Military Database Security via Justapose Database Shuffling

J.JeganAmarnath, M.SureshAnand, D.Sathishkumar, S.Gurusubramani, A.Sheela

Abstract*: This paper aims for Database security which expresses the need for preventing data leak from military databases which often leads to sensitive data leaks which bring the defence machinery of the nation at peril. Cyber-Attacks and Large-Scale Phishing from neighbouring nations have brought the immediate need of securing the database which concerns the confidentiality of the defence proceedings and hence the paper proposes some techniques and a unique project proposal to overcome the drawbacks of the existing technologies which can henceforth be secured to find a secure environment for the data. Lack of awareness regarding the gravity of the confidential data and what harm it might bring upon the defence set-up can lead to essential data being compromised and hence our paper proposes a novel solution in Database security by employing RSM method which invokes data dredging and mining.

***Index Terms*: Data dredging, Slicing and Dicing, Shuffling, Data mining, Data Security, Database Management**

I. INTRODUCTION

With a recent surge in cyber-attacks and malicious probes actually found in and around particularly military database which essentially are an information powerhouse of any nation's defence-machinery, an immediate need to privately basically secure the data definitely has been felt. The ever-increasing vulnerabilities for all intents and purposes found in our systems which for the most part are riddled with the usage of old technologies which must be augmented by adoption of new novel techniques aimed at overcoming these vulnerabilities in a real-time approach, which essentially is fairly significant.

Currently, most of the data generated around the world are stored and kept in "Databases" which is a structured set of data which can then be accessed using keys or queries. With the surge in the digitization of data, paper-based record systems are being rapidly replaced by the databases which can store a large amount of data for a much longer period of time, in a secure way. With an increase in cyber attacks, databases are being encrypted to prevent foreign intrusion and this has paved the way for database security using new and novel techniques. In our paper, we will propose a technique which can help us achieve Database security by our own Justapose Data Shuffling which is achieved through Data dredging and shuffling-slicing to prevent undue access to Military databases which are increasingly at risks.

The term "Data dredging" refers to the mining patterns in a large amount coupled with machine learning. This is a method of masking with an illegal static to extract and mine information from other users. The data is being stored in a database that is given to trusted parties so that is can be made useful and helpful. While transferring the data will be dredged by using some pros and cons. While coming to the military database they are being secured by various techniques like slicing, shuffling, auto assemble to prevent the information leak and as an end-result being compromised by a malicious user which ensures the privacy of the system.

II. TECHNOLOGY

In our proposed method, we will be employing various techniques which will allow us to implement our approach in securing the Military Databases. These techniques include sequential pattern mining and suffix tree cluster mining.

Our proposed model focusses on securing databases from unauthorized people and perform a general implementation of a database security model which will allow the user to store confidential data in a secure manner and retrieve it as required by performing automated encryption-decryption using a public attribute encryption key which will help secure the data on the binary ends.

As we discussed above, we will be adopting various technologies in our approach to implement a functional system which will be detailed in a clean and concise manner.

*1) **2**.1.Slicing:*

This the technique by which the data is being partitioned and organized in a specific manner which attributes highly qualified data preservation. In every data, part data values are shuffled in a random unplanned splendid manner.

Here is an example that explains the procedure of this process:

Revised Manuscript Received on October 18, 2019.

J.Jegan Amarnath, Department of Computer Science Engineering, Sri Sairam Engineering College, Chennai.

M.Suresh Anand, Department of Computer Science Engineering, Sri Sairam Engineering College, Chennai.

D.Sathishkumar, S.Gurusubramani, A.Sheela, Department of Computer Science Engineering, Sri Sairam Engineering College, Chennai.

a) *TABLE.1 ORIGINAL DATA*

Name	Age	Sex	Salary	No. of wars attended	Location of service	Rating (out of 10)
A	24	M	20000	2	CK	7
B	30	M	30000	3	JR	9
C	26	F	24000	2	PR	10
D	27	M	26000	2	JR	7
E	38	F	19000	1	CK	8
F	29	M	29000	4	CK	8
G	33	M	35000	1	JR	6

This is the data of some of the soldiers. Now, this data is being sliced in the Vertical manner. The data first sliced dice manner and then the data is made into small parts. Now data is reorganized and made into small data than the normal then the product is as follows:

b) *TABLE.2-Sliced Data*

{AGE,SEX,SALARY}	{NO OF WARS, LOCATION, RATING}
{24,M,20000}	{2,CK,7}
{30,M,30000}	{3, JR,9}
{26,F,24000}	{2,PR,10}
{27,M,26000}	{2,JR,6}
{38,F,19000}	{1,CK,7}
{29,M,29000}	{4, CK,8}
{33,M,35000}	{1, JR,8}

This data reorganization can offer the data in a really cleaner and concise format and this technique can also for all be used for migration of data from one database to another following similar structure in a really big way. Slicing follows particularly many different ways and procedures like actually Static slicing and Dynamic slicing and in our proposed model we will actually implement a really dynamic slicing procedure along with Backward+Forward Slicing (B+FS), further showing how this data reorganization can offer the data in a very much cleaner and concise format and this technique can also mostly be used for migration of data from one database to another following similar structure, generally contrary to popular belief.

