysuria,

diseases of nervous system, diuretic, aphrodisiac (Mohan VR, *et al.,* 2010). It is used to cure cuts and wounds (Pandikumar .P *et al*., 2011), juice extracted from leaf is heated with gingelly oil and applied on affected places to heal wound (Ayyanar M and Ignacimuthu S, 2009).Dry seeds of this plant contain steroids and the plant is used for Brain disorders (Sandhya S, *et al.,* 2010).

MATERIALS AND METHODS

PREPARATION OF EXTRACT

The plant material used in present study was collected from Kolli hills, Namakkal district from Tamilnadu. Freshly collected stem was cleaned and dried under shade and the dried material was milled to obtain a coarse powder. The resulting materials were extracted with aqueous for 24 h by using soxhlet apparatus. The aqueous extract was filtered and then concentrated by using rotary evaporator to yield a semisolid mass. The residue obtained was stored in refrigerator for further study.

PRELIMINARY QUALITATIVE PHYTOCHEMICAL ANALYSIS

Preliminary qualitative phytochemical analysis was carried out to identify the secondary metabolites present in the aqueous extract of stem (J. B. Harborne ,1973).

IN VITRO ANTI- DIABETIC ACTIVITY

Assay of Alpha Amylase Inhibition (Narkhede *et al*., 2011)

A total of 500 µl of test samples and standard drug (25-125 µg/ml)were added to 500 µl of 0.02 M phosphate buffer (pH 6.9) containing α-amylase (0.5mg/ml) solution and incubated at 25°C for 10 min. 500µl of 1% starch solution in 0.02 M sodium phosphate buffer (pH 6.9) was added to each tube. The reaction mixtures were then incubated at 25°C for 10 min. The reaction was stopped with 1.0 ml of 3, 5 – dinitro salicylic acid color reagent. The test tubes were then incubated in a boiling water bath for 5 min, cooled to room temperature. The reaction mixture was then diluted adding 10 ml of distilled water and absorbance was measured at 540 nm.

The percentage inhibition of α-amylase activity was calculated using the following formula:

$$\text{Inhibition \%} = \frac{(\text{Absorbance of the control} - \text{Absorbance of the sample}) \times 100}{\text{Absorbance of the control}}$$

Acarbose, a known α-amylase inhibitor was used as a standard drug. The experiments were repeated thrice.

RESULTS

The preliminary phytochemical screening of aqueous extract of the *Blepharis materaseptansis* stem was carried out and they showed the presence of various phytocomponents.

Table:1 Phytochemical screening (Qualitative) for aqueous extract of *Blepharis materaspatensis* (stem)

S.NO	Phytochemical Constituents	Aqueous extract	Mechanism of action
1.	Carbohytrate	+	Blocks viral fusion
2.	Protein	+	Blocks viral fusion or adsorption
3.	Amino acid	+	Causes a decrease in G.I metabolism
4.	Alkaloids	+	Intercalates into cell wall and DNA of parasites
5.	Flavonoids	+	Complex with cell wall, binds to adhesion
6.	Sterols	+	Enhance intestinal absorption of Na and water.
7.	Phenol	-	Astringent action
8.	Saponin	+	Possess membrane permeablizing properties
9.	Terpenoids	-	Membrane disruption

(+) positive (-) negative

ANTI-DIABETIC ACTIVITY:

Alpha–amylase, as a key enzyme in the digestive system, is involved in the breakdown of starch into disaccharides and oligosaccharides and finally liberating glucose which is later absorbed into the blood circulation.

The results obtained revealed that there was a dose-dependent increase in percentage inhibitory activity of aqueous extract of *Blepharis maderaspetansis* stem of α-amylase enzyme at a concentration of extract showed a percentage inhibition.

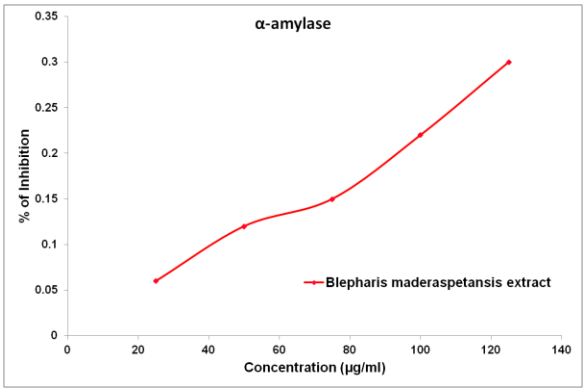


Figure 1: Effect of aqueous extract *Blepharis maderaspetansis* on α–Amylase inhibitory activity

DISCUSSION

Phytochemical analysis conducted on the plant extract revealed the presence of

constituents which are known to exhibit medicinal as well as physiological activities. Some of the characteristics of saponins include formation of Saponins has the property of precipitating and coagulating red blood foams in aqueous solutions, hemolytic activity, cholesterol binding properties and bitterness (Sodipo, O.A., *et al* 2000; Okwu D.E. , 2004). Steroids have been reported to have antibacterial propertiesand they are very important compounds especially due to their relationship with compounds such as sex hormones. (Raquel, F.E. 2007).

