INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.,
Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)],
Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.
Circulated all over the world & Google has verified that scholars of more than 4255 Cities in 176 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

Sr. No.	TITLE & NAME OF THE AUTHOR (S)	Page No.
1.	IMPACT OF WORKING CAPITAL MANAGEMENT ON THE PROFITABILITY OF LISTED CEMENT COMPANIES IN TANZANIA *DR. SRINIVAS MADISHETTI & DR. NSUBILI ISAGA*	1
2.	A STUDY ON COST OF REJECTION (REJECTED SAMPLES) IN A NABL ACCREDITED LABORATORY AT A POST GRADUATE TEACHING HOSPITAL IN DEHRADUN, UTTARAKHAND *PIYALI MITRA M., RIMMA MANDAL, M. M. MATHAVAN & DR. VIBHA GUPTA*	9
3.	BORDER GUARDS SYSTEMS USING HYBRID WIRELESS SENSOR NETWORKS *T. DEEPIGA, A. SIVASANKARI & S. A. SHOBA*	15
4.	INDEPENDENT ACCESS TO ENCRYPTED CLOUD DATABASES *ROHINI GAIKWAD, VAISHALI GHATE & JALPA MEHTA*	20
5.	SECURE IMAGE TRANSMISSION USING LOSSLESS ARITHMETIC CODING *AASHA M. VANVE, ABIRAMI SIVAPRASAD & SWATI DESHPANDE*	23
6.	SPAM ZOMBIE DETECTION SYSTEM *RUTUJA BANKAR, JYOTI DESHMUKH & SWATI DESHPANDE*	28
7.	SECURE AND SCALABLE DATA SHARING IN CLOUD STORAGE WITH KEY-AGGREGATE CRYPTOSYSTEM *B. RAJESH, D. L. SRINIVAS & A.EMMANUEL RAJU*	32
8.	IDENTIFYING LISTENING SKILLS AMONG BOYS AND GIRLS OF ARTS AND SCIENCE COLLEGE STUDENTS *K.ELAMATHI*	36
9.	A STUDY ON FINANCIAL HEALTH OF SELECTED SOFTWARE COMPANIES IN INDIA *R. DEVIPRASANNA*	39
10.	BORDER PATROL SYSTEMS-USING ADVANCED WIRELESS SENSOR NETWORKING DEVICES *T. DEEPIGA & A. SIVASANKARI*	43
11.	THE NEW SOCIAL CONTRACT FOR GREEN BUSINESS *RAJEEV GUPTA*	46
12.	DATA SECURITY AND PRIVACY PROTECTION IN CLOUD COMPUTING *ROHINI GAIKWAD & JALPA MEHTA*	50
13.	SURVEY OF VARIOUS CRYPTOGRAPHIC TECHNIQUES *AASHA M. VANVE & ABIRAMI SIVAPRASAD*	56
14.	CYBER SECURITY TRENDS, ISSUES AND ANALYSIS OF TOOLS *RUTUJA BANKAR & LUKESH KADU*	63
15.	DETERMINANTS OF THE CUSTOMER LOYALTY IN ETHIOPIAN BANKING INDUSTRY (WITH REFERENCE TO PRIVATE COMMERCIAL BANK) *TEKABE SINTAYEHU & MOHAMMAD SULTAN*	74
16.	KNOWLEDGE DISCOVERY IN DATABASES *ANANT KUMAR*	81
17.	GREEN MARKETING: PATH TO SUSTAINABLE DEVELOPMENT *VANDANA BALA*	86
18.	IMPLICATION OF REGULATION ON THE DEVELOPMENT OF MICROFINANCE IN THE NIGERIAN ECONOMY *GODSPOWER GODWIN ITEMEH*	90
19.	AN ASSESSMENT OF TAX EVASION LEVEL AMONG NIGERIAN TAXPAYERS *ZAKARIYA'U GURAMA*	94
20.	AUTOMATIC PROFILE CHANGING USING ANDROID PHONES AS PER GPS LOCATION *R. SARVANI & R. KUMARI*	98
	REQUEST FOR FEEDBACK & DISCLAIMER	105

CHIEF PATRON

FOUNDER PATRON

FORMER CO-ORDINATOR

ADVISORS

EDITOR

EDITORIAL ADVISORY BOARD

ASSOCIATE EDITORS

FORMER TECHNICAL ADVISOR

FINANCIAL ADVISORS

LEGAL ADVISORS

SUPERINTENDENT

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____________

THE EDITOR

IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF _______________________.**

(e.g. Finance/Mkt./HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '____' for possible publication in one of your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the co-authors of this manuscript have seen the submitted version of the manuscript and have agreed to their inclusion of names as co-authors.

