Dynamic Trust Emergency Role-based Access Control (DTE-RBAC)

Amar Arora
Scientific Assistant, NIC
MeitY, Govt. of India
Delhi, India

Anjana Gosain
Professor, USICT
GGSIPU
Delhi, India

ABSTRACT
Data Warehouse (DW) security has always been a critical challenge for DW designers because of its global reachability via public networks. In order to maintain trade-off among security and accessibility, Role-Based Access Control (RBAC) has been considered a balanced approach over time. However, RBAC being inflexible, makes way for a flexible approach like break-the-glass (BTG) for emergencies. It allows overriding of all access control policies during an emergency like a fire, etc. To prevent any misuse of emergencies in BTG, Emergency RBAC (E-RBAC) proposed a combination of flexibility of BTG and separation of duty (SOD) constraints. Here, SOD constraints help in limiting user access to a certain level. In order to prevent any misuse, E-RBAC only allows users with high trust levels to initiate emergencies. The trust levels of users are calculated based on predefined parameters like experience, training hours, and user skill attributes, and thus remain fixed for a user. Here, in this paper, a dynamic trust analysis of the user based on the actions taken by them during the acquired emergencies has been proposed. The trust of the user can be dynamically modified to a lower level in case the action of the user leads to a breach of trust. The dynamic trust level of users prevents the system from any further damage in case of attempted misuse of emergencies. This paper also proposes the DTE-RBAC model, which provides a complete security solution to deal with the situation of breach of trust by highly trusted users in an automated fashion.

Keywords
Data Warehouse Security, Role-Based Access Control, Emergency RBAC.

1. INTRODUCTION
Data Warehouse (DW) [1] security has always been a concern for designers as it stores sensitive information about businesses. Its global accessibility via the internet makes it more challenging to provide a balance among security challenges and accessibility. Here, RBAC [2] seems to have been considered one of the suitable mechanisms to control the access of users as per their role in the organization structure [3]. The roles and associated predetermined privileges in an RBAC environment make it behave like a static mechanism. This inflexible approach makes RBAC unsuitable for solving emergencies [4]. For, e.g., a DW's junior executive may have to perform actions of DW administrator in emergencies. Thus, a flexible approach break-the-glass (BTG) [5] proposed to deal with the emergencies. It allows the overriding of the access permissions by the user to deal with the emergency in a controlled manner [6].

In the context of DW, various RBAC and its extensions [7–13] have been proposed over time. The focus of all these approaches has been on improving the balance among flexibility and security of access control mechanisms. In RBAC, each user acquires some roles, and roles access is limited to permissions to access objects [11]. However, in case of an emergency, the restrictions have to be minimized, along with maximizing the auditing of the actions performed [4, 5]. Here, the minimization of restrictions opens a new threat of misuse of these minimized restrictions. However, none of the approaches handle the emergency; therefore, in [4], the authors proposed that during emergencies, the users holding the highest level of trust are mostly allowed to handle it. Here, the authors proposed that each user holds a predefined trust level based on various parameters like work experience, hours of training, skill attribute, etc. Under the existing system, there is no check on the trust levels in the event of abuse of trust. In this paper, a dynamic trust level of the users has been introduced, where the system can lower the trust level in case misuse of the system is detected. It can prevent any further damage to the system when the trusted user tries to exploit the system's emergency for its advantage.

The main contributions of this paper are as follows:

- It introduces the dynamic user trust mechanism by the inclusion of misuse detection connected to the audit system.
- It lowers the user trust level at run time based on the feedback of the misuse detector. It will not only prevent the breach of trust but also prevent the misuse or damage to the system in the ongoing emergency.

The rest of the paper has been structured as follows: Section 2 discusses related work. Whereas Section 3 discusses the proposed dynamic trust model, including misuse detection, Section 4 provides a case study on the proposed solution and its advantage, and Section 5 concludes with outcomes and possible future work.

2. RELATED WORK
The number of work has been performed in the literature [14, 15] on the security of DWs over time. Out of all the different security mechanisms such as Mandatory Access Control [16], Adaptive Mandatory Access Control over OLAP [17], DW Encryption [18], Query Over Encrypted Warehouse [19, 20], etc., the user's accessibility over the different elements is still managed by Role-Based Access Control (RBAC) [2] and its proposed extensions. Initially, DWs are widely using RBAC as its security component, but it faces many issues regarding the decision process, multiple roles, multiple sessions, and many other temporal dependencies [9]. Thus, Extended-RBAC combines RBAC with UCON [21] to provide robust access and usage control security mechanisms. In another variation of RBAC, Temporal RBAC [11] has allowed temporary limitations on roles, user-permission assignments (UA), permission-role assignments (PA), and role hierarchies

(RH). The generalized temporal role-based access control (GTRBAC) model [22], on the other hand, capable of expressing a wide range of temporal constraints. This model allows expressing periodic as well as duration constraints on roles, user-role assignments, and role-permission assignments. Another approach considers the location-aware separation of duty while designing the role of the users and their respective access controls [23]. In another research proposal, a spatiotemporal information based access control [24] proposed an association of each component of RBAC with spatiotemporal information. Some recently proposed extensions of RBAC include RNBAC Model [25] and RNBAC-SC [26].