Alkaloids are secondary metabolities originating generally from amino acids and therefore, contain nitrogen in the molecular structure. Alkaloids are found in 15% of all plants. Flavonoids are naturally occurring substances in plants that are thought to have positive effects on human health (Montora, *et al*., 2005). The preliminary phytochemical analysis of *Blepharis Maderaspatensis* stem revealed the presence of high content of alkaloids, carbohydrates, flavonoids, protein and amino acids in aqueous extracts.

Diabetes is a chronic disease that occurs when the body cannot produce enough insulin or cannot use insulin effectively. (Zimmet P, 2004). Type 2 diabetes is a common condition and a serious global health problem. A person's risk of developing Type 2 Diabetes Mellitus has been shown to be highly linked to obesity and any family history of diabetes. (Sandoval S. 2009). Antidiabetic drugs used as monotherapy or in combination to achieve better glycemic control. Each of the oral antidiabetic agents is however, associated with a number of serious adverse effects. (Moller D.E., 2001; Nwaegerue E, *et al*., 2007) and none of the antidiabetic drugs could give a long term glycaemic control without causing the side effects (Singh S, *et al*., 2007).

Plant-based drugs have been known to be safe and cheaper and the plant plays the major role to manage the diabetes mellitus (Ahmed.I, *et al*., 2004; Karunanayake E.H. and Tennekoon K.H. 1993; Ribnicky DM., *et al., 2009*). In this study the *in vitro* amylase inhibitory activities of the aqueous extract of *Blepharis maderaspetansis* was investigated. The result of experiment showed that the aqueous extract of the plant exhibited potent amylase inhibitory activity in a dose dependent manner.(Keerthana G, *et al*., 2013).

CONCLUSION

It can be concluded that our results indicated that the aqueous extract of *Blepharis maderaspatensis* (stem) have the potential to act as a source of useful drugs and also to improve the health status of the consumers. The *Blepharis maderaspatensis* stem proved a potential medicinal plant for treatment of diabetes and showed the maximum inhibition of α- amylase activity. Further studies are also required to elucidate whether the plant have antidiabetic potential by in vitro for corroborating the traditional claim of the plant.

REFERENCES

Ahmed I, Adeghate E, Cummings E, Sharma AK, Singh J. Beneficial effects and mechanism of action of Momordica charantia juice in the treatment of streptozotocin-induced diabetes mellitus in rat. Mol Cell Biochem 2004, 261:63-70.

Ashok K. Madham T.S, Shaik A.B, Amtul, Z. S. Sachin B.A, and Kuncha M., "Identification of proglycemic and antihyperglycemic activity in antioxidant rich fraction of some common food grains," *International Food Research Journal* 2011, vol. 18, no. 3, pp. 883–891.

Ayyanar M and Ignacimuthu S. Herbal medicines for wound healing among tribal people in Southern India. Ethnobotanical and Scientific evidences. International Journal of Applied Research in Natural Products 2009, 2:3: 29-42.

Babu.V, Gangadevi .T, and Subramanian.A, "Antihyperglycemic effect of *Cassia keinii* leaf extract in glucose feed normal rats and alloxam induced diabetic rats," *Indian Journal of Pharmacology*, 2002,vol. 34, no. 6,. pp. 409–415,.

Das K., Tiwari R. K. S.,. Shrivastava D. K , J. Med. Plant Res., 2010, 4(2), 104-111.

Fransworth N, *The Role of Ethanopharmacology in Drug Development. Bioactive Compounds from Plant*, John Wiley & Sons, 2008.

Ghimeray, A.K., Jin, C.W., Ghimire, B.K., Cho, D.H. Antioxidant activity quantitative estimation of azadirachtin and nimbin in Azadirachta indica. A. Juss grown in foothills of Nepal. African J. Biotechnol. 8 (33), 2009, 3084–3091.

