Implementing Severity Factor to Mitigate Malicious Insider

Aziah Asmawi, Lilly Suriani Affendey, Nur Izura Udzir, Ramlan Mahmod

Abstract: ***Nowadays, the use of XML database is expending. XML is designed to store and transport data. A large quantity of information is presented in XML format on the web for easy transportation. Due to the increased use of XML database over the web, the need to protect this database is vital. In a multiuser system, where the information is being shared across users who have different permissions, the need to implement a security model which gives controlled access to the authorized users is very important. XML access control was introduced to suit this purpose. XML access control is a security mechanism which restricts the access of the XML data to authorized users. Many access control models and enforcement mechanisms have been proposed to prevent the unauthorized release of XML data. Who can access which information under what circumstances is implemented based on the access control policies.***

A database is very significant where it contains sensitive data that have been coordinated and maintained over usually long period of time, which make their loss or damage more costly. Databases used to save the data that have been collected and maintained over usually long period of time were loss of such data will cost more than any other components [1]. The problem of malicious insider is more risky in database systems because it manages precarious data. Many security technologies have been established to prevent threats from outsiders, but they have limited use in mitigating insiders misuse attacks. For instance, cryptography and encryption technique protects information from an outsider attack trying to obtain unauthorized access to it. However, these approaches could not provide an effective countermeasure against malicious insiders who already have authorized access to internal assets. Currently, there are some research techniques on detecting insider misuse attacks but the task of prohibited privileged insiders from internal assets still remains a challenge today.

It is essential to tackle security problems in XML databases to decrease the malicious insider threats. One of important factor that we had to consider when we talk about database security is the severity of each transaction. In this research, we propose severity factor to indicate severity value for each bad transaction in order to improve security level in XML database.

Index Terms: ***XML database, insider misuse, severity, trust value, access control***

I. INTRODUCTION

Insider misuse is one of the vital security issues in any database. Insider is a person who has privileges in the computer system can abuse their privilege to fulfil their bad intention.

Insider can abuse their privileges by typing in malicious inputs causing the application to crash, behave unpredicted manner or result in compromised integrity of data. Besides that, anomalous access of databases by the insider can result in the disclosure of confidential information and fraud. Insiders may misuse databases holding medical records, credit-card records, criminal records, customer data, personal records and statistical information related to businesses. For that reason, it is crucial to detect the misuse in database systems as it could provide the most relevant data, as well as this is the place where users directly interact with the application environment. This work focused on mitigating insider misuse attacks which using VIEW, INSERT, UPDATE and DELETE statements to compromise user privileges in XML database stored procedure.

II. OBJECTIVE

To implement severity-aware trust-based access control to provide protection for XML database-centric Web services to mitigate malicious insider.

III. LITERATURE REVIEW

An insider threat issue is cited as one of the most serious security problems; therefore have received significant attention (Richardson, 2008). It is also considered the most difficult issue to deal with because insiders often have the abilities not known to outsiders, and as a consequence can cause severe damage (Shatnawi et al. (2011).

Insider threats can impact in multiple dimensions such as financial loss, disruption to the organization, loss of reputation, and long-term impacts on organizational culture (Hunker & Probst, 2008).

Dealing with insider attack incidents is one of the most significant security issues faced by today’s information-based infrastructures. Researchers have proposed various mitigation techniques to tackle this threat [2] presented a threat evaluation system based on certain profiles of user behaviour. He presented a process of creating a language tailored to describe insider threat incidents.

[3] suggested a mixture of technical and psychological approaches to deal with insider threats while [4] had introduced trust-based access control for XML databases. It depends on a trust management system, which automatically calculates and updates the trust values of users.

Furthermore, [5] established a psychosocial model to evaluate employees’ behaviour, while [6] proposed an approach that combines Structural Anomaly Detection from social and information networks and Psychological Profiling of individuals so as to identify threats.

Revised Manuscript Received on May 05, 2019.