All the works involving RBAC and its variations provide an access control solution for different situations and perspectives. Here, every user shares a single or, multiple roles and each role has been assigned permissions to access resources. However, in an emergency like a fire breakout, a user may have to perform some additional tasks beyond his role permissions. Two different approaches, BTG [5, 6] and delegation [27, 28], have been proposed in the literature to tackle emergencies. Delegation methods work on a principle of transfer of jobs with access rights from one user to another [27]. The delegation has been mostly temporary and revoked after the expiry of the time limit.

On the other hand, BTG [5, 6] policy allows overriding of the existing access control. It allows a user to have access to the inaccessible areas in case of emergencies. Over time, BTG has also evolved with many enhancements like specifying break-glass policies with support to model-driven development techniques [29]. Another approach [30] allows the possibility to override a denied decision. During any proposal of access control override, the system prepares logs for every access or action taken for special auditing. In one of the recent proposals, TS-RBAC [31] proposed to bring dynamic changes in user permissions through transformation. It brings flexibility to the system by keeping the safety introduced by BTG-RBAC; it achieves this by changing the role-to-user assignment (UA) dynamically. Since modification of role and system constraints is a tedious task, [4] introduced a concept of separation of duty (SOD), where SOD controls and limits user access in emergencies. It also introduced the concept of the trust level (Ut), depending on predefined factors like user work experience (Aue), user training hours attribute (Aut), and user skill attribute (Aus). The trust level (Ut) categorizes a trust level of user as Low(L), Medium(M), and High(H), which decides the accessibility to Normal, Emergency, and Exception situations. However, these trust levels are static and pre-deterministic and can be a case of security threat. Section 4 discusses the complete scenario in detail with the help of a case study.

3. DYNAMIC TRUST EMERGENCY ROLE-BASED ACCESS CONTROL MODEL

The proposed DTE-RBAC has three significant components 1. Emergency RBAC, 2. User Trust Analyzer, and 3. Misuse Detector, as given in Fig 1.

1. Emergency RBAC deals with all the RBAC controls to provide controlled access of DW resources to users as per their role. It also has the responsibility to define the emergency roles, obligations, and permissions, which is similar to the one proposed in E-RBAC [4].
2. The misuse detector is connected directly to the audit logs and has the responsibility to detect any case of misuse of the emergency role by the user. Whenever a misuse is detected, it provides the information of the detected user to the user trust analyzer.
3. The user trust analyzer has the responsibility to determine the user's trust level at the run time and providing it to the emergency RBAC for further action.

Section 3.1 provides the complete working of DTE-RBAC in detail.