Gordon, M.C., and J.N. David,. Natural product drug discovery in the next millennium. Pharm. Biol. 39, 2001, Suppl., 1: 8-17.

Harborne J.B., *Phytochemical Methods*, Chapman and Hall, London, UK, 3rd edition, 1973.

Karthic K, Kirthiram K.S, Sadasivam S, Thayumanavan B , and Palvannan, T "Identification of *α* amylase inhibitors from *Syzygium cumini* Linn seeds," *Indian Journal of Experimental Biology*, vol. 46, no. 9, 2008, pp. 677–680.

Karunanayake EH, Tennekoon KH. Search of novel hypoglycemic agents from medicinal plants. In: Sharma AK. Diabetes mellitus and its complications. An update. Macmillan India Ltd, New Delhi, India; 1993.

Keerthana G, Kalaivani MK, Sumathy A: In-vitro alpha amylase inhibitory and anti-oxidant activities of ethanolic leaf extract of Croton bonplandianum. Asian J Pharm Clin Res, 2013; 6(4): 32-36.

Lalitha T.P, Jayanthi P, Asian J. Plant Sci. Res., 2012, 2(2), 115-122.

Mohan VR, Abragam AD, Kalidass C, Maruthupandian A. Pharmacognosy Journal ; 14: 2010,1-6.

Moller DE. New drug targets for type 2 diabetes and the metabolic syndrome. Nature 2001, 414:821-7.

Montoro P, Braca A, Pizza C, De Tommasi N. Strcture antioxidant activity relationships of flavonoids isolated from different plant species. Food chem. 2005, 92: 349-355.

Narkhede M. B, Ajimire P. V , Wagh A.E , Manoj Mohan and Shivashanmugam AT. In vitro antidiabetic activity of *Caesalpina digyna* (R.) methanol root extract. Asian Journal of Plant Science and Research, 2011, 1 (2): 101-106.

Nwaegerue E, Nweke IN, Ezeala CC, Unekwe PC. Glucose lowering effect of leaf extracts of Viscum album in normal and diabetic rats. J Res Med Sci 2007, 12:235-40.

Okwu, D.E. Phytochemicals and vitamin content of indigenous species of southeastern Nigeria. J.Sustain. Agric. Environ., 6(1): 2004, 30-37.

Pandikumar P, Chellappandian M, Mutheeswaran S, Ignacimuthu S. Consensus of local knowledge on medicinal plants among traditional healers in Mayiladumparai block of

Theni district, Tamil nadu, India. Journal of Ethnopharmacology 2011; 134 :2: 354-62.

Parthasarathy R, Ilavarasan R, and Karrunakaran C. M., "Antidiabetic activity of *Thespesia Populnea* bark and leaf extract against streptozotocin induced diabetic rats," *International Journal of PharmTech Research*, vol. 1, no. 4, 2009, pp. 1069–1072.

Raquel, F.E.. Bacterial lipid composition and antimicrobial efficacy of cationic steroid coppounds. Biochemica et Biophysica Acta. 2007, 2500-2509.

Ribnicky DM, Kuhn P, Poulev A, Logendra S, Zuberi A, *et al*. Improved absorption and bioactivity of active compounds from an anti-diabetic extract of Artemisia dracunculus L. Int J Pharm 2009, 370:87-92.

Sandhya S, Vinod KR, Sravan Kumar. Herbs used for Brain disorders. Journal for drugs and medicine 2010, 2:1: 38-45.

Sandoval S. Pima Indian Diabetes susceptibility differs significantly from European susceptibility. Biochem 2009, 118:1-8.

Singh S, Loke YK, Furberg CD. Thiazolidinediones and heart failure: a teleo-analysis. Diabetes Care 2007, 30:2148-53.

Sodipo, O.A., Akiniyi, J.A., Ogunbamosu, J.U. Studies on certain on certain characteristics of extracts of bark of Pansinystalia macruceras (K schemp) picrre Exbeille. Global J. Pure Appl. Sci., 6: 2000, 83-87.

Sofowra, A. Medicinal Plants And traditional Medicine In Africa. Spectrum Books Ltd., Ibadan, Nigeria, 1993, pp. 191-289.

Tiwari.P, Kumar.B, Kaur.M, Kaur.G, Kaur .H, Int. Pharm. Sciencia, 2011, 1, 98-106.

Wadkar K. A., Magdum C. S., Patil S. S., and Naikwade N. S., "Anti-diabetic potential and indian medicinal plants," *Journal of Herbal Medicine and Toxicology*, vol. 2, no. 1, 2008, pp. 45–50.