Aziah Asmawi, Universiti Putra Malaysia
Lilly Suriani Affendey, Universiti Putra Malaysia
Nur Izura Udzir, Universiti Putra Malaysia
Ramlan Mahmod , Universiti Putra Malaysia

[7] have also proposed a system for insider threat detection based on feature extraction. More recently, [8] define a tree-structure profiling approach that integrates the details of activities conducted by each user and each job role. These kinds of information are used to obtain a consistent representation of features that provide a description of the user's behaviour. Deviance can be defined based on the amount of variance that each user exhibits across multiple attributes.

Furthermore [9] focus on using the electrocardiogram (ECG) signals that arise from the user's heart activities in combination with the electroencephalogram (EEG) signals that arise from the user's brain activities and use them in insider threat detection. The proposed system analyses the user's bio-signals, extracts features, and classifies them in order to detect the malicious activities.

There are drawbacks in this approach, the setting of cables and electrodes may cause arousal or different emotions in people and therefore alter the results. Table 1 summarize the existing works on insider misuse attacks.

Research works presented in this paper have been recently proposed that solved the insider threat issue, but none focus on the insider misuse in XML database stored procedure. Furthermore, the problem solution proposed by previous works still cannot mitigate most of insider misuse attacks. Hence, this research enhances and extends the trust-based access control for XML database by [4] with the additional of severity feature for each query issued to the database. The key idea in this work is to prove that with the addition of severity factor to the calculation of trust value, it should enhance the security of the XML database.

A. Trust-Based Access Control Approach

Applying access control is one of the main approaches to guarantee security in any system. The access control model manages access to data and prevents unauthorised processes [10]. There are many access control models have been proposed and used. The traditional types are discretionary access control (DAC), mandatory access control (MAC), and role-base access control (RBAC) [11].

Unfortunately, most traditional access control models defend data from outsider's malicious activities instead of from insider's [12].

Trust-based access control for XML databases has been developed to increase security and provide dynamic access control for XML databases. It aims to offer secure access control by detecting insider threats through assessing users' operations over time.

Trust-based access control for XML databases accomplishes the access policy depending on users' trustworthiness and may avoid unauthorised processes, malicious transactions and misuse from insiders.

Outsiders who are not related to the system can be assumed to have no access right but outsiders imitating insiders should be detected. Trust scores are updated on the basis of users' histories. Users' privileges are automatically modified and adjusted over time depending on user behaviour to deal with insider threats.

Trust-based access control has become recognised in many applications [4]. It uses a trust management system that automatically calculates users' trust values which updated according to an evaluation of the user's history.

Trust depends on beliefs, operations, and recommendations [13]. It needs effort and time to achieve but it can be lost quickly and easily [14]. Trust is taken from the real world scenarios and applied to the digital world. In the access control, trust means the subjects can trust entities such as other subjects, applications and firms on the basis of past history, operations, behaviour, experience and recommenda -tions over time [15].

Table 1. Existing Works on Insider Misuse Attacks

Author (Year)	Existing Works on Insider Misuse Attacks	Analysis
Magklaras et al. (2006)	Introduced a threat evaluation system based on certain profiles of user behaviour. He presented a process of constructing a language tailored to describing insider threat incidents	failure to use logs, retain them, or analyse them makes it difficult to deal with repudiation threats
Kandias et al. (2010)	proposed a mixture of technical and psychological approaches to deal with insider threats	approach places too much emphasis on biology when clearly humans are influenced by many other factors
Farooqi & North, (2011)	had introduced trust-based access control for XML databases. It depends on a trust management system, which automatically calculates and updates the trust values of users.	yields weaker security and there are computational overhead occurs
Greitzer et al. (2012)	developed a psychosocial model to assess employees' behaviour	it can be confusing and misleading to use it correctly and appropriately for a new user
Brdiczka et al. (2012)	proposed an approach that combines Structural Anomaly Detection from social and information networks and Psychological Profiling of individuals so as to identify threats	the difficultly of defining rules and detect new attack
Eldardiry et al. (2013)	Proposed a system for insider threat detection based on feature extraction.	Mislabelled examples in feature selection and feature construction may induce the choice of wrong variables
Legg et al. (2015)	define a tree-structure profiling approach that incorporates the details of activities conducted by each user and each job role	this approach cause a lot of overhead if the memory locator do not efficient enough at creating tree nodes
Hashem et al. (2015)	Detect insider threat using psychophysiological signal monitoring	costly and complex to apply and people are fitted up with cables and electrodes

