ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Survey on Authentication and Authorization for User Roles and Attack Detection in Relational Data

Aditi V. Bhadke[1], Jyoti Raghatwan[2]

M.E., Dept. of Computer, RMD Sinhgad School of Engineering, Pune, India[1]

Assistant Professor, Dept. of Computer, RMD Sinhgad School of Engineering, Pune, India[2]

ABSTRACT: Information security is concerned for cyber attack, malicious. Information sharing in social media has lost privacy of relational data like social application, relational database, and smart services. Also, there are number of users with smart devices and equipment, including officials, students and people, data administrator etc., these user personnel different services on smart devices like smart grid devices group of internet users for accessing social services. Also database administrator services for accessing application database, Relational database are used to access and modify and remove data from by personnel like DBA. Thus proposed technique implements secure approach to limits different insider and outsider attack to use personnel information. These novel approaches present the method for user policy based service. Digital signature based security is provided for access control for relational database.

KEYWORDS: Insider Attacks, Anomaly Detection, Application Profile, SQL Injection, digital signature, K-Admin etc

I. INTRODUCTION

Relational database is wide application storage for their information like personal information; data files. There is inadequate security for user information storage. Multiuser access for relational database services like oracle, mysql etc there are many personnel used to perform operation like insert, update, and delete over relational database. Due to enormous storage of relational databases attack includes insider and outsider attack over data and resources. SQL injection, XSS attack these are zombie may create serious threat to application and database server.

Proposed technique provides a two-factor authentication. First the authentication is performed for each user as well as the device with unique identity in a batch with the signature authentication of every device at the server of the substation. Next to that, a Onetime password (OTP) is sent to the user's device or phone to verify the actual user who is accessing the device. Proposed system also shares for dealing with physical and remote access for resources like smart grid. These smart devices are more vulnerable to threaten for system.

Existing system implement symmetric key based security over smart grid network [7]. But, if a shared key is compromised, it can reveal the confidential information to the intruders. Further, an attacker can't separate any data based on connection capacity among various smart devices, as these devices store hash values relating to every user role. For every device, these values are varying for every user role.

This technique beat various outsider attacks and in addition insider attacks, incorporating man-in-the-middle attacks, replay attacks, impersonation assaults, integrity violation, attacks by client or user of the framework, known key attacks, and repudiation attacks. Proposed work avoids insider attacks where (i) a user accesses the resource with the identity of other user without advising him/her, and (ii) a maverick device is installed by a legitimate engineer in the system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

II. RELATED WORK

It includes the brief overview of existing work of various techniques used for authentication and authorization of different users and devices:

In [1], the original user is accessing information made by the correct device at the expected area at the best possible time, communicated by utilizing the expected protocol, and the information hasn't been changed. Many individuals demonstrate the grid's control frameworks as working in a situation of certain trust, which has affected design decisions. In the event that a few members aren't trustfulness, new techniques of addressing to these past existing monitoring methodologies may be required.

In [2], system proposes a novel authentication scheme that employs the Merkle hash tree technique to secure smart gird communication. Particularly, the proposed authentication technique considers the smart meters with calculation obliged attacks and puts the less calculation overhead on them. Comprehensive security examination demonstrates its security quality, to be specific, flexibility to the replay attack, the message injection attack, the message investigation attack, and the message change attack.

In [3], Outsider attacks give a genuine danger to grid operations on specific interest are sparse attacks that include the compromise of a moderate number of meter readings. A productive algorithm to locate all unremarkable attacks including the trade off of precisely two power injection meters and a arbitrary number of power meters on lines is displayed. This requires flops for a power framework with buses and line meters. In the event that all lines are metered, there exist accepted structures that describe every one of the 3, 4, and 5-sparseun perceptible attacks.

In [4], proposed work presents new approach, secure, and versatile M2M information collection protocol for the Smart Grid. Framework utilizes a hierarchical approach with delegate hubs gathering and relaying the information safely from measurement devices back to the power administrator. While the information collectors verify the integrity, they are not offered access to the content, which may likewise make ready for outsider suppliers to convey esteem included administrations or even the information accumulation itself.

In [5], proposed a completely useful character based encryption technique (IBE). The technique has picked Cipher content text security in the arbitrary oracle model accepting a variation of the computational Diffe-Hellman issue. The framework depends on bilinear maps between groups. The Weil pairing on elliptic curves is a case of such a map. Later give exact definitions for secure identity based encryption techniques and give a few applications for such frameworks.

With the rationale all open - and shared key primitives are formalized furthermore the idea of a fresh message. This makes it conceivable to formalize a challenge response protocol. BAN logic is implied for thinking over cryptographic protocols. Confirmation with BAN logic does not really infer that no attacks on the protocol are conceivable. A proof with the BAN logic was a decent confirmation of accuracy, based on the assumptions. Be that as it may, inquiries may emerge over the semantics of the logic and the logic excludes conceivable attacks [6].