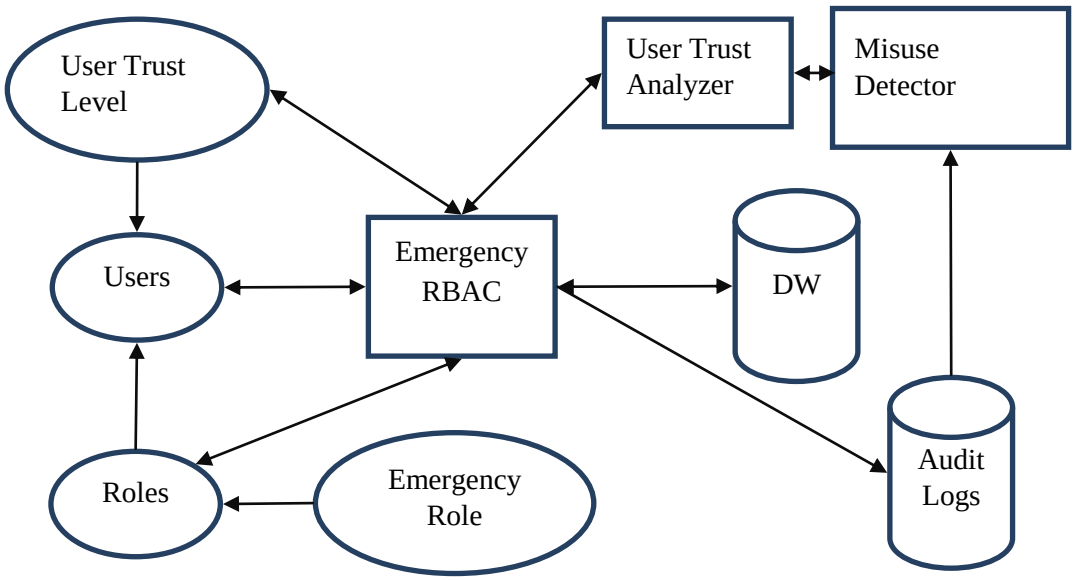

Fig 1: Dynamic Trust Emergency Role-Based Access Control (DTE-RBBAC) Model

3.1 Working of DTE-RBAC

The detailed working of the DTE-RBAC has been given below:

1. Initially, a user enters into the system after clearing the initial authentication phase. Once authenticated, the user acquires a role and then its access to the DW elements controlled by the Emergency RBAC as per its acquired

role(s).

2. The user trust analyzer calculates the user trust level based on predefined parameters such as experience, hours of training, etc. and also on the feedback from the Misuse Detector about the user's historical actions from the audit logs. Initially, when the user enters the system for the first time, the misuse detector's feedback remains zero.
3. The user trust analyzer classifies the user trust level as High, Medium, or Low and informs the same to Emergency RBAC for further action.
4. Then, Emergency RBAC assigns the trust level calculated by the user trust analyzer to the respective user.
5. Once a user requests an emergency role, Emergency RBAC checks the user's trust level. If the trust level is not High, then the request is immediately dropped.
6. Otherwise, an emergency role is provided only after performing obligations, such as enabling the audit system, notification to system administrators regarding emergency, etc. After that, the user can perform emergency operations.
7. On completion of the emergency task, the user informs Emergency RBAC, which immediately revokes the emergency role from the role list of the user.
8. Here, the misuse detector keeps analyzing the audit logs for any suspicious activity from the user in previously or currently acquired emergencies. If any abuse of emergency is detected, the misuse detector triggers the misuse event to the user trust analyzer.
9. Based on the trigger from the misuse detector, the user trust analyzer again calculates the user trust level, including the feedback from the misuse detector. It immediately informs Emergency RBAC about the new trust level of the user.
10. Emergency RBAC assigns the new trust level to the respective user accordingly.
11. Once the trust level of the user drops from High to a lower trust level, Emergency RBAC blocks the user's access to an emergency role, including the currently acquired, if any.
12. This lowering of the user's trust level helps to avoid any abuse of an emergency role and also prevents the system from any further damage.

Here, the misuse detector will always be in listening mode and analyzing the audit logs for any misuse. So, in case any user tries to steal any information or tries to corrupt any data during emergency role acquisition, his attempt can be foiled. Here, lowering the trust level of the user will help in blocking the access to the emergency role any further along with protection to the ongoing emergency role misuse. During emergencies, the RBAC has minimum control over the system; the breach of trust can be very costly to the entire organization. Therefore, misuse detection can be a vital tool to prevent any damage to the system due to a breach of trust by highly trusted users.

4. CASE STUDY

Let us consider a healthcare system scenario, where the hospital staff members are classified into High, Medium, and Low trust levels as per their level in the organization, the experience they hold, and the training they have undertaken. Based on their trust levels, it has been decided that only employees with High trust levels will be able to access the backup systems during emergencies like fire or waterlogging in the data center. However, before performing backup operations, one has to perform obligations, such as enabling the audit system, notification to all the heads, and system administrators regarding emergency and other required steps in the emergency manual. After that, the user can proceed for an emergency backup of all the databases and upload it on the cloud systems, etc. Here, after taking backup, the user needs to complete the post backup formalities again, like, sending the notification, switching off all the systems, etc. In the above scenario, the user handling the emergency might need to override all the access controls if he does not belong to the system administrators. Here, every action performed by the user during the emergency has been logged and used for audit purposes. It helps establish the responsibility of users for each action they take during the emergency as they are accessing many resources outside their access rights.

Here, E-RBAC [4] solves these scenarios by defining emergency roles, role-to-user assignment, administrative role range, permission-to-role assignment, and SSD (static separation of duty) constraints. Initially, once a user asks for the emergency role, his trust level is verified in the role-to-user assignment. If the trust level is High, and the user role is within the administrative role range, then further checks are initiated, else the request for emergency role stands denied. Further checks involve verification of SSD constraints, which verified the role of the user and the classification of duties that need to be performed. E.g., a doctor has a high trust level, cannot be given a data backup task. If the emergency role requested does not lie in SSD constraint, an emergency role can be given to the user where it performs tasks as per rights provided in the permission-to-role assignment. Every user action gets logged into the audit logs as it creates full responsibility for the user for his actions undertaken during an emergency.

