Abstract: Data warehouse and its safekeeping is mainly challenging and decisive issue in contemporary technical turf. Numerous papers have been compiled and theories formulated for diverse category of data warehouse architecture and ensuring its safekeeping. Developers are trying to augment the intricacy of the cryptographic modus operandi to boost the safekeeping of the data warehouse. At this juncture, where countless modus operandi has arrived, it is requisite to unearth the distinction and benefit of one process over the other.

For the very intention, a comprehensive study is prerequisite. The proposed work is a comprehensive study and comparative analysis on the diverse cryptographic modus operandi in offer. The assortment of cryptographic modus operandi in discussion is already well established. Additionally, study on diverse realization avenue has been ensured. Based on the same, a comprehensive and comparative study is ensured and offered in tabular form for simplicity of understanding and endowing with exclusive opinion. The comparative analysis is based on distinct parameters, which has been well exhibited in the respective table. The paper could serve as a reference paper while compiling fresh and novel cryptographic modus operandi. The proposed work could save the stretched haul of exploring and studying diverse papers from an assortment of sources.

KEYWORDS: Data Warehouse, Cryptography, Encryption, Decryption, Dual Key, MMC, LFC, SSTC

1. INTRODUCTION

Data warehouse, also recognized as an enterprise data warehouse is a system used for adept coverage and facts examination. Data warehouse are fundamental repository of incorporated data from one or more incongruent sources. It amasses existing and historical data and employs the same for engendering analytical reports for apiece adept acquaintance all through the enterprise. Consequently, the contemporary business houses have stern rivalry amid business models and the capacity to seize, amass and efficiently employ the communal facts of the organization. Triumph of contemporary industries would rely on an effectual data supervision approach of data warehousing and adept data analysis competence that culminates with data mining. Data warehousing systems have surfaced as one of the foremost technological approaches to the expansion of newer and highly lucrative corporate association.

Data warehouse architecture is exemplified for simplicity in understanding:

Cryptography is the study of information concealing. It is frequently called code, but this is not an accurate name in actuality. The focal point is to ensure that the information is undisclosed and safe. Cryptography is employed in diversified fields of work and finds a considerable acumen, viz; ATM cards, computer passwords, internet shopping, whatsapp messages, medical establishments, military activities, educational avenues, etc. When a message is transferred employing cryptography, it is altered (or encrypted) prior to being sent. The scheme of altering text is called a "code" or, more specifically, a "cipher". The altered text is called "cipher text". The
alteration makes the message tough to be unearthed. Someone who yearns to read it must be equipped to alter it back (or decrypt). The paper is an amalgamation of Data warehouse and Cryptography. There are diverse categories of Data Warehouse architecture and Cryptographic modus operandi. With a piecemeal fleeting instant, newer modus operandi and ways of cryptography is being formulated and the motto is merely to craft encryption and decryption modus operandi protected so that the susceptibility to third party incursion turn out to be less. Consequently, formulating new cryptographic algorithms and data warehouse architectural models encompass an imperative fragment of the present technological world. Formulating something new and improved in a righteous manner, the formerly formulated methodologies are requisite for assessment and deliberated towards comprehensive study which subsequently leads to comprehensive study and comparative analysis of existing modus operandi.

2. LITERATURE REVIEW

The section emphasizes the interrelated attempt available in the identical category, expectant in the compilation of the proposed paper [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]. There are reasonably a small number of interrelated efforts on data warehouse and its safekeeping mechanism, which have been accepted and acknowledged prior, though the precise devise, insight and incorporation of the revolutionary algorithm is notable and extremely pleasant for contemporary researchers. The extensive study of few papers necessitates cautious disclose and the crispy tips are affirmed in finer points for simplicity in declaration [3, 4, 5, 8, 9, 12].

In the paper titled “Towards Data Security in Affordable Data Warehouse,” the data warehouse modus operandi is based on clustering and the star schema is fragmented over the nodes of the cluster. Dimension table is imitated in apiece node of the cluster and fact table is dispersed employing strict round robin or hash partitioning [12].

The paper titled “Design and Implementation of Security Mechanism for Data Warehouse Performance Enhancement Using Two Tier User Authentication Techniques” ensures the design and realization of safekeeping for data warehouse output augmentation, with the integration of the well-knitted twin tier user authentication modus operandi. The data warehouse safekeeping comprises of couple of fragments, namely; safekeeping realization by user authentication at tier one and safekeeping realization by conveying an auto engendered code to users’ mobile phone at tier two [5].