The problem arises in earlier system is overcome in next generation. The examination of the proposed protocol indicates that the protocol can prevent different attacks. The transmission of symmetric key to the remote users is productively handled by the protocol. Here’s the concept of OTP which is send on users mobile phone(mobno) is used but it has poor communication overhead and computation overhead. In our system all the problems will be recovered and defeat all the insider and outsider attacks and improve the efficiency of communication overhead and computation overhead. In existed system a user authentication and authorization technique for accessing a wide range of sorts of devices in the SG [8]. This technique can be effortlessly applied to various user-roles, for example, auditors, researcher, and so forth., who access various devices in the SG framework, as every user-role is processed progressively in light of attribute based access control. This scheme empowers two-factor authentication so that a rouge device couldn't re-utilize the previous caught data of a legitimate user. A bilinear pairing cryptography-based shared secrete key is created between the user and the device for further secure communication during a session. The proposed scheme is effective as far as both, communication and calculation overheads in comparison with the existing techniques and can crush some notable outsider attacks and additionally insider attacks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

III. PROPOSED ALGORITHM

A. *DESIGN CONSIDERATIONS:*

- Initially user to user connected network is considered.
- Users as Hop count is measured in terms of path between multiple users.
- Keeping track of users mutually connected in paths.
- Considered all possible paths at beginning.
- Assigning policy to user and resources(device) for online security
- The time when no way is accessible to transmit the packet is considered as the system lifetime.

B. *DESCRIPTION OF THE PROPOSED ALGORITHM:*

Proposed algorithm specifies how the access evaluation procedure works. When an accessing user a requests an action against target user t, the system will look up user a action policy, user t action policy and the system specified policy corresponding to action. When user a requests an action against a resource t, the system will retrieve all the corresponding policies of rt. Although every user can just determine one approach for every activity per target, there may be numerous users indicating strategies for a same pair of activity and target. Multiple policies might be collected in each of the three policy sets: AUP, TUP/TRP and SP.

IV. PSEUDO CODE

Algorithm1. User action Authentication (user $_a$, action, target)
Step 1: (User Policy Assignment)
Step 2: if target ==u_t then
AUP is user a policy for action,
TUP is user t policy for action,
SP system's policy for action
Step 3: else
AUP is user a policy for action,
TRP is resource t policy for action,
SP is system's policy for action,
(resource.typename, resource.typevalue)
Step 4: (User Policy authentication)
Step 5: for all policy in AUP, TUP/TRP and SP do
Generate graph models (start, path rule) from policy
Step 6: for all graph model extracted do
Step 7: Determine the starting node, specified by start, where the path evaluation starts
Step 8: Determine the evaluating node which is the other user involved in access
Step 9: Extract path rules path rule from graph rule
Step 10: Find every path spec path, hop count from path rule
Step 11: Path-check each path spec using Algorithm 2
Step 12: Check combined result based on conjunctive or disjunctive connecting path specs and negation on individual path nodes.
Step 13: Collect final result from the result of each policy.

Algorithm 2. DFSPathChecker(Graph, path, hopcount, starting node, evaluating node)

1: Calculate DFA from given path where path is in the RE (Regular expression) form.
2: by looking the history of state, DFA starts at the initial state
3: check if hopcount is not equal to zero, if true then
4: return to the starting node

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

V. PROPOSED SYSTEM

The proposed system present secure and efficient mutual authentication and authorization methods are required in the smart devices to prevent different insider and outsider attacks on many different devices. This work propose an authentication and authorization scheme for reducing outsider and insider threats the user authorization and performing the user authentication together whenever a user accesses the devices. This strategy considers user-roles dynamically utilizing attribute based get to control and confirms the personality of user together with the resource. User device security and framework performance analysis represent that the proposed techniques keeps away from different insider and also outsider attacks, and is more effective regarding communication and calculation costs in comparison with the existing techniques. The accuracy of the proposed scheme is also defined by using BAN-Logic and Proverif mechanism.

1. User to User relationship:

In social media network manage security by user to user relationship for implementing user relation based access control.

2. Access Mode based attack detection:

This approach is based the examination and profiling of the application in context to make a brief representation of its communication with the database. Such a profile keeps a mark for each submitted query furthermore the significant constraints that the application program must finish to submit the query. After that, in the discovery stage, at whatever point the application issues a query, a module catches the query before it finds the database and checks the relating signature and constraints against the existing setting of the application. If there is a mismatch, the query is marked as anomalous.