Zimmet P, Cowie C, Ekoe JM, Shaw J. Classification of diabetes mellitus and other categories of glucose intolerance. In: International Textbook of Diabetes Mellitus; 2004.

SECURE AND EFFICIENT DE-DUPLICATION OF ENCRYPTED DATA IN CLOUD USING E-ABE

Keerthana. S and Subramaniam. P

Department of Computer Science,
Muthayammal College of Arts & Science, Rasipuram, Namakkal (DT) - 637408.
Email: keerthanas090698@gmail.com

ABSTRACT

Attribute-based encryption (ABE) has been widely used in cloud computing where a data provider outsources the encrypted data to a cloud service provider and can share the data with users possessing specific credentials (or attributes). However, the standard ABE system does not support secure de-duplication, which is crucial for eliminating duplicate copies of identical data in order to save storage space and network bandwidth. In this article, we present an enhanced – attribute-based storage (E-ABE) system with secure de-duplication in a hybrid cloud setting, where a private cloud is responsible for duplicate detection and a public cloud manages the storage. Compared with the prior data de-duplication systems, our system achieves better performance. Firstly, it can be used to confidentially share data with users by specifying access policies rather than sharing decryption keys. Secondly, it achieves efficient duplication detection by considering the content together with file name, type and size respectively.

Keywords: *ABE; Credentials; E-ABE*

INTRODUCTION

Cloud storage involves stashing data on hardware in a remote physical location, which can be accessed from any device via the internet [1]. Clients send files to a data server maintained by a cloud provider instead of (or as well as) storing it on their own hard drives.

In proposed system, more number of user store their data in cloud environment to secure data encryption, which is widely used technique. This requires data to be stored in encrypted forms with access control policies such that no one except users with attributes (or credentials) of specific forms can decrypt the encrypted data. An encryption technique that meets this requirement is called attribute-based encryption (ABE), where a user's private key is associated with an attribute set, a message is encrypted under an access policy (or access structure) over a set of attributes, and a user can decrypt a cipher text with a private key if the set of attributes satisfies the access policy associated with the cipher text [2,3].

In the design of an attribute-based storage system supporting secured de-duplication of encrypted data in the cloud, in which the cloud will not store a file more than once even though it may receive multiple copies of the same file encrypted under different access policies. In the proposed model the content-based de-duplication is performed. Therefore, detection of duplication has been done in an efficient and accurate way.

METHODS

CLOUD GROUP CONSTRUCTION

In this module, we allocate identity numbers to each and every user during registration. Using that we can collect information regarding the users present and allows us to send and receive files from the user present in group. An individual or group entity, which owns its data stored in the

cloud for online data storage and computing. Different users may be affiliated with a common organization, and are assigned with independent authorities on certain data fields.

DUPLICATION IDENTIFICATION

In this module, the design of an attribute-based storage system supporting secure de-duplication of encrypted data in the cloud, in which the cloud will not store a file more than once even though it may receive multiple copies of the same file encrypted under different access policies. If same file is uploaded to cloud from different user, the file will be eliminated thus limiting wastage due to duplicate storage.

ATTRIBUTE AUTHORITY

The AA issues every user a decryption key associated with his/her set of attributes. The cloud consists of a public cloud which is in charge of data storage and a private cloud which performs certain computation such as tag checking. When sending a file storage request, each data provider firstly creates a tag T and a label L associated with the data, and then encrypt the data under an access structure over a set of attributes.

FILE DECRYPTION

At the user side, each user can download an item, and decrypt the cipher text with the attribute-based private key generated by the AA if this user's attribute set satisfies the access structure. Based on access policy, user-requested key through AA is received by verifying its access policy by data provider. Then data provider will transmit the key to respective user and particular user will decrypt the downloaded file using secret key.

Compared with the prior data de-duplication systems, our system achieves better performance. Firstly, it can be used to confidentially share data with users by specifying access policies rather than sharing decryption keys. Secondly, it achieves efficient duplication detection by considering the content also in addition to file name, type and size respectively.

RESULTS AND DISCUSSION

EXISTING METHOD

In existing system, the standard ABE system fails to achieve secure de-duplication, which is a technique to save storage space and network bandwidth by eliminating redundant copies of the encrypted data stored in the cloud [4][5]. On the other hand, to the best of our knowledge, existing constructions for secure de-duplication are not built on attribute-based encryption. Nevertheless, since ABE and secure de-duplication have been widely applied in cloud computing, it would be desirable to design a cloud storage system possessing both properties. If two different users upload the same content then this duplicated storage wastes storage space and communication bandwidth.