Here, the user trust level acts as a first check to verify its access to initiate an emergency, and it remains static throughout as it is dependent on his experience, training hours, and skills. What if there is a breach of trust? E.g., the user has tried to delete a specific record during an emergency while initiating the backup or tries to copy a record to separate files other than backup sent to the cloud systems. These actions might be by the trusted user itself or an attacker who enter the system using compromised credentials of a highly-trusted user. There is no existing system in place where the user's trust level can be modified based on the analysis of audit logs. Here, the proposed model in section 3 introduced a misuse detector within the emergency role-based access control. The misuse detector notifies the user trust analyzer whenever it detects any user's suspicious action during an emergency. After that, the user trust analyzer lowers the user's trust level dynamically to prevent any further loss to the system.

5. CONCLUSION AND FUTURE WORK

This paper proposed the DTE-RBAC model to prevent misuse of emergency roles by any user. It proposed a misuse detector that analyses the audit logs to identify any breach of trust by highly-trusted users. Moreover, the trust level of the user can be lowered dynamically based on the feedback of the misuse detector. The dynamic trust level of users makes it difficult for any user to keep acquiring an emergency role by making a

fake emergency call. It prevents any further damage to the system on the detection of misuse during an emergency acquired by a user. As trust level acts as an initial check for the acquisition of an emergency role, the dynamic trust analysis, and its modification make it difficult for an attacker to attack using a highly trusted user's compromised credentials.

A misuse detector with a signature-based algorithm will be desiged to make it robust and self-learning in further studies. There is also a plan to implement the system in a standard DW environment like TPC-H to analyze its performance.

6. REFERENCES

[1] Inmon WH. 1991. Building the Data Warehouse. Wiley and Sons

[2] Sandhu R. 1995. Issues in RBAC. In: RBAC '95. ACM, New York, Gaithersburg, Maryland, USA, p 6

[3] Vela FLG, Montes JLI, Rodríguez PP, et al. 2007. An architecture for access control management in collaborative enterprise systems based on organization models. Sci Comput Program 66, 44–59. https://doi.org/10.1016/j.scico.2006.10.005

[4] Nazerian F, Motameni H, Nematzadeh H. 2019. Emergency role-based access control (E-RBAC) and analysis of model specifications with alloy. J Inf Secur Appl 45, 131–142. https://doi.org/10.1016/j.jisa.2019.01.008

[5] Ferreira A, Chadwick D, Farinha P, et al. 2009. How to Securely Break into RBAC: The BTG-RBAC Model. In Proceedings of the 2009 Annual Computer Security Applications Conference. IEEE, pp 23–31

[6] Rissanen E, Firozabadi BS, Sergot M. 2004. Towards a Mechanism for Discretionary Overriding of Access Control. In Proceedings of the Christianson B, Crispo B, Malcolm JA, Roe M (eds) Security Protocols. Springer Berlin Heidelberg, Berlin, Heidelberg. pp 312–319

[7] Sandhu RS, Coyne EJ, Feinstein HL, Youman CE. 1996. Role-based access control models. Computer 29, 38–47. https://doi.org/10.1109/2.485845

[8] Fernández-Medina E, Trujillo J, Villarroel R, Piattini M. 2006. Access control and audit model for the multidimensional modeling of data warehouses. Decis Support Syst 42, 1270–1289. https://doi.org/10.1016/j.dss.2005.10.008

[9] Thuraisingham B, Iyer S. 2007. Extended RBAC - Based Design and Implementation for a Secure Data Warehouse. In Proceedings of the ARES'07. IEEE, Vienna, Austria. pp 367–382

[10] Zou D, He L, Jin H, Chen X. 2009. CRBAC: Imposing multi-grained constraints on the RBAC model in the multi-application environment. J Netw Comput Appl 32, 402–411. https://doi.org/10.1016/j.jnca.2008.02.015

[11] Uzun E, Atluri V, Vaidya J, et al. 2014. Security analysis for temporal role based access control. J Comput Secur 22, 961–996. https://doi.org/10.3233/JCS-140510

[12] Longstaff J, Noble J. 2016. Attribute Based Access Control for Big Data Applications by Query Modification. In Proceedings of the 2016 IEEE Second International Conference on Big Data Computing Service and Applications (BigDataService). pp 58–65