In the paper titled “Towards Design, Analysis and Performance Enhancement of Data Warehouse by Implementation and Simulation of P2P Technology on Proposed Pseudo Mesh Architecture” a faction of dimension tables interconnected with one another, ascents that time complexity of the data warehouse is presented through the compilation of the proposed work is improved. Fact tables and dimension tables have been employed here, in their normalized form, to weaken duplication [4].

In the paper titled “Proposed Business Principles Governing Enterprise Data Warehouse Design: Conceptual Framework with Enhancement of Knowledge Infrastructure via Context Model” the design of context model is based on the seven new projected business principles and their alliance with the obtainable seven principles of Enterprise Data Warehouse design stated by Rich Cohen [8].

In the paper titled “Proposed Hybrid Data Warehouse Architecture Based on Data Model” a fifth variation of previously obtainable data model is classified. Hybrid Architecture, Hybrid Implementation of data warehouse is established. In the proposed model, both the architecture and the implementation is bidirectional by nature [9].

In the paper titled “Design and Implementation of Proposed Drawer Model Based Data Warehouse Architecture Incorporating DNA Translation Cryptographic Algorithm for Security Enhancement” the data warehouse model is based on the obtainable ETL model and the algorithm is based on genetic coding. The devised algorithm ascertains that there would be sizeable decline of admittance point in time, keeping in wits the apt reclamation of all essential data from the data vaults [3].

In the paper titled “Towards Design, Analysis and Performance Enhancement of Data Warehouse by Implementation and Simulation of P2P Technology on Proposed Pseudo Mesh Architecture” a faction of dimension tables interconnected with one another, ascents that time complexity of the data warehouse is presented through the compilation of the proposed work is improved. Fact tables and dimension tables have been employed here, in their normalized form, to weaken duplication [4].
3. PROPOSED WORK

The proposed work is basically oriented towards comprehensive study and comparative analysis for an assortment of distinguished cryptographic modus operandi and their realization amid distinct safekeeping of data warehouse. Not only the architecture but also the safekeeping is requisite for address. A number of cryptographic modus operandi has been developed till date, out of which some of the algorithms have been chosen for study and comparison. The comparison would unfasten novel mode for progress of newer modus operandi which in a way would be enhanced than the existing process.

Diverse cryptographic modus operandi has been elucidated for ease in understanding:

3.1. Matrix and Mutation Based Cryptosystem [MMC]: Out of numerous cryptographic modus operandi, the first one for comprehensive study is Matrix and Mutation Based Cryptosystem (MMC). In this paper, both encryption and decryption methodologies have been proposed. The algorithm is based on matrix transposition and shifting of rows and columns along with hexadecimal number system. In this algorithm, color code is used to obtain the cipher text. The algorithm is compared with T-DES and GFC algorithm based on text files (.txt), executable files (.exe) and Dynamic Link Libraries (.dll). The result shows that apiece time MMC takes less time for encryption and decryption than T-DES and takes less or equivalent time than GFC. Furthermore, the result also exhibits that the algorithm maintains homogeneity [16].

3.2. Dual Key and Matrix Based Iterative Encryption Technique [DKMBIET]: The second work addresses the issue of safekeeping in data transfer. To ensure additional safekeeping of data transfer, dual key is engendered in the said algorithm. Firstly, a key is created according to the number of characters in the key text, then employing the key, another key is engendered, which is employed in the encryption process. In this way, a 16 bit key is engendered. Dual key engendering makes the algorithm stronger on the basis of safekeeping [18].

3.3. Logarithmic Function Based Cryptosystem [LFC]: Logarithmic Function Based Cryptosystem (LFC) is proposed to minimize time complexity. In order to attain the same, symmetric key cryptographic modus operandi is employed in LFC. In LFC, identical key is employed at the time of encryption and decryption. In the formulated algorithm, security measures are also very strong as three generation of numbers is engendered. Employing the highest and lowest number from the three generations, the key of the cryptographic modus operandi is crafted. Employing Genetic functions like Crossover and Mutation during the formulation of the said algorithm, adds a feather in the cap. The algorithm is tested on text files and DLL files and the result shows that LFC is in vicinity in all respects with RSA and T-DES [15].