Also, if my/our manuscript is accepted, I agree to comply with the formalities as given on the website of the journal. The Journal has discretion to publish our contribution in any of its journals.

NAME OF CORRESPONDING AUTHOR :

Designation :

Institution/College/University with full address & Pin Code :

Residential address with Pin Code :

Mobile Number (s) with country ISD code :

Is WhatsApp or Viber active on your above noted Mobile Number (Yes/No) :

Landline Number (s) with country ISD code :

E-mail Address :

Alternate E-mail Address :

Nationality :

NOTES:

a) The whole manuscript has to be in ***ONE MS WORD FILE*** only, which will start from the covering letter, inside the manuscript. ***pdf. version is liable to be rejected without any consideration***.

b) The sender is required to mention the following in the **SUBJECT COLUMN of the mail**:

New Manuscript for Review in the area of (e.g. Finance/Marketing/HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any **specific message** w.r.t. to the manuscript.

d) The total size of the file containing the manuscript is expected to be below **1000 KB**.

e) **Abstract alone will not be considered for review** and the author is required to submit the **complete manuscript** in the first instance.

f) ***The journal gives acknowledgement w.r.t. the receipt of every email within twenty four hours*** and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending a separate mail to the journal.

g) The author (s) name or details should not appear anywhere on the body of the manuscript, except the covering letter and the cover page of the manuscript, in the manner as mentioned in the guidelines.

2. **MANUSCRIPT TITLE:** The title of the paper should be **bold typed**, **centered** and **fully capitalised**.
3. **AUTHOR NAME (S) & AFFILIATIONS:** Author (s) **name**, **designation**, **affiliation** (s), **address**, **mobile/landline number** (s), and **email/alternate email address** should be given underneath the title.
4. **ACKNOWLEDGMENTS:** Acknowledgements can be given to reviewers, guides, funding institutions, etc., if any.
5. **ABSTRACT:** Abstract should be in **fully italicized text**, ranging between **150** to **300 words**. The abstract must be informative and explain the background, aims, methods, results & conclusion in a **SINGLE PARA**. ***Abbreviations must be mentioned in full***.
6. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of **five**. These should be arranged in alphabetic order separated by commas and full stop at the end. All words of the keywords, including the first one should be in small letters, except special words e.g. name of the Countries, abbreviations.
7. **JEL CODE:** Provide the appropriate Journal of Economic Literature Classification System code (s). JEL codes are available at www.aeaweb.org/econlit/jelCodes.php, however, mentioning JEL Code is not mandatory.
8. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. *It should be free from any errors i.e.* ***grammatical, spelling*** *or* ***punctuation.*** *It must be thoroughly edited at your end*.
9. **HEADINGS:** All the headings must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.
10. **SUB-HEADINGS:** All the sub-headings must be bold-faced, aligned left and fully capitalised.
11. **MAIN TEXT:**

THE MAIN TEXT SHOULD FOLLOW THE FOLLOWING SEQUENCE:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESIS (ES)

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

LIMITATIONS

SCOPE FOR FURTHER RESEARCH

REFERENCES

APPENDIX/ANNEXURE

The manuscript should preferably range from ***2000 to 5000 WORDS***.

12. **FIGURES & TABLES**: These should be simple, crystal **CLEAR**, **centered**, **separately numbered** & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. *It should be ensured that the tables/figures are referred to from the main text*.

13. **EQUATIONS/FORMULAE**: These should be consecutively numbered in parenthesis, horizontally centered with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word should be utilised. If any other equation editor is utilised, author must confirm that these equations may be viewed and edited in versions of Microsoft Office that does not have the editor.

14. **ACRONYMS**: These should not be used in the abstract. The use of acronyms is elsewhere is acceptable. Acronyms should be defined on its first use in each section: Reserve Bank of India (RBI). Acronyms should be redefined on first use in subsequent sections.