[13] Jabbar S, Khan M, Silva BN, Han K. 2018. A REST-based industrial web of things' framework for smart warehousing. J Supercomput 74, 4419–4433. https://doi.org/10.1007/s11227-016-1937-y

[14] Santos RJ, Bernardino J, Vieira M. 2011. A survey on data security in data warehousing: Issues, challenges and opportunities. In Proceedings of the 2011 IEEE EUROCON - International Conference on Computer as a Tool. pp 1–4

[15] Gosain A, Arora A. 2015. Security Issues in Data Warehouse: A Systematic Review. In Proceedings of the International Conference on Computer, Communication and Convergence (ICCC 2015). Procedia Computer Science. Elsevier. pp 149–157

[16] Osborn S, Sandhu R, Munawer Q. 2000. Configuring role-based access control to enforce mandatory and discretionary access control policies. ACM Trans Inf Syst Secur TISSEC 3, 85–106. https://doi.org/10.1145/354876.354878

[17] Pietraszek T. 2004. Using Adaptive Alert Classification to Reduce False Positives in Intrusion Detection. In Proceedings of the International Workshop on Recent Advances in Intrusion Detection. Springer, Berlin, Heidelberg. pp 102–124

[18] Santos RJ, Bernardino J, Vieira M. 2012. Evaluating the Feasibility Issues of Data Confidentiality Solutions from a Data Warehousing Perspective. In Proceedings of the International Conference on Data Warehousing and Knowledge Discovery. Springer, Vienna, Austria. pp 404–416

[19] Kadhem H, Amagasa T, Kitagawa H. 2013. Optimization Techniques for Range Queries in the Multivalued-partial Order Preserving Encryption Scheme. In Proceedings of the Fred A, Dietz JLG, Liu K, Filipe J (eds) Knowledge Discovery, Knowledge Engineering and Knowledge Management. Springer Berlin Heidelberg, Berlin, Heidelberg, pp 338–353

[20] Lopes CC, Times VC, Matwin S, et al. 2014. Processing OLAP Queries over an Encrypted Data Warehouse Stored in the Cloud. In Proceedings of the Bellatreche L., Mohania M.K. (eds) Data Warehousing and Knowledge Discovery. Springer. pp 195–207

[21] Park J, Sandhu R. 2004. The UCON ABC usage control model. ACM Trans Inf Syst Secur TISSEC 7, 128–174. https://doi.org/10.1145/984334.984339

[22] Joshi JBD, Bertino E, Latif U, Ghafoor A. 2005. A generalized temporal role-based access control model. IEEE Trans Knowl Data Eng 17, 4–23. https://doi.org/10.1109/TKDE.2005.1

[23] Gupta A, Kirkpatrick MS, Bertino E. 2014. A formal proximity model for RBAC systems. Comput Secur 41, 52–67. https://doi.org/10.1016/j.cose.2013.08.012

[24] Ray I, Toahchoodee M. 2007. A Spatio-temporal Role-Based Access Control Model. In Proceedings of the Barker S, Ahn G-J (eds) Data and Applications Security XXI. Springer Berlin Heidelberg, Berlin, Heidelberg. pp 211–226

[25] Wang S, Yang Y, Xia T, Zhang W. 2018. A Role and Node Based Access Control Model for Industrial Control Network. In Proceedings of the 2nd International

Conference on Cryptography, Security and Privacy. Association for Computing Machinery, New York, NY, USA. pp 89–94

[26] Cruz JP, Kaji Y, Yanai N. 2018. RBAC-SC: Role-Based Access Control Using Smart Contract. IEEE Access 6, 12240–12251

[27] Osborn SL, Wang H. 2013. A Survey of Delegation from an RBAC Perspective. J Softw 8, 266–275

[28] Schefer-Wenzl S, Bukvova H, Strembeck M. 2014. A Review of Delegation and Break-Glass Models for Flexible Access Control Management. In Proceedings of the Abramowicz W, Kokkinaki A (eds) Business Information Systems Workshops. Springer International Publishing, Cham. pp 93–104

[29] Brucker AD, Petritsch H. 2009. Extending Access Control Models with Break-Glass. In Proceedings of the 14th ACM Symposium on Access Control Models and Technologies. Association for Computing Machinery, New York, NY, USA. pp 197–206

[30] Alqatawna J, Rissanen E, Sadighi B. 2007. Overriding of Access Control in XACML. In Proceedings of the Eighth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'07). IEEE. pp 87–95.

[31] Liu G, Zhang R, Song H, et al. 2016. Ts-RBAC: A RBAC model with transformation. Comput Secur 60, 52–61.https://doi.org/10.1016/j.cose.2016.03.006