3.4. Stochastic Seed Based Cryptographic Technique [SSCT] Using Dual Formula Key [DFK]: Akin to the prior algorithm, the said algorithm is symmetric key cryptographic modus operandi too, employing which ascertains the algorithm to be faster. But in the said algorithm, unlike in symmetric key cryptography, the key is not sent alone to the receiver through any secure medium, which could be hacked with utmost ease by the hackers, if the medium is not protected enough. To curtail the type of risk, the key is not sent alone to the receiver, but it is merged with the cipher text and hence it becomes tricky for the hackers to hack the key, even if the transmission is less protected. In the algorithm, two keys are engendered and by merging the two keys, the final key is crafted. The exclusive attribute of the algorithm is that, for apiece character, a corresponding 256-bit binary number would be engendered, which augments the safekeeping stratum of the cipher text [17].

3.5. Design and Implementation of RNS Model Based Steganographic Technique for Secured Transmission: In the said paper, the modus operandi is based on steganography, where data is hidden within image. RNS model is proposed in the algorithm and RNS object is employed during the formation of the foreground image as well as the background image. In the algorithm, for mixing two images, alpha factor is employed. If the value of the alpha factor is 0.5, then the two images are mixed equally. If the value of alpha factor is less than 0.5, then the contribution of the background image is more than the foreground image. But the obtained image is a stego image which endows with the impression to the viewers about the availability of coordinates only, without any direction. For this reason, the security parameter of the proposed modus operandi is intensified [14].

3.6. Logarithmic Formula Generated Seed Based Cryptographic Technique [LFGSBCT] Using Proposed Alphanumeric Number System [ANS] and Rubik Rotation Algorithm [RRA]: In the proposed algorithm, massive quantity of data could be transferred amid two parties. It is an innovative approach of the said algorithm, where ANS table is employed. ANS table comprises of 94 popularly employed characters (Inclusive of numerals), lower case and upper case English alphabets and special characters, which could be imputed through the keyboard by the user. In the said paper, the cipher text is engendered in two distinguished stratum. Initially, a seed is engendered employing logarithmic formula and subsequently employing the seed, the pain text is converted to cipher text.

In the second level, Rubik Rotation algorithm is applied on the engendered cipher text. At an instant, 24 characters could take part in Rubik Rotation algorithm, as it employs 2^2*2 Rubik Cube. Then apiece 24 -character cipher text is merged and the seed is inserted into n/2th position, which is right padded with zero, thereby furnishing the final cipher text.
The engendered seed employed in the encryption is entirely based on random character engendering test. Throughout the algorithm, the seed remains concealed, which augments safekeeping of the algorithm. Rubik Rotation algorithm also augments the randomization of the cipher text and hence it is exceedingly complicated for the malicious intruder to crack the safekeeping and obtain the plain text [13].

4. RESULT ANALYSIS

The section deals with the comparative analysis based on the comprehensive study, namely:

<table>
<thead>
<tr>
<th>Data Warehouse papers</th>
<th>Architectural Model Employed</th>
<th>Parameters</th>
<th>Feasibility</th>
<th>Accessibility</th>
<th>Assessment Time</th>
<th>Response Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Towards Data Security in Affordable Data Warehouse</td>
<td>ETL Data Warehouse Model</td>
<td>3</td>
<td>2</td>
<td>Medium</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>Design and Implementaiton of Security Mechanism for Data Warehouse Performance Enhancements Using Two Tier Architectures</td>
<td>Two Tier Architectures</td>
<td>4</td>
<td>4</td>
<td>High</td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>

Note: The rating in Table–1 is exhibited amid the range of 1 to 5, wherein 1 is the lowest value endowed with and 5 is the highest value endowed with on a piece parameter.
After decisively analyzing, ratings have been formulated as high, medium and low. SSTC using DFK, LFGSBCT using ANS and RRA and RNS based Steganographic techniques find being placed above other techniques in the aforementioned table. Conclusively, the cryptographic modus operandi would be labeled as secured algorithms, which not only endow with safekeeping but also hassle free access to data.

5. CONCLUSION

Comprehensive study and comparative analysis ensured during the formulation of the paper would not only aid to realize the progress in the respective fields and existing modus operandi but also would aid to review parameters. The same should be kept in mind while emerging with novel cryptographic modus operandi or data warehouse architectural model for prospective future. The culmination of the paper furnishes a sneak peek into data warehouse safekeeping augmentation employing cryptographic modus operandi. The paper could act as a reference paper for contemporary researchers working either exclusively on papers pertaining to data warehouse and cryptographic modus operandi or cohesively with the amalgamation of data warehouse safekeeping employing cryptographic modus operandi. In any case, the paper could dish out lot of precious inputs for timely incorporation by the concerned researchers.