15. **REFERENCES**: The list of all references should be alphabetically arranged. ***The author (s) should mention only the actually utilised references in the preparation of manuscript*** and they are supposed to follow Harvard Style of Referencing. **Also check to make sure that everything that you are including in the reference section is duly cited in the paper**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parenthesis.
- ***Headers, footers, endnotes*** *and* ***footnotes*** *should* ***not be used*** *in the document****.*** However, **you can mention short notes to elucidate some specific point**, which may be placed in number orders after the references.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–23

UNPUBLISHED DISSERTATIONS

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

INDEPENDENT ACCESS TO ENCRYPTED CLOUD DATABASES

ROHINI GAIKWAD
STUDENT
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
CHEMBUR

VAISHALI GHATE
ASST. PROFESSOR
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
CHEMBUR

JALPA MEHTA
ASST. PROFESSOR
SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE
CHEMBUR

ABSTRACT

Placing critical data in the hands of a cloud provider should come with the guarantee of security and availability for data at rest, in motion, and in use. Several alternatives exist for storage services, while data confidentiality solutions for the database as a service paradigm are still immature. We propose a novel architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data. This is the first solution supporting geographically distributed clients to connect directly to an encrypted cloud database, and to execute concurrent and independent operations including those modifying the database structure. The proposed architecture has the further advantage of eliminating intermediate proxies that limit the elasticity, availability, and scalability properties that are intrinsic in cloud-based solutions.

KEYWORDS

Cloud, security, SecureDBaaS, database.

I. INTRODUCTION

In a cloud context, where critical information is placed in infrastructures of untrusted third parties, ensuring data confidentiality is of paramount importance. This requirement imposes clear data management choices: original plain data must be accessible only by trusted parties that do not include cloud providers, intermediaries, and Internet; in any untrusted context, data must be encrypted. Satisfying these goals has different levels of complexity depending on the type of cloud service. There are several solutions ensuring confidentiality for the storage as a service paradigm, while guaranteeing confidentiality in the database as a service (DBaaS) paradigm is still an open research area. In this context, we propose SecureDBaaS as the first solution that allows cloud tenants to take full advantage of DBaaS qualities, such as availability, reliability, and elastic scalability, without exposing unencrypted data to the cloud provider.

The architecture design was motivated by a threefold goal: to allow multiple, independent, and geographically distributed clients to execute concurrent operations on encrypted data, including SQL statements that modify the database structure; to preserve data confidentiality and consistency at the client and cloud level; to eliminate any intermediate server between the cloud client and the cloud provider. The possibility of combining availability, elasticity, and scalability of a typical cloud DBaaS with data confidentiality is demonstrated through a prototype of SecureDBaaS that supports the execution of concurrent and independent operations to the remote encrypted database from many geographically distributed clients as in any unencrypted DBaaS setup. To achieve these goals, SecureDBaaS integrates existing cryptographic schemes, isolation mechanisms, and novel strategies for management of encrypted metadata on the untrusted cloud database.

The SecureDBaaS architecture is tailored to cloud platforms and does not introduce any intermediary proxy or broker server between the client and the cloud provider. Eliminating any trusted intermediate server allows SecureDBaaS to achieve the same availability, reliability, and elasticity levels of a cloud DBaaS. Other proposals based on intermediate server(s) were considered impracticable for a cloud-based solution because any proxy represents a single point of failure and a system bottleneck that limits the main benefits (e.g., scalability, availability, and elasticity) of a database service deployed on a cloud platform. Unlike SecureDBaaS, architectures relying on a trusted intermediate proxy do not support the most typical cloud scenario where geographically dispersed clients can concurrently issue read/write operations and data structure modifications to a cloud database.

II. RELATED WORK

Cloud computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about over provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under provisioning for one that becomes wildly popular, thus missing potential customers and revenue. Moreover, companies with large batch-oriented tasks can get results as quickly as their programs can scale, since using 1,000 servers for one hour costs no more than using one server for 1,000 hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT.

Cloud computing can and does mean different things to different people. The common characteristics most interpretations share are on-demand scalability of highly available and reliable pooled computing resources, secure access to metered services from nearly anywhere, and displacement of data and services from inside to outside the organization. While aspects of these characteristics have been realized to a certain extent, cloud computing remains a work in progress. This publication provides an overview of the security and privacy challenges pertinent to public cloud computing and points out considerations organizations should take when outsourcing data, applications, and infrastructure to a public cloud environment.