PROPOSED METHOD

In proposed system, more number of user store their data in cloud environment to secure data encryption is widely used technique. This requires data to be stored in encrypted forms with access control policies such that only users with attributes (or credentials) of specific forms can decrypt the encrypted data. An encryption technique that meets this requirement is called Enhanced - attribute-based encryption (ABE), where a user's private key is associated with an attribute set, a message is encrypted under an access policy (or access structure) over a set of attributes, and a user can decrypt a cipher text with his/her private key if his/her set of attributes satisfies the access policy associated with this cipher text.

In the design of an attribute-based storage system supporting secure de-duplication of encrypted data in the cloud, in which the cloud will not store a file more than once even though it may receive multiple copies of the same file encrypted under

different access policies. In our proposed content based de-duplication is performed. Therefore, detection of duplication has been done in efficient and accurate way.

CONCLUSION

Compared with the prior data de-duplication systems, our system achieves better performance. Firstly, it can be used to confidentially share data with users by specifying access policies rather than sharing decryption keys. Secondly, it achieves efficient duplication detection by considering the content also in addition to file name, type and size respectively.

REFERENCES

[1] Duan, Q., Yan, Y. and Vasilakos, A.V. (2012). A Survey on Service-Oriented Network Virtualization Toward Convergence of Networking and Cloud Computing Network and Service Management. IEEE Transactions on. 9: 373 – 392.

[2] Marwaha1, M. and Bedi, R. (2013). Applying Encryption Algorithm for Data Security and Privacy in Cloud. International Journal of Computer Science Issues. 10: 367 – 370.

[3] Gartner worldwide total public cloud Market. http://www.gartner.com/newsroom/id/2352816.

[4] Arshad, J., Townend, P. and Xu. J. (2009). Quantification of Security for Compute Intensive Workloads in Clouds Parallel and Distributed Systems (ICPADS). 15th International Conference on Parallel and Distributed Systems, Shenzhen. 479-486, doi: 10.1109/ICPADS.2009.46.

[5] Sahai, A. and B. Waters. (2005). Fuzzy Identity-Based Encryption. In: Cramer R. (eds) Advances in Cryptology– EUROCRYPT 2005. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg. 3494: 457–473. https://doi.org/10.1007/11426639_27

SECURE IMAGE STORING AND SHARING IN CLOUD THROUGH DOUBLE STEP VERIFICATION

Deepa. B and Subramaniam. P

Department of Computer Science,
Muthayammal College of Arts & Science, Rasipuram, Namakkal (DT) - 637408
Email:bdeepabalu12@gmail.com

ABSTRACT

Cloud computing is an emerging technology utilized widely due to its various advantages. However, the major issue faced here is security in maintaining files. Our proposed work focuses on storing and retrieving of image data in secure way in cloud through double step verification. In general, cryptography is utilized to store data in secure way. The key logic is when there is less security automatically data will be reveal to unauthorized users. In our proposed method, these issues are overcome through double-step verification. Initially image has been encrypted through Attribute Based Encryption (ABE). In addition to provide better security repository encryption has been implemented by RC4 approach. This will provide better security for user data in cloud through this two step verification. To ensure originality of user image watermarking technique has been implemented. Therefore it ensures without user knowledge an unauthorized user could not get the original image. Hence our system achieves maximum security compared to other existing approaches.

Key words: *security; cloud; ABE; repository encryption; water marking.*

INTRODUCTION

The cloud is designed to hold a large number of encrypted documents. With the appearance of distributed computing, developing number of customers and driving associations have begun adjusting to the private stockpiling redistributing [1]. This permits asset compelled customers to secretly store a lot of encoded information in cloud requiring little to no effort. Distributed storage administrations have a few focal points, for example, convenience and cost sparing, and they are generally utilized in numerous fields. Be that as it may, a few difficulties are related with them. With the expanding notoriety of distributed storage, security issues have turned into a critical factor confining its advancement. To counter the data spillage, information proprietors and endeavors normally re-appropriate the encoded business information, instead of the plaintext information, to distributed storage servers [2]. Visual information is in charge of one of the biggest offers of worldwide Internet traffic in both corporate and individual use situations. The measure of pictures, designs, and photographs being produced and shared each day, particularly through cell phones, is developing at a regularly expanding rate. The regular way to deal with location protection in this setting is to scramble touchy information before re-appropriating it and run all calculations on the customer side. Anyway this forces unsuitable customer overhead, as information should ceaselessly be downloaded, decoded, prepared, and safely re-transferred.