REFERENCES


<table>
<thead>
<tr>
<th>Dual Key and Matrix Based Iterative Encryption Technique [DKMBIET]</th>
<th>High</th>
<th>Medium</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logarithmic Function Based Cryptosystem [LFC]</td>
<td>Medium</td>
<td>Medium</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Stochastic Seed Based Cryptographic Technique [SSCT] Using Dual Formula Key [DFK]</td>
<td>High</td>
<td>High</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Design and Implementation of RNS Model Based Steganographic Technique for Secured Transmission</td>
<td>High</td>
<td>High</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Logarithmic Formula Generated Seed Based Cryptographic Technique [LFGSBCT] Using Proposed Alphanumeric Number System [ANS] and Rubik Rotation Algorithm [RRA]</td>
<td>High</td>
<td>High</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 2: Comparison of distinguished Cryptographic modus operandi pertaining to Incorporation of Safekeeping in Data Warehouse to Augment Performance

In the section, two distinct tables have been formulated based on some requisite parameters to analyze decisively about the data warehouse architecture and the allied cryptographic modus operandi adhered.

In Table–1, the studied papers in concern and their architectural models employed have been endowed with. Next, apiece paper is analyzed and studied employing four standard parameters, namely; feasibility, accessibility, assessment time and response time. As an inference from Table–1, it could be visualized that the Drawer Model based architecture has an imposing rating over the concerned parameters.

The Drawer Model based architecture is secured with DNA based algorithm. The data is obtainable effortlessly and precisely. Though, apiece model discussed in Table–1 have appreciable approaches in their way, having some merits and demerits too. The discussion has been based on a fixed number of parameters and it could be apt for any organization based on its need.

In Table–2, comparative analysis of distinguished cryptographic modus operandi has been ensured with some parameters, namely; confidentiality, authentication, distinct complexities and ease of encryption and decryption.
Volume 6, Issue 6, November - December 2017


AUTHORS

Prof. Rajdeep Chowdhury is Head of Department of Computer Application at JIS College of Engineering, Kalyani, West Bengal, India. He has Published more than 65 Research Papers in Peer Reviewed International/National Journals and Conferences (ACM, IEEE, Springer, SCOPUS,
Taylor & Francis, CRC Press, Thomson Reuters, Bloomsbury, Tata McGraw Hill), along with being Program Committee Member in more than 60 International Conferences in various parts of the World and Advisory Board Member in numerous International Conferences.

He is also in the Editorial Board of around 20 International Journals. He has 3 Published Patents.

His works have been published in more than 25 Anthologies all over the world.

He is the Editor of highly appreciated Books 'Creative Corner: Crafting Emotion,' 'Cologne of Heritage: Incredible Bengal,' & 'Spring: The Season of Love' Published by Vishwabharati Research Centre.

He has numerous Media Coverage by leading News Channels and Newspapers for Online Interview/Print Interview/Cover Story/Headline News.

He is invited for Keynote Address/Invited Lecture/Panel Discussion and Chairing Technical Session at diverse International Conferences/Symposiums all around the globe.

He has been recipient of numerous Accolades, Awards and Honor by Corporate bigwigs and Academia.

He is also the Award winning and Record setting Author of the Innovative and Unique Book 'POISINE: Bengali Cuisine with Poetry (Level-1: Starters).'

The Book is in Asia Pacific Records.

Paromita Mitra is an Under Graduate Student pursuing B.Tech in Electronics and Communication Engineering from JIS College of Engineering, Kalyani, West Bengal, India. She has 2 Published Patents. She has been to the Finals of CSI InApp National Project Awards 2017 along with Prof. Rajdeep Chowdhury. Her fields of interest include Cryptography, Data Warehouse and Network Security.

Rohit Ghosh is an Under Graduate Student pursuing B.Tech in Mechanical Engineering from JIS College of Engineering, Kalyani, West Bengal, India. His fields of interest include Cryptography and Data Warehouse.

Sukhwant Kumar is an Under Graduate Student pursuing B.Tech in Mechanical Engineering from JIS College of Engineering, Kalyani, West Bengal, India. His fields of interest include Cryptography and Network Security.