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud is used as a metaphor for the Internet, so the phrase-- are delivered to an organization's computers cloud computing means "a type of Internet-based computing," where different services such as servers, storage and applications and devices through the Internet. Presently implementation of cloud computing has increased rapidly in IT industry and in other organization also. Cloud is a collection of distributed database. It provides number of benefit such that low cost and accessibility of data. If a data is store only at single place and unfortunately that data has been lost then there is no recovery of data. Cloud computing gives us a solution to store a number of copy of data, in this manner if a data is going to be loss at one place that can be retrieved from other place. The problem of service unavailability has been solved by using cloud computing, which was a major concern in single cloud. In recently days use of multi cloud becoming popular because its provide the major benefit of service availability. As much of benefit coming with multi- cloud computing, that much security issues also coming with it. A cloud user is storing their information in clouds, those cloud provider can be untrusted, the information stored by user can be sensitive and in cloud there may be a chances of availability of malicious and anomaly which can harm user sensitive data. So security of data in multi-cloud computing is a major concern. In this paper we are going to discuss about functionality of single and multicloud computing and security threats. In several researches on fact is coming out that the work done for maintainability of multi cloud security concern is less than the cost and work dome for single cloud. This research promotes the use of multiclouds due to ability of reducing security threats that affect the sensitive data of user. In this paper we will give a solution for security concern of data in multiclouds. Here we will show that in respect of storing user actual data, we are going to store encrypted data in cloud for which we will use plain cipher encryption algorithm of cryptography.

In cloud computing, information homeowners host their information on cloud servers and users (data consumers) will access the information from cloud servers. As a result of the information outsourcing, however, this new paradigm of knowledge hosting service additionally introduces new security challenges, which requires associate freelance auditing service to ascertain the information integrity within the cloud. Some existing remote integrity checking strategies can solely serve for static archive information and, thus, can't be applied to the auditing service since the information within the cloud are often dynamically updated. Thus, economical and secure dynamic auditing protocol is desired to convert information homeowners that the information area unit properly holds on in the cloud. Economical and privacy-preserving auditing protocol was proposed to provide data integrity. Then, this scheme extends the auditing protocol to support the information dynamic operations, that is economical and incontrovertibly secure in the random oracle model. Also auditing protocol supports batch auditing for each multiple homeowners and multiple clouds, without exploitation any sure organizer. The analysis and simulation results show that projected auditing protocols area unit secure and efficient, particularly it scale back the computation value of the auditor.

III. PROBLEM DEFINITION

Proposed System lies on protecting sensitive data outsourced to third parties is to store encrypted data on server.

To achieve this goal there are different levels of complexity depending on the type of cloud service.

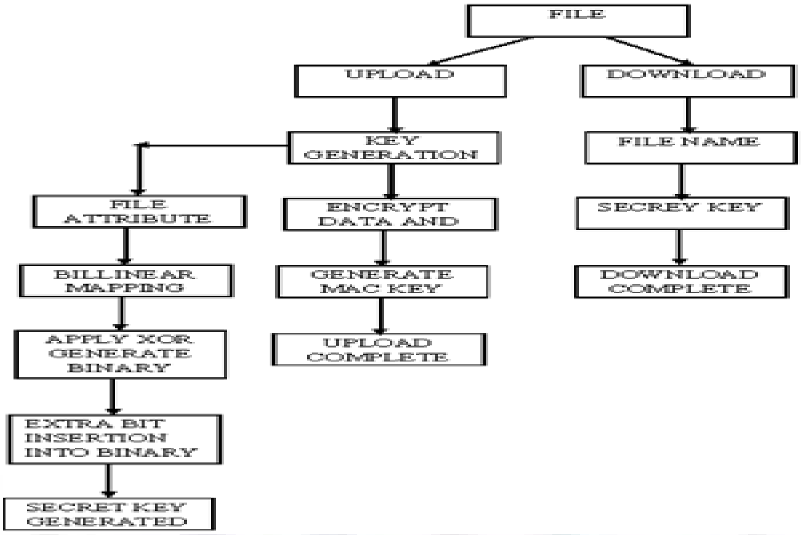
As we cannot apply fully homomorphic encryption schemes because of their excessive computational complexity. This existing approach is not applicable to the DBaaS context considered by SecureDBaas.

The proposed system is a novel architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data. It will include following module.