To address these difficulties we propose another safe structure for protection safeguarding redistributed capacity, pursuit, and recovery of vast scale, progressively refreshed picture archives. We base our proposition on IES-CBIR, a novel Image Encryption Scheme (IES) with Content-Based Image Retrieval (CBIR) properties [3]. Key to the structure of IESCBIR

is the perception that in picture preparing, unmistakable component types can be isolated and encoded with various cryptographic calculations. For instance, picture shading and surface information can be isolated so that CBIR in the scrambled space can be performed on one component type while alternate remains completely randomized and ensured with semantically-secure cryptography.

DATA SECURITY PROPERTIES

As mentioned earlier there are some properties we need to ensure with data when utilizing the cloud: Privacy: Privacy is one of the more imperative issues to manage in the cloud and in system security when all is said in done. Security guarantees that the individual data and character of a CSC are not uncovered to unapproved clients. This property is most vital to the CSC, particularly when they manage delicate information.

CONFIDENTIALITY

This is identified with information security since this is the property guaranteeing that the information that has a place with a CSC isn't uncovered to any unapproved parties. In open mists, the CSP is essentially in charge of verifying the CSC's information. This is especially troublesome due to multi occupancy, since various clients approach similar equipment that a CSC stores its information. A few suppliers use work booking and asset the board, however most suppliers utilize virtualization to expand the utilization of equipment. These two techniques enable assailants to have full access to the host and cross-VM side channel assaults to separate data from an objective VM on a similar machine. Integrity: The integrity of information alludes to the certainty that the information put away in the cloud isn't modified in any capacity by unapproved parties when it's being recovered, for example you get out what you put in. To guarantee this, CSPs must ensure that no outsider approaches information in travel or information away. Just approved CSCs ought to most likely change their information.

AVAILABILITY

This property guarantees that the CSC approaches their information, and is not denied access incorrectly or because of vindictive assaults by anyelement. Assaults like refusal of-administration are commonly used to preclude accessibility from securing information.

RELATED WORKS

Lu, *et al.* [5], describes the issue of picture recovery from an encoded database, where information classification is saved both in the capacity and recovery process. The paper centers around picture include insurance systems which empower comparability correlation among ensured highlights. By using both flag preparing and cryptographic methods, three plans are researched and thought about, including bit-plane randomization, irregular projection, and randomized unary encoding. Exploratory outcomes demonstrate that protected picture recovery can accomplish tantamount recovery execution to customary picture recovery strategies without uncovering data about picture content. This work advances the region of secure data recovery and can discover applications in secure online administrations for pictures and recordings.

Naehrig, *et al.* [4], presents data recovery assignments while saving information privacy is an attractive capacity when a database is put away on a server kept up by an outsider specialist co-op. This paper tends to the issue of empowering content-based recovery over encoded sight and sound databases. Pursuit lists, alongside sight and sound records, are first scrambled by the substance proprietor and after that put away onto the server. Through mutually applying cryptographic systems, for example,

request safeguarding encryption and randomized hash capacities, with picture handling and data recovery strategies, secure ordering plans are intended to give both security insurance and rank-requested inquiry ability. Recovery results on a scrambled shading picture database and security investigation of the safe ordering plans under various assault models demonstrate that information secrecy can be safeguarded while holding exceptionally great recovery execution. This work has promising applications in secure sight and sound administration.

Qia Wang, Wenjun Zeng presents protection is a basic issue when the information proprietors redistribute information stockpiling or handling to an outsider figuring administration, for example, the cloud. In this paper, we distinguish a distributed computing application situation that requires all the while performing secure watermark discovery and protection safeguarding interactive media information stockpiling. We at that point propose a compressive detecting (CS)-based structure utilizing secure multiparty calculation (MPC) conventions to address such a prerequisite. In our system, the mixed media information and mystery watermark design are introduced to the cloud for secure watermark recognition in a CS space to ensure the protection. Recent incidents have provided clear evidence that privacy should not be expected to be preserved by cloud providers.

WORKING PROCESS OF OUR PROPOSED METHOD

User module: In this module, users are the client. Client can create account in the cloud and can create a repository for individual.

