Chapter 17

Automated Detection of SQL Injection Attack on Blockchain-Based Database

Keshav Sinha
https://orcid.org/0000-0003-1053-3911
Birla Institute of Technology, India

Amit Kumar Keshari
Birla Institute of Technology, India

ABSTRACT

In the era of computing, where the data are stored in a cloud or distributed environment, the privacy of data is one of the challenging tasks. The attacks like denial of service attacks (DoS), insider attack compromised the security of the system. In this chapter, the authors discussed a blockchain-based database, where data are encrypted and stored. The Web API is used as an interface for the storage and sharing of data in the blockchain system. There are several types of attacks that are performed by the adversary on the database to destroy the vulnerability of the system. Here, the authors are mainly focused on the SQL injection attack which is performed by the adversary on Web API. To cope with this problem, they present the case study based on the Snort and Moloch for automated detection of SQL attack, network analysis, and testing of the system.

INTRODUCTION

Blockchain has become one of the significant technologies in the field of IT industry. From the last few decades, blockchain came to the headlines, for the success of crypto-currency and smart contracts technology. After that many companies adopt the blockchain technology for their products. The blockchain technology is started in the year 1991, where the trusted time-stamping protocol is used for data privacy (Haber, 1991). Later on in the year 1992, the Merkle tree is proposed for storing the multiple data in the single block (Bayer, 1992). After that researchers are not given much focused to evolve the technology
because of the emergence of a centralized system. There are various research has been down in the field blockchain in the different time frames which is shown in Figure 1.

*Figure 1. The Various Development in the Field of Blockchain at Different Time Frame*

---

**Blockchain Safety and Security**

The blockchain technology is based on the public ledger, where the data are stored at several nodes for transmission. There are various security principles and features of the blockchain system such as:

1. **Decentralization:** There is no single point failure present in the blockchain system because the nodes are distributed across the internet and all transactions over the network can be seen by all the nodes.
2. **Confidentiality:** The public key cryptography is used to identify the authentic users, and provide the secure transmission of the data over the internet.
3. **Integrity:** The blockchain technology is based on the concept of time-stamped, where every data is signed with unique time, and any nodes can easily trace and validate the transaction.
4. **Transparency:** In the blockchain system the unique agreement is signed by the nodes and the network before the transmission of data.
5. **Immutability:** The blockchain is the concept of the block, where the data ones added to the network will not we destroyed or modified.

The blockchain systems are operated by public ledger, where every node has access to the network data. Any transaction that has occurred on the network is reviewed and validated by the different node members. This creates the data transparency and it is not possible to alter the ledger without seeing by any actor within the system network. This concluded that the blockchain systems are resisted against any type of attack. Based on the theory there are no virtual attacks that are possible to the blockchain system. But in the year 2017, there is 10 percent of attacks are executed on the blockchain system (Passeri, 2017).
19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/automated-detection-of-sql-injection-attack-on-blockchain-based-database/272320

Related Content

Sustainable Information Development Practices and Societal Transformation in Kenya
www.irma-international.org/article/sustainable-information-development-practices-and-societal-transformation-in-kenya/279832

Adoption of Open Source Software in Libraries in Developing Countries
www.irma-international.org/article/adoption-of-open-source-software-in-libraries-in-developing-countries/198401

Predictors of Undergraduate Satisfaction With the Usage of University of Ilorin Web Portal

The 21st Century Library and Information Services for the Enhancement of Teacher Education
www.irma-international.org/chapter/the-21st-century-library-and-information-services-for-the-enhancement-of-teacher-education/191555

One Year Forward: The 2013 Update to the E-Readers and E-Books in Public Libraries Survey
www.irma-international.org/chapter/one-year-forward/191560