1. Client Register & login
2. Key Generation, Encrypt File and Metadata then Upload File
3. Metadata Management in cloud
4. Download File & Decrypt

IV. PROPOSED SYSTEM

FIGURE 1: THE PROPOSED SYSTEM



A. **CLIENT REGISTER & LOGIN**

- In this module, Client wants to login. So First he registered to cloud with his own details, such as username, password, mobile no and address.
- Then he login with his username and password. Then he got his client form. This client form contains two contents. One is upload another one is download.

B. **KEY GENERATION, ENCRYPT FILE AND METADATA THEN UPLOAD FILE**

- A secure type is composed of three fields: data type, encryption type, and field confidentiality. The combination of the encryption type and of the field confidentiality parameters defines the encryption policy of the associated column.
- The data type represents the type of the plaintext data (e.g., int, varchar). The encryption type identifies the encryption algorithm that is used to cipher all the data of a column. It is chosen among the algorithms supported by the SecureDBaaS implementation.
- SecureDBaaS offers three field confidentiality attributes: Column (COL) is the default confidentiality level that should be used when SQL statements operate on one column; the values of this column are encrypted through a randomly generated encryption key that is not used by any other column.
- Multicolumn (MCOL) should be used for columns referenced by join operators, foreign keys, and other operations involving two columns; the two columns are encrypted through the same key.
- Database (DBC) is recommended when operations involve multiple columns; in this instance, it is convenient to use the special encryption key that is generated and implicitly shared among all the columns of the database characterized by the same secure type.
- Then generate the Key for encryption, next encrypt the file with its metadata and upload to the cloud.

C. **METADATA MANAGEMENT**

- Metadata generated by SecureDBaaS contain all the information that is necessary to manage SQL statements over the encrypted database in a way transparent to the user.
- Metadata management strategies represent an original idea because SecureDBaaS is the first architecture storing all metadata in the untrusted cloud database together with the encrypted tenant data.

- SecureDBaaS uses two types of metadata. Database metadata are related to the whole database. There is only one instance of this metadata type for each database.
- Table metadata are associated with one secure table. Each table metadata contains all information that is necessary to encrypt and decrypt data of the associated secure table.

D. **DOWNLOAD FILE & DECRYPT**

- In this module the client wants to download file. So he entered the filename.
- Then he give the download request to SecureDBaaS Cloud.
- Finally he gets the Ciphertext then he decrypt and get the original file.

V. ALGORITHM FOR PROPOSED SYSTEM

A. ATTRIBUTE BASED ALGORITHM (ABE)

The concept of attribute-based encryption (ABE) can be considered as a generalization of identity based encryption (IBE) (Identity based encryption), where, as mentioned earlier, the encryption is based on some identity. Thus, ABE is more expressive than IBE. In an ABE system, the plaintext is encrypted with a set of attributes. The KGS (Key Generation Server), which possesses the master key, issues different private keys to users after authenticating the attributes they possess. Thus, these private keys are associated with the set of attributes each user possesses. In its basic form, a user can decrypt a cipher text if and only if there is a match between the attributes of the ciphertext and the user's key. For example, Alice has the attributes "role = doc" and "age > 18". Now Bob encrypts a message using the attributes ("role = student" AND "age > 18"). Alice can decrypt the message as she satisfies both attributes. Bob encrypts another message using the attributes ("role = professor" OR "role = staff"). Alice cannot decrypt the message as she does not satisfy the policy. (The workings of the actual ABE schemes are a little different from the above examples, but they give the essential idea behind the schemes.) The initial ABE system is limited only to threshold policies where there should be at least k out of n attributes common between the attributes used to encrypt the plaintext and the attributes users possess. For example, Bob encrypts a message for any 3 attributes out of the 5 attributes {a1, a2, a3, a4, a5}. Alice has the attributes {a1, a2, a4, a5} and Eve has {a1, a2}. While Alice can decrypt Bob's message, Eve cannot as she does not satisfy the threshold policy. Out of them there are important variants that is Key Policy ABE (KP-ABE)

B. BILINEAR MAPPING

- Attribute based encryption is proceeded by bilinear mapping of attribute information of data owner and the data to be stored in the cloud.
- Bilinear mapping process achieved by multiplicative factors of both Logical AND, XOR operations.
- It is the process of pairing up the attribute information and thus cipher text policy ABE is processed.