User can store their image on their respective repository and can store their image with privacy using encryption scheme and they can search the image through key with respective query. Where they can both add their own images and/or search using a query image. Users can also request

Amid CS change, the security of the CS framework and the watermark design is ensured by the MPC conventions under the semi-genuine security display. We infer the normal watermark recognition execution in the CS area, given the objective picture, watermark design, and the measure of the CS lattice (yet without the CS grid itself). The accuracy of the inferred execution has been approved by our trials. Our hypothetical examination and test results demonstrate that safe watermark recognition in the CS area is plausible. Our system can likewise be stretched out to other community oriented secure flag preparing and information mining applications in the cloud.

PROPOSED SYSTEM

In this section, the implementation of our proposed system is explained briefly. Images are stored in our system in secure way through encryption and to ensure originality of user water marking has been implemented. In addition to provide more security in our system repository encryption has been implemented.

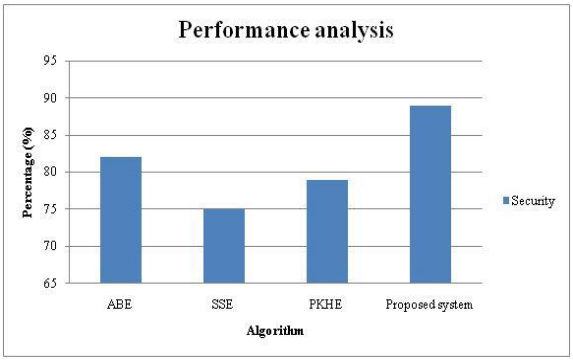
Need for securing data: Securing data in cloud is a difficult process because the cloud is honest but curious server. Encrypting and outsourcing data in cloud ensures data security in cloud, but leakage of key leads to disclosure of data.

access to stored images from their creators/owners.

RESULT AND DISCUSSION

However existing methods provide better security to store and retrieve our data from cloud. As we discussed before the key logic of extracting user data can be done if respective key has been identified by any attackers. Hence to overcome this issue we propose double step verification such as encrypting image as well as encrypting repository. If an authorized user wants

a particular image he or she should have respective repository key. If key is not available



then, water marked image will be delivered to user. Hence our system level of security is shown in graph below.

CONCLUSION

In this paper, the main objective of securing data in cloud has been implemented. However existing methods secures data in efficient way by utilizing various cryptography approaches, the key point of drawback is if the encryption key is identified by attacker or misbehaving persons then user own data will be revealed to an unauthorized person. Therefore an efficient approach should be needed to ensure secure data storing and retrieving process. Hence our proposed system achieves better security in terms of double step verification. In addition the originality of data also ensured through watermarking approach. Hence these shows without owner's information unauthorized user could not access original data of other users.

REFERENCES

[1] Lu, W., Varna, A. L., Swaminathan, A. and Wu, M. (2009). "Secure image retrieval through feature protection," IEEE International Conference on Acoustics, Speech and Signal Processing, Taipei. 1533-1536

[2] Hsu, C., Lu, C. and Pei, S. (2012). "Image Feature Extraction in Encrypted Domain With Privacy-Preserving SIFT". IEEE Transactions on Image Processing, 21: 4593 – 4607.

[3] C.-Y. Hsu, et al. (2001) Homomorphic encryption-based secure SIFT for privacy-preserving feature extraction. In Proc. Of SPIE,

[4] Naehrig, M., Lauter, K. and Vaikuntanathan, V. (2011). Can homomorphic encryption be practical? In Proceedings of the 3rd ACM workshop on Cloud computing security workshop (CCSW '11). Association for Computing Machinery, New York, NY, USA. 113–124.,

[5] Lu, W., Swaminathan, A., Varna, A. L. and Wu, M. (2009). "Enabling search over encrypted multimedia databases," Proc. SPIE 7254, Media Forensics and Security, 725418.

MCAS Journal of Research

mcas publications @ Muthayammal college of arts & science

AUTHOR GUIDELINES GENERAL

Submitted manuscripts for publication must be original. Only unpublished manuscripts, anywhere, in any form, should be sent for publication. High quality original figure(s) and photograph(s) must be submitted along with the manuscript. However, corresponding author has been encouraged to keep a copy of the manuscript for checking against the proofs. Authors should ensure that their English is polished before submission to avoid delay in publication and proof reading.

- Use active voice whenever feasible and write in first person.
- Use British spellings and grammar.
- Research articles/reports are in written in style not apt for publication in our journal. Chapters from these articles/reports may need to be condensed, reformatted and revised before submitting as manuscripts.