[4] previously has been use trust-based access control for XML databases in their research. They developed Trust Module which associated with the Access Control Module to form the whole system. This combination works to provide a secure environment to access XML databases depending on the evaluation of the users' history. Linking these two modules to work together generates the system processes that relate to both modules at the same time. The system architecture for trust-based access control is shown in Figure 1.

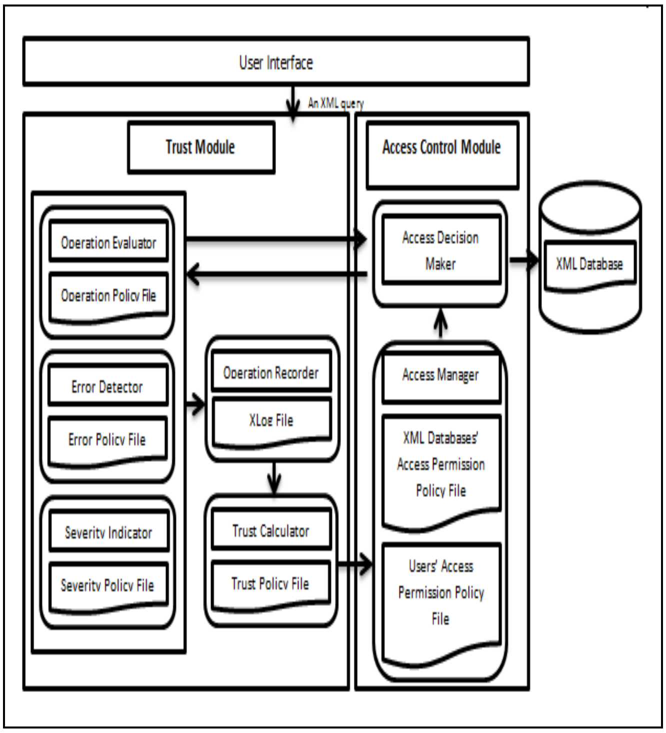

Fig. 1 Trust-based access control's system architecture [4]

Based on the Figure 1, there are two main modules in this architecture. The first module is Trust Module and the other module is Access Control Module. The Trust Module receives transactions from users, evaluates the transactions and calculates their TVs. The evaluation process depends on the users existing TVs, new bad transactions, and new errors. After that, it will send the TV to the Access Control Module to update the user's privileges.

B. Proposed Approach: Severity-Aware Trust-Based Access Control

This work proposes severity-aware trust-based access control to prevent insider misuse within XML database stored procedure. This approach increases data security by evaluating users' histories and operations. We extend the existing work by [4] by allowing for severity feature in calculating trust values. Our approach addresses insider misuse based on the calculation of Trust Value (TV) for each query issued by insider before they are executed in XML database. This kind of approach enhances the existing work proposed by [4], which used trust-based access control technique without severity-aware feature.

We adopt the idea of [16]) which use severity level in their classification scheme research. In this work, severity is defined as one of the additional feature in TV calculation to evaluate the query whether the query is allowed or denied. The rules of severity are stored in Severity Policy File. Severity Indicator will define each Data Manipulation Language (DML) in database stored procedure (SELECT, INSERT, UPDATE, DELETE) with its own severity values. We developed a prototype which employs the severity-aware trust based access control. The system architecture of severity-aware trust-based access control as depicted in Figure 2.

