











TABLE XIV  
ADMINISTRATOR AND USER ROLES: ACCESS SCHEMA

```
CREATE ROLE user_entry;
GRANT user_entry TO user_view;
...
GRANT ALL ON
transaction TO admin_view;
```

The software development methodology for the secure web application proposed in this paper provides a consistent analysis and design method for security, which is different from the existing OOAD methodology and provides correlation with Java EE and database, which UMLsec cannot provide, do. Accordingly, we proposed 'A software development methodology for a secure web application,' which is applied to the existing OOAD methodology, security, Java EE, and database.

We verified the efficacy of the proposed methodology by examples of the online banking system. Using authentication, we can prevent attacks that try to disguise an unauthorized user as an authorized user, like in Fig. 4. Using authorization, we can prevent one who tries to conceal one's grade, like in Fig. 5. Using confidentiality and data integrity, we can prevent one who tries to edit or eavesdrop important user information, like in Fig. 6.

<https://localhost:8080/mvc1board/admin/Member.jsp>

Account Information		
ID	Password	C
Guest1	Guest1	tc

Fig. 6 Customer management page

#### IV. CONCLUSIONS

This paper proposes an integrated software development methodology for a secure web application. To this end, security emphasized modeling language UMLsec and O-R mapping for relational database design is used. Also, to implement the analysis and design results of security, we implemented the role-based access control using DDL and DCL syntax of Java EE and SQL. Accordingly, the security application was reflected then a consistent method was to the entire system development cycle.

A software development methodology for a secure web application proposed in this paper provides a consistent analysis and design method for security that was not provided by existing OOAD methodology. Also, the association with Java EE and database that UMLsec does not provide is also provided through role-based access control.

Therefore, it is possible to securely and consistently analyze and design the pre-system development cycle by firmly presenting the existing OOAD methodology, security, then the correlation between Java EE and relational database. Our methodology is verified by applying it to the development of an online banking system.

#### ACKNOWLEDGMENT

The Soonchunhyang University Research Fund supported this research.

#### REFERENCES

- [1] Eduardo Fernandez-Medina, Juan Trujillo, Rodolfo Villarreal, and Mario Piattina, 2007, "Developing secure data warehouses with a UML extension," *Journal Information Systems archive*, Vol 32, No 6, pp. 826-856.
- [2] G.Popp, J. Jurjens, G.Wimmel, R. Breu., 2003, "Security-Critical System Development with Extended Use Case," *Asia-Pacific Software Engineering Conference*, 5-1 self.
- [3] Madan, s., 2010, "Security Standards Perspective to Fortify Web Database Applications From Code Injection Attacks," *International Conference on Intelligent Systems, Modelling and Simulation(ISMS)*, Vol. 10, pp. 226-230.
- [4] Iqra Basharat, Farooque Anam, Abdul Wahab Muzaffar., 2012, "Database Security and Encryption: A Survey Study," *International Journal of Computer Application*, Vol. 47, No. 12, pp28-34.
- [5] David Basin, Jürgen Doser, and Torsten Lodderstedt., 2006, "Model Driven Security: from UML Models to Access Control Infrastructures," *ACM Transactions on Software Engineering and Methodology (TOSEM)*, Vol. 15 No. 1, pp39-91.
- [6] Kyung-Soo Joo, Jung-Woong Woo., 2012, "A Development of the Unified Object-Oriented Analysis and Design Methodology for Security-Critical Web Application Based on Object-Relational Database -Focusing on Oracle 11g-", *Korea Society of Internet Information*, Vol 17, No 12, pp. 169-177.
- [7] Byeong-Seon Jeon., 2005, *CBD WHAT&HOW*, Wowbooks Publishing Company, Seoul.
- [8] Heung-Seok Chae., 2009, *Object-oriented CDB Project for UML and Java as learning*, Hanbit Media. Seoul.
- [9] Mang Su, Fenghua Li, Guozhen Shi, and Li Li, "An Action-Based Access Control Model for Multi-level Security," *IJSIA*, 6, pp. 359-366 (2012).
- [10] Allaoua Maamir, Abdelaziz Fellah, Lina A. Salem, "Fine Granularity Access Rights for Information Flow Control in Object-Oriented Systems," *IJSIA*, 2, pp. 81-92 (2008).
- [11] Brett D. McLaughlin, Gary Pollice, David West., 2007, *Head First Object-Oriented Analysis & Design*, habit media, Seoul.
- [12] Seung-Yun Bang, Kyung-Soo Joo., 2003, "Design Methodology for XML Schema Application based on UML," *Soonchunhyang Univ*, pp.71-75.
- [13] Mang Su, Fenghua Li, Guozhen Shi, Li Li., "An Action-Based Access Control Model for Multi-level Security.," *International Journal of Security and Its Applications*, 6(2), 359-366. 2012
- [14] Egbunike, Celestine, and S. Rajendran. "The implementation of the negative database as a security technique on a generic database system.," *Circuit, Power and Computing Technologies (ICCPCT), 2017 International Conference on. IEEE*, 2017.