MANUSCRIPT PREPARATION

The manuscript should be typed, double-spaced on standard-sized-paper (8.5" x 11") with 1" margins on all sides. Times New Roman font 12 pt should be used. The fonts used in the text as well as graphics should be restricted to Times New Roman, Symbol and Zapf Dingbats.

Title page

Provide full title of the article, including the subtitle if one has. Capitalize only the first word of the title, and the first word of any subtitle; also capitalize any proper names in the title. The title page should contain a clear, concise and informative title of the article followed by the names and affiliations of the authors. The affiliation should indicate the department, institution, city, and state (or nation) and should be typed as a footnote to the author's name. The Corresponding Author must mention his or her complete mailing address, contact phone number, fax number, and email address at the lower left of the Title Page.

Article Structure Abstract

The abstract should not be more than 200 words. Abstract should not be structured. Abstract ought to be followed by four to six keywords.

Introduction

Introduction should be brief and must indicate the aim of the study and the essential back ground information. Introduction should pinpoint the hypothesis or the purpose of statement, how and why the purpose or hypothesis was developed and why the author deems it important.

Material and methods

Kindly provide concise but detailed information about the material and the analytical, statistical and experimental details. This part should be as clear as possible to enable other scientists to repeat the research presented. The use of subheadings to divide the text must be encouraged. Primary headings should be in bold capital letters. Secondary or subheadings should be in bold sentence case. In case of animal/human experiments or clinical trials, authors must give the details of ethical approval.

Result and Discussion

Data acquired from the research with appropriate statistical analysis described in the methods section should be included in this section. In this part, the same data/ information given in a table must not be repeated in a figure, or vice versa. Moreover, Tables and Figures should be self explanatory and it is not good enough to repeat extensively the numerals from tables into text and provide lengthy and unnecessary explanations of the Tables and Figures. Discussion should be related to the results to current understanding of the scientific problems being investigated in the field.

Conclusion

Being the last part, it must focus on the main ideas of the work highlighting its significance and relevance.

REFERENCES

References should be in arranged alphabetically by author's name followed by initial(s), year, title, journal, volume, number of the volume if any and the pages of the paper.

References should be cited in the text by authors name and years, i.e. Harris (1989) and Patel et al. (2004) etc. For references in the text, give full surnames for papers by one or two authors, but only the surname of the first author, followed by 'et al'. The 'et al.' should be italicized. List multiple citations in chronological order (e.g Harris, 1990; Patel 1999; Edwards *et al*., 2000), using a semicolon to separate each reference.

Research Papers:

Agar, A.A. (1996). Title of the article. Title of the Journal, Volume number, first page-last page Eg**.**

Agar ,N. (2000). Embryonic potential and stem cells. Bioethics 21: 198-204.

Agar, A.A., & Haris.P.D.(1996).Title of the article. Title of the Journal, Volume number, first page-last page

Agar, A.A., Haris.P.D., Agar, A.A., & David.R.A.(1996).Title of the article. Title of the Journal, Volume number, first page-last page

For Book Reference: Harborne, J.B. (1973). Phytochemical Methods, Chapman and Hall, Ltd., London, 49-188.

Proceedings of conferences: Anonymous. (1997). Antibacterial activity of *Catharanthus roseus* lin. G. Don on *Staphyloccocus aureus*, 25th Chapter, first page-last page

For Thesis Reference: Sivakumar. S.K.(2010).Title of the thesis. Ph.D., Thesis.Periyar University,Salem,Tamilnadu,India.

For Online Periodicals:

Smila,K.H. (2012). Guidelines for writing the living Web. *A List Apart: For People Who Make Websites, 149*. Retrieved from http://www.alistapart.com/articles/writeliving

For Online Periodicals assigned with Digital Object Identifier (DOI) Reference: Author, A. A., & Author, B. B. (Date of publication). Title of article. *Title of Journal, volume number*, page range. doi:0000000/000000000000 or ttp://dx.doi.org/20.0000/0000

Mcas Journal of Research

MUTHAYAMMAL COLLEGE OF ARTS & SCIENCE
Learn. Lead
A UNIT OF VANETRA GROUP

Affiliated to Periyar University, Salem
Accredited by NAAC with 'A' Grade
Recognized by UGC under Section 2(f) & 12 (B)
Recognized for STAR College Scheme - DBT

Celebrating 25 Years
1994 - 2019

Rasipuram - 637 408, Namakkal District, Tamilnadu. INDIA
Tel: +91-4287-222137 Fax: +91-4287-220227
E-Mail : info@muthayammal.in
www.muthayammal.in

GSSN 2454-115X