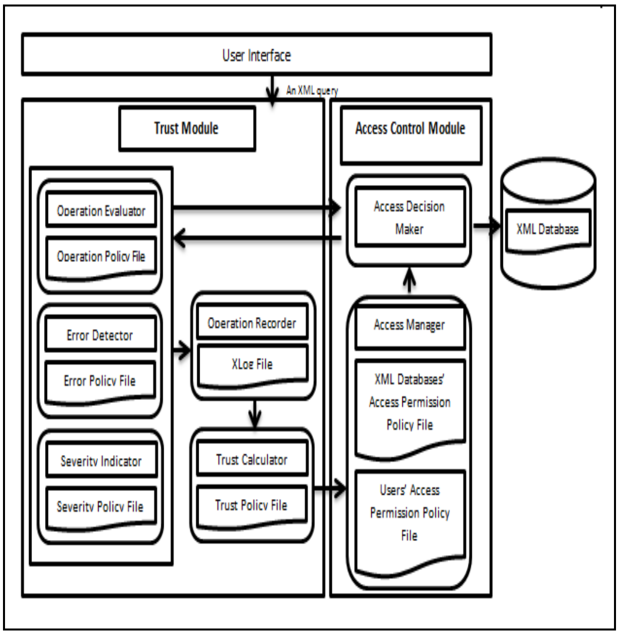

Fig. 2 Severity-aware trust-based access control's system architecture

C. Severity Indicator

We propose the Severity Indicator as part of the Trust Module in this work. The function of Severity Indicator is to initiate severity value for each bad transaction in user query. The process of indicating severities depends on the policy rules defined in the Severity Policy file. When user issue a transaction, the Severity Indicator will checks on the Severity Policy file to indicate severity value for the transaction. Like the Operation Evaluator and Error Detector, Severity Indicator cooperates with the Access Control Module through sharing the TV for users and data with the Access Decision Maker to indicate severity value for each transaction. When the severity already indicated, it will be comprised in the evaluation process for user behaviour since it reflects on the user trustworthiness when retrieving sensitive data. The Severity Policy file includes the policy rules of indicating severities as depicted in Figure 3.

Each of statement has different impact to the execution in database. For that reason, each transaction has different severity value. As an example, insider misuse using DELETE transaction can cause data missing or even database corruption. The Severity Policy file is a standard XML file that uses some specific tags to indicate severity for each transaction issued by user.

The root node is defined by <Severities>. Each severity is defined by <Severity> and all severities are classified by their identifier and type. The <ID> tag is used to identify each rule. The <Type> defines the rule and the <Value> defines the value of severity for each type of transaction. The structure of the Severity Policy file is described in Figure 3.

```
<Severities>
<Severity>
  <ID>1</ID>
  <Type> Read unauthorized node </Type>
  <Value>0</Value>
 </Severity>
 <Severity>
  <ID>2</ID>
  <Type> Write unauthorized node </Type>
  <Value>0.25</Value>
 </Severity>
 <Severity >
  <ID>3</ID>
  <Type> Delete unauthorized node </Type>
       <Value>0.50</Value>
 </Severity>
 <Severity>
  <ID>4</ID>
  <Type> Delete root node </Type>
       <Value>0.75</Value>
 </Severity >
 <Severity >
  <ID>4</ID>
       <Type> Delete parent node with existing
       Children </Type>
       <Value>1.00</Value>
 </Severity >
</Severities>
```

Fig. 3 Severity Policy File

IV. CONCLUSION

It is significant to tackle security problems in XML databases to reduce the insider threats. One of important factor that we had to consider when we talk about database security is the severity of each transaction. In this research, we indicate severity value for each bad transaction in order to improve security in XML database. In this work, we presented the implementation of severity factor to provide protection for XML database-centric Web services towards malicious insider. We develop a prototype tool that implement severity-aware in trust-based access control for preventing malicious XPath code in XML database stored procedure.