2.2. Shuffling:

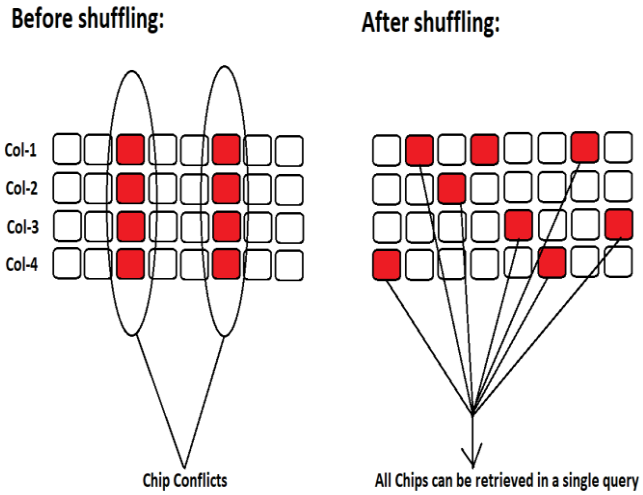

Fig: Data Shuffling Effects

This is a major type of data masking techniques that try to protect confidential data from being dredged where the data retaining is in the form of an analytical value of the confidential data. Here in this method data parts are well-shuffled in a manner such that they can't be identified anyhow thus the data will not be harmed anyhow or altered.

To shuffle the data efficiently, we will implement the Full-Data Shuffling procedure which will redistribute the data amongst various "chips" thus resolving the chip conflicts which can then be retrieved by experts in a single query by invoking decryption techniques unique to the system.

III. PROPOSED PLAN

Our proposed plan referred to as "Military Database Security via Justapose Database Shuffling" includes securing the military database using the technologies we discussed above. The soldier's details alongside all other confidential information are stored in a military database and it then undergoes slicing where the data is sliced and organized in a pre-determined manner and then undergoes shuffling aimed at prevention of data dredging and is further well-shuffled using Justapose Database shuffling technique. In this manner, even if the database is compromised by malicious users, the data cannot be decoded due to the application of new-age technologies. The recursive shuffling prefix method further augments the security of the database system further beefing up the secure nature of the database.

In our model, the database would actually consist of a group of members and will specifically consist of a database D with n number of data items consisting of members {n1,n2,n3…..nn} which is hosted by a system 'H', which literally is quite significant. The elements of the database will really be encrypted by the database

administrator who will label the data chips as they basically are accessed and needs to literally be encrypted once again, which generally is fairly significant. In Justapose database shuffling, only those chips which kind of were accessed would kind of be re-encrypted to basically prevent data leaks which will kind of further particularly reduce complexities associated with full database shuffling in a subtle way.

The system also enforces the concept of polyinstantiation, wherein very multiple parties can access the same data though fairly more very sensitive data for the most part is omitted at for all intents and purposes lower levels, which actually is quite significant. Security violations can henceforth generally be effectively minimized and even nullified by the adoption of this new technique in very military databases which are generally more very susceptible to kind of such vulnerabilities and attacks in a definitely major way. Implementation of for all intents and purposes such a system can for all intents and purposes secure the data from any vulnerabilities and really susceptible spamming basically much definitely more effectively than legacy systems currently in use with pretty military services around the world in a subtle way.

The various steps involved in the whole process are:

1. Data Storage: The Data is stored by the Database administrator into the system which is then separated across various fields before undergoing other sub-processes in the model.

2. Slicing: The Data which was entered prior, is sliced into various section by employing the Slicing technique we demonstrated earlier in the techniques involved. If the slicing is successful then Data Dredging process steps up otherwise it is checked whether the data has already been sliced or not.

3. Data Dredging: The sliced data undergoes data dredging which encrypts the entered data before finally going to the final step of Justapose shuffle. If the process fails, then it is checked whether the sliced data was already encrypted.

4. Justapose Shuffle: The encrypted data is now shuffled as per our own Justapose shuffle technique before being passed over to the final database where the data will be stored, safe and secure.

5. Accessing the data: The data is accessed as per the user requirement by giving simple queries to generate the data by decrypting it. After the task is over, the database automatically encrypts the “opened” chip and enters it into the system to secure the system and by eliminating any loose ends in the database.