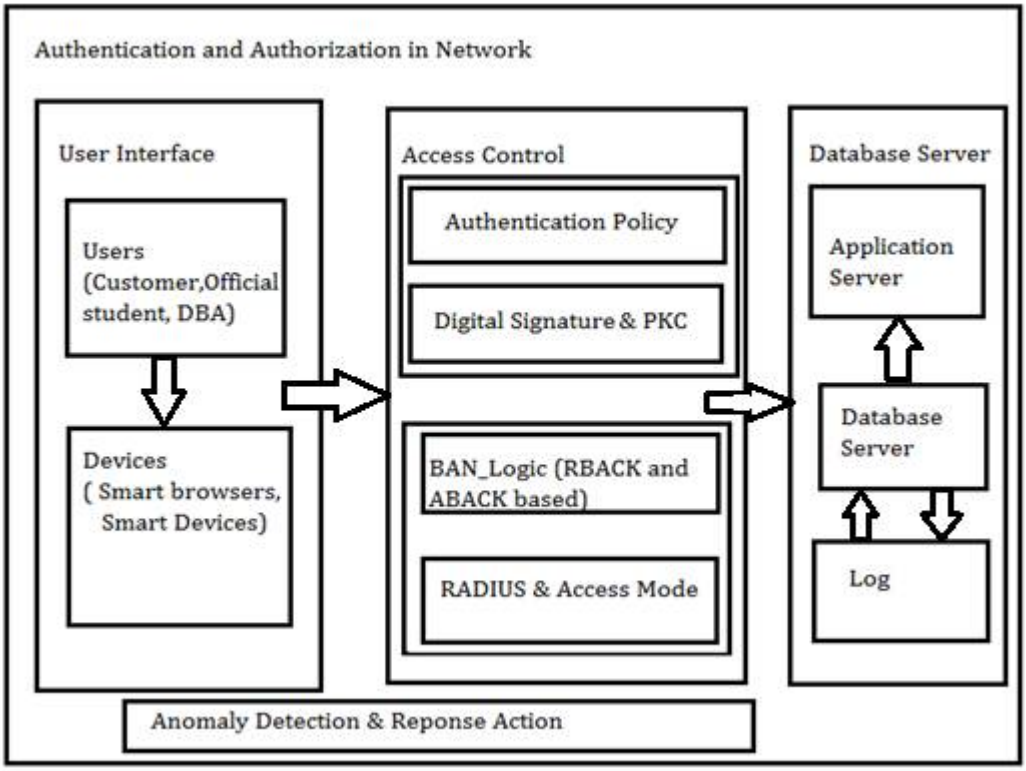

Fig.1:- Proposed System Architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

3. Policy based authentication:

In this approach user policy is used for access control authentication at database server and application server. It helps in authorization to user access by access policy.

4. User role based administrative action:

Multi admin user authentication scheme is designed for user role policy used at service provider.

VI. CONCLUSION AND FUTURE WORK

Online social network authentication and authorization by analysis of user to user relationship, proposed scheme has applied to different user-roles, such as users and devices etc., which access different devices in the communication media. Every user-role is assigned dynamically based on attribute-based access control using different access policy with (mode of access, department, location, access behaviour, device for using system) attributes provided by each user and attributes retrieved by system diagnosing. Proposed system enables two-factor authentication so that a device could not re-use the previous captured information of a legitimate user. We use pairing cryptography based shared secret key is generated between the user and the device for further secure communications within a session. Proposed system ensures the user integrity by digital signature generation at time of user registration and device registration. These credentials are authenticated at proxy server, which works as authentication server for user role assignment and authorization.

REFERENCES

[1] H. Khurana and M. Hadley, "Smart-grid security issues," IEEE Security & Privacy Magazine, vol. 8, no. 1, pp. 81-85, Feb. 2010.
[2] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient merkletree- based authentication scheme for smart grid," IEEE Systems Journal, vol. 8, no. 2, pp. 655-662, May 2014.
[3] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," IEEE Transactions on Smart Grid, vol. 4, no. 3, pp. 1244-1253, Sep. 2013.
[4] R. Tabassum, K. Nahrstedt, E. Rogers, and K. S. Lui, "SCAPACH: scalable password-changing protocol for smart grid device authentication," in Proc. ICCCN, Nassau, Bahamas, pp. 1-5., Aug. 2013
[5] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in Proc. CRYPTO, S.B., USA, pp. 213-229, Aug. 2001
[6] J. Wessels, "Applications of BAN-logic," CMG Finance B.V.. [Online]. win.tue.nl/ipa/archive/springdays2001/banwessels.pdf. , 2001
[7]H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient authentication and key management mechanisms for smart grid communication," IEEE Systems Journal, vol. 8, no. 2, pp. 629-640, Jun. 2014.
[8]N. Saxena and B. J. Choi, "State of the art authentication, access control, and secure integration in smart grid," Energies, vol. 8, pp. 11883-11915, Oct. 2015.