REFERENCES

1. Gertz M., Jajodia S. (2007). Handbook of database security. Berlin: Springer-Verlag.
2. Magklaras, G. B., Furnell, S. M., & Brooke, P. J. (2006). Towards an insider threat prediction specification language. Information management & computer security, 14(4), 361-381.
3. Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., & Gritzalis, D. (2010). An insider threat prediction model. In Trust, privacy and security in digital business (pp. 26-37). Springer Berlin Heidelberg..
4. Farooqi, N., & North, S. (2011). Trust-based access control for XML databases. 2011 International Conference for Internet Technology and Secured Transactions, (December), 764–765.
5. Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. C., & Hohimer, R. E. (2012). Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. In System Science (HICSS), 2012 45th Hawaii International Conference on (pp. 2392-2401). IEEE.
6. Brdiczka, O., Liu, J., Price, B., Shen, J., Patil, A., Chow, R., & Ducheneaut, N. (2012). Proactive insider threat detection through graph learning and psychological context. In Security and Privacy Workshops (SPW), 2012 IEEE Symposium on (pp. 142-149). IEEE.
7. Eldardiry H., Bart E., Liu J., Hanley J., Price B., Brdiczka O.(2013). Multi-Domain Information Fusion for Insider Threat Detection. SPW, 2013, 2013 IEEE CS Security and Privacy Workshops (SPW2013) pp. 45-51, doi:10.1109/SPW.2013.14.
8. Legg P. A., Buckley O., Goldsmith M., and Creese S. (2015). Caught in the act of an insider attack: Detection and assessment of insider threat," in Proc. IEEE Int. Symp. HST, Waltham, MA, USA, 2015, in press.
9. Hashem Y., Takabi H., GhasemiGol M., and Dantu R.(2015). Towards insider threat detection using psychophysiological signals. In Proc. of the 7th ACM CCS International Workshop on Managing Insider Security Threats (MIST'15), Denver, Colorado, US, pages 71–74. ACM, October 2015.
10. Verma, B., Kumar, S. & Sharma, P. (2012). A Novel Approach for Multi-Tier Security for Xml Based Documents. IOSR Journal of Computer Engineering (IOSRJCE), Volume 5, 1-4.
11. Zhu, H., Jin, R. & Lu, K. (2007). A Flexible Mandatory Access Control Policy for Xml Databases. The 2nd International Conference on Scalable Information Systems, Suzhou, China, 1366890: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 1-4.
12. Chagarlamudi M., Panda B. and Hu Y. (2009). Insider Threat in Database Systems: Preventing Malicious Users' Activities in Databases in 2009 Sixth International Conference on Information Technology: New Generations, ITNG '09, 2009, pp. 1616-1620.
13. Singh S., "Trust Based Authorization Framework for Grid Services. (2011). Journal of Emerging Trends in Computing and Information Sciences, vol. 2, pp. 136-144, 2011.
14. Lin A., Vullings E. and Dalziel J. (2006). A Trust-based Access Control Model for Virtual Organizations, in Fifth International Conference on Grid and Cooperative Computing Workshops, GCCW '06, 2006, pp. 557-564.
15. Zhao, L., Liu, S., Li, J. & Xu, H. (2010). A Dynamic Access Control Model Based on Trust. International Conference on Environmental Science and Information Application Technology (ESIAT), 548-551.
16. Tripathi, A., & Singh, U. K. (2013). Evaluation of severity index of vulnerability categories. International Journal of Information and Computer Security, 5(4), 275-289

AUTHORS PROFILE

Aziah Asmawi (Dr.)
D.Sc. (UPM), B.Sc. (UPM), M. Sc. In Database Security (UTM), Ph.D(UPM)
Expertise : Database Security, Cyber Security, Digital Forensic

Nur Izura Udzir (Assoc. Prof. Dr.)
B.Sc. (UPM), M. Sc. (UPM), Ph.D (York)
Expertise : Access Control, Intrusion Detection Systems, Computer Security, Coordination in Distributed Systems

Lilly Suriani Affendey (Assoc. Prof. Dr.)
B.Sc. (UPM), M.Sc. (Bradford), Ph.D (UPM)
Expertise : Database Systems, Multimedia Database, Content-based Video Retrieval

Ramlan Mahmod (Prof. Dr.)
B.Sc. (Western Michigan, University, U.S.A.), M. Sc. (Central Michigan, University, U.S.A.), Ph. D (Bradford University, UK)
Expertise : Security in Computing, Cryptography, Artificial Intelligent