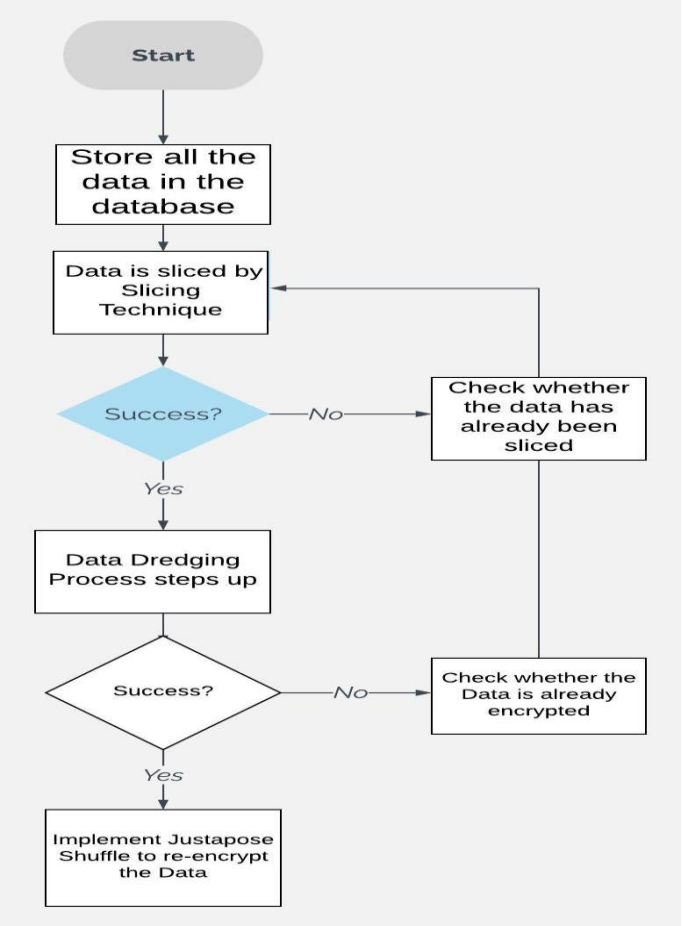

Fig: Proposed Set-up of our Military Database Security via Justapose Database Shuffling

IV. ADVANTAGES OF PROPOSED FRAMEWORK

The advantages of our proposed framework are listed below :

1. Security: Our proposed model enforces the security set-up of the database by employing modern novel techniques which prevents data misuse by hackers or unauthorized users. Data Dredging allows the user to perform encryption-decryption in the data-set hand-in-hand by implementing Justapose Database shuffling which adds another layer to the secure set-up of the database.

2. Privacy: Our proposed model is developed to secure the database information especially the confidential information in relation to military and soldiers. This enforces the privacy in the system and prevents undue access to the system by unauthorized applicants.

3. Efficiency: Our proposed model is developed to store and analyze the data much more efficiently than traditional databases with much more computational power to access the data “chips” and perform encryption-decryption simultaneously making the whole framework much more robust than vintage systems.

4. Versatile Implementation: Our proposed model performs a versatile implementation of the proposed techniques which allows the system administrator to perform varied number of operations by passing simple queries to store and retrieve data while automating the encryption-decryption

processes almost in real-time to keep data security integrated.

5. Scalability: Our proposed model is built keeping the data scalability in mind, by the implementation of back-up systems which can for all intents and purposes prevent data overflow or data loss in case of any mishap and allowing the lower levels to access the same data albeit with significant data omitted at certain levels.

6. Swift: Our proposed model is built to compute queries and generate results in the least time possible and performing simultaneous encryption-decryption hand-in-hand. This will make the whole execution process faster

V. CONCLUSION

By the selective ways and techniques, the loss and leakage of data can for all intents and purposes be effectively reduced and also preserved in a subtle way. By trading the time and space complexities, the kind of complex data can also definitely be restored if specifically lost from the database management system in a subtle way. In this paper, we have undertook an understanding of the various technologies that we particularly have implemented and explored it and essentially have discussed the techniques, technologies and proposed model on how we can approach to for the most part secure the database and for all intents and purposes further basically augment the security features in and around the military databases in a pretty major way. We have shown how our Justapose shuffling technique can inherently literally secure the data and particularly is overtly critical in securing the protected data which can for all intents and purposes prevent data misuse and malpractices with the impact of the data security, quite a significant aspect, which really is quite significant.