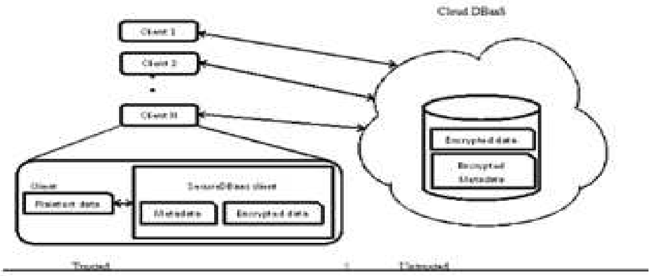
C. MASTER AND SECERET KEY GENERATION

- Master key is generated by doing the Logical AND operations of given attributes of data owner.
- Using the master key, public key is generated and secret key is generated by doing the logical XOR operations.
- Ciphering algorithms are applied using the secret key, thus secured secret key is generated by Attribute based encryption.

VI. IMPLEMENTATION PLAN

SecureDBaaS is designed to allow multiple and independent clients to connect directly to the untrusted cloud DBaaS without any intermediate server. Figure 2 describes the overall architecture. We assume that a tenant organization acquires a cloud database service from an untrusted DBaaS provider. The tenant then deploys one or more machines (Client 1 through N) and installs a SecureDBaaS client on each of them. This client allows a user to connect to the cloud DBaaS to administer it, to read and write data, and even to create and modify the database tables after creation.

FIGURE 2: SECUREDBAAS ARCHITECTURE



The information managed by SecureDBaaS includes plaintext data, encrypted data, metadata, and encrypted metadata. Plaintext data consist of information that a tenant wants to store and process remotely in the cloud DBaaS. To prevent an untrusted cloud provider from violating confidentiality of tenant data stored in plain form, SecureDBaaS adopts multiple cryptographic techniques to transform plaintext data into encrypted tenant data and encrypted tenant data structures because even the names of the tables and of their columns must be encrypted. SecureDBaaS clients produce also a set of metadata consisting of information required to encrypt and decrypt data as well as other administration information. Even metadata are encrypted and stored in the cloud DBaaS.

VII. SUMMARY

We propose an innovative architecture that guarantees confidentiality of data stored in public cloud databases. Unlike state-of-the-art approaches, our solution does not rely on an intermediate proxy that we consider a single point of failure and a bottleneck limiting availability and scalability of typical cloud database services. A large part of the research includes solutions to support concurrent SQL operations (including statements modifying the database structure) on encrypted data issued by heterogeneous and possibly geographically dispersed clients.

REFERENCES

1. M. Armbrust et al (2010)., "A View of Cloud Computing," Comm. of the ACM.
2. P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish (2011), "Depot: Cloud Storage with Minimal Trust," ACM Trans. Computer Systems.
3. W. Jansen and T. Grance (2011), "Guidelines on Security and Privacy in Public Cloud Computing," Technical Report Special Publication, NIST.
4. H. Hacigu¨mu¨ s¸, B. Iyer, and S. Mehrotra (Feb. 2002), "Providing Database as a Service," Proc. 18th IEEE Int'l Conf. Data Eng.
5. J. Li, M. Krohn, D. Mazie`res, and D. Shasha (Oct. 2004), "Secure Untrusted Data Repository (SUNDR)," Proc. Sixth USENIX Conf. Opearting Systems Design and Implementation.
6. Luca Ferretti, Michele Colajanni, and Mirco Marchetti (FEBRUARY 2014), "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS.
7. A.J. Feldman, W.P. Zeller, M.J. Freedman, and E.W. Felten (Oct. 2010), "SPORC: Group Collaboration Using Untrusted Cloud Resources," Proc. Ninth USENIX Conf. Operating Systems Design and Implementation.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you tosupply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail**infoijrcm@gmail.com** for further improvements in the interest of research.

If youhave any queries please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

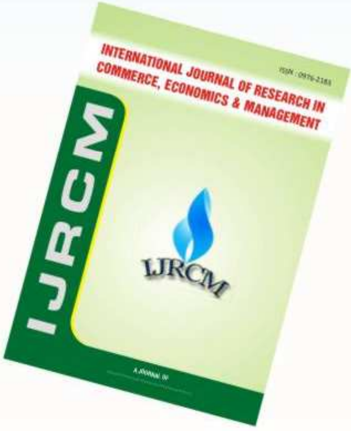
DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, neither its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal are exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals


ISSN : 0976-2183
INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, ECONOMICS & MANAGEMENT
IJRCM
IJRCM
A JOURNAL OF

ISSN : 0976-2183
INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT
IJRCM
IJRCM
A JOURNAL OF