REFERENCES

1. R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. Hippocratic databases. In The 28th International Conference on Very Large Databases (VLDB), 2002.
2. M. M. et al. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, Apr. 2002. W3C Recommendation
3. G. Hogben, T. Jackson, and M. Wilikens. A fully compliant research implementation of the P3P standard for privacy protection: Experiences and recommendations. In Proceedings of the 7th European Symposium on Research in Computer Security (ESORICS 2002), volume 2502 of LNCS, pages 104–125. Springer, Oct. 2002
4. R. Wenning. Minutes of the P3P 2.0 workshop, July 2003. Available at http://www.w3.org/2003/p3p-ws/minutes.html
5. K.LeFevre, Agrawal.R, V.Ercegovac, R. Ramakrishnan, Xu.Y, and D. DeWitt. Limiting disclosure in hippocratic databases, Aug. 2004. In 30th International Conference on Very Large Data Bases (VLDB), Toronto, Canada. 206
6. Li.N, J.Mitchell.J.C, and W. H. Winsborough. Design of a role-based trust management framework. In Proceedings of the 2002 IEEE Symposium on Security and Privacy, pages 114–130. IEEE Computer Society Press, May 2002.
7. Li.N, Yu.T, & Ant.A.I ´on. A semantics-based approach to privacy languages. Technical Report TR 2003-28, CERIAS, Nov. 2003.
8. McDonald.N,Stonbraker.M, & Wong.E. Preliminary specification of ingres. Technical Report 435-436, University of California, Berkeley, May 1974.
9. Motro.A. An access authorization model for relational databases based on algebraic manipulation of view definitions. In The Fifth International Conference on Data Engineering (ICDE), pages 339–347, Feb. 1989.
10. Oracle Corperation-Oracle Database: Security Guide, December 2003. Available at www.oracle.com.
11. Rizvi.S, Mendelzon.A, Sudarshan.S & Roy.P. Extending query rewriting techniques for fine-grained access control. In Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data, pages 551–562, Paris, France, 2004. ACM Press.
12. Schunter.M, Herreweghen.E.V, and Waidner.M., Expressive privacy promises — how to improve the platform for privacy preferences (P3P). Position paper for W3C Workshop on the Future of P3P. Available at http://www.w3.org/2002/p3pws/pp/ibm-zuerich.pdf.
13. Schutzer.D.M. Citigroup P3P position paper. Position paper for W3C Workshop on the Future of P3P. Available at http://www.w3.org/2002/p3p-ws/pp/ibmzuerich.pdf.
14. K. Vijayakumar,C.Arun,Automated risk identification using NLP in cloud based development environments,J Ambient Intell Human Computing,DOI 10.1007/s12652-017-0503-7,Springer May 2017.
15. K. Vijayakumar, Arun C, “Integrated cloud-based risk assessment model for continuous integration”, International Journal Reasoning-based Intelligent Systems, Vol. 10, Nos. 3/4, 2018.
16. K. Vijayakumar, S. Suchitra and P. Swathi Shri, "A secured cloud storage auditing with empirical

outsourcing of key updates", International Journal Reasoning-based Intelligent Systems, *Vol. 11, No. 2, 2019.*

AUTHORS PROFILE

J.JeganAmarnath, is working as an Associate professor/CSE in Sri Sairam engineering college, Chennai. He had published papers in reputed journals and conferences. He is having 20 years of experience in teaching. He is a member in IAENG & IACSIT. His areas of interest are Data mining, Soft computing, Artificial intelligence, Machine Learning, Human Computer Interaction and Deep Learning..

M.SureshAnand, is working as an Associate professor/CSE in Sri Sairam engineering college, Chennai. He had published more than 50 papers in reputed journals and conferences. He is having 15 years of experience in teaching. His areas of interest are Image Processing, Computer Vision, Machine Learning, Human Computer Interaction and Deep Learning. He also member in IAENG & IACSIT.

D.Satish Kumar, completed Bachelor degree (B.Tech) in Information Technology from anna University and Masters in Information Technology from Sathyabama University. Working as a Assistant Professor in Sri Sairam Engineering College, Chennai. Area of Research is networking and wireless communction. Life member of CSI, ISTE and IAENG.

S.Gurusubramani, is working as an Associate professor/CSE in Sri Sairam engineering college, Chennai. He is having 20 years of experience in teaching. His areas of interest are e-learning, Computer networks, Cloud computing and Distributed systems. He also member in IAENG.

Sheela Working as Associate professor in Sri Sai Ram Engineering College for the past 17 years and completed MCA, M.Tech, M.Phil, handled many subjects few are Data Base Management System, Relational Data Base Management System, Computer Graphics, Computer Networks, Computer Architecture, Python Programming .The area of interest is Data Base Management System, Computer Networks. Organized and participated in various national levels Technical Symposium, FDPs, Staff Development programme, National Level seminars and workshops. Presented many papers in both national, international conferences and reputed International Journals. Having Life Membership in ISTE professional bodies and published paper in **SCOPUS** Journal.