International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Enhancing Security and Privacy in Web Services using Blockchain

Nagendra Kumar Singh[a], *Santosh Kumar*[b]

[a]*Assistant Professor, Department of Computer Science, Era University, Lucknow*
[b] *Professor, Department of Computer Science, Era University, Lucknow*

ABSTRACT

Blockchain has emerged as an innovatory technology of this neoteric age which is having a colossal impact on the modern society for its transparency, decentralization and security properties. The first application of Blockchain was done by the cryptocurrency Bitcoin and that is why this technology has attracted a lot of attention in a very short span of time. This paper presents research on the use of Blockchain technology in strengthening trust, privacy, and security in Web services environment. In this paper, the Web services and Blockchain technology are formally defined and reviewed the existing literature based on these requirements. Finally, the role of Blockchain technology in enhancing trust, privacy, confidentiality, and security in Web services is analyzed.

Keywords: Blockchain, Web Services, Security, Privacy, Trust.

1. Introduction

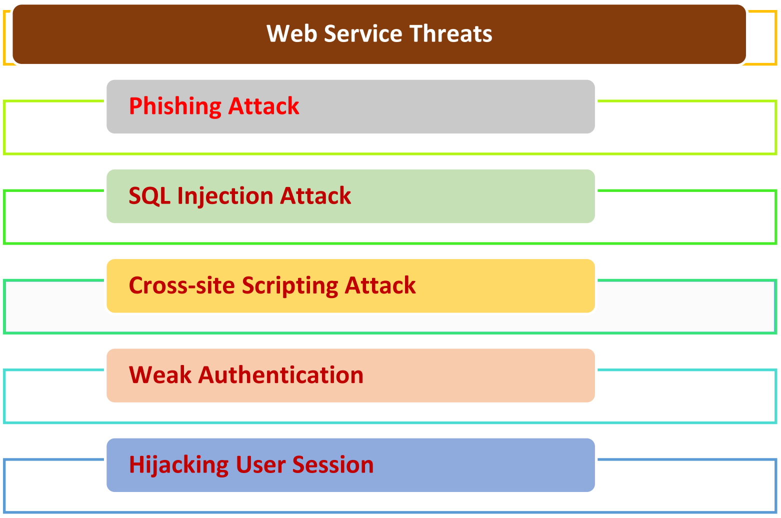
The expansion of internet services has made most of the services available online, due to which a person has been able to avail countless services like banking, education, shopping, bill payment, government services etc. sitting at home. Web services have emerged as a new generation of Web applications that are self-contained, self-describing, and modular, and can be published, located, and invoked across the Web [1]. Web services are developing very fast and are witnessing exponential growth [2]. The browser is used as a gateway to web services to interact with various critical service systems to access web services. Web services store huge amounts of multimodal data in the backend database, which includes information from social, commercial and personal areas. To avail the benefits of web services, a person has to share his personal and confidential information with the web service provider, in which there is a risk of unauthorized use of the information. Reducing the privacy risks in web services will greatly facilitate their dissemination.

At the same time, Blockchain is an emerging technology of today's time which has made a strong place for itself. Blockchain technology is a technology based on crypto currency, most notably Bitcoin [3]. Bitcoin uses the Blockchain as a way to solve the long-standing problem of double spending as digital cash and a decentralized approach to digital transaction processing without the need for any trusted third parties. Blockchain is defined as an open distributed ledger in which blocks of data are linked to each other as a chain of blocks. Initially Blockchain technology was used only to store transactions of digital currencies, but now it is being used in other applications beyond currency and payments [4].

One of the main benefits of Blockchain technology is its ability to provide a secure and transparent platform for record keeping. Transactions are recorded in a decentralized network, making it difficult for hackers to alter or tamper with the data. One of the main benefits of Blockchain technology is its ability to provide a secure and transparent platform for record keeping. Transactions in a Blockchain network are recorded in a decentralized network, making it difficult for hackers to alter or tamper with the data. This paper analyzes how Blockchain technology features can be used to secure web services. The paper has been drafted as follows. Section 2 provides detailed information about security threats to web services. In section 3, the role of Blockchain to counter them is analyzed. Finally, conclusions are given in Section 4.

2. Security Threats in Web Services

While the expansion of web services has proved to be a milestone in providing easy access to various services to the common people, it has also exposed serious security threats. Security threats to web services are primarily a form of Internet-borne cybersecurity menace that can harm users online and cause unsolicited actions or events [5]. Security threats to web services are constantly emerging and evolving exponentially day by day. Some of the common security threats to Web services are [6]:



2.1 Phishing Attack

Phishing attack is a form of online social networking attack that extracts user's cryptic information along with their login information such as id and password.

2.2 SQL Injection Attack

SQL injection is a web security threat in which external attackers attempt to steal confidential information of a web service user by exploiting vulnerabilities in the application code.

2.3 Cross-site Scripting Attack

This attack allows malicious intruders to execute scripts in the client's browser, which can destroy users' sessions, deface web sites, or redirect users to malicious sites.

2.4 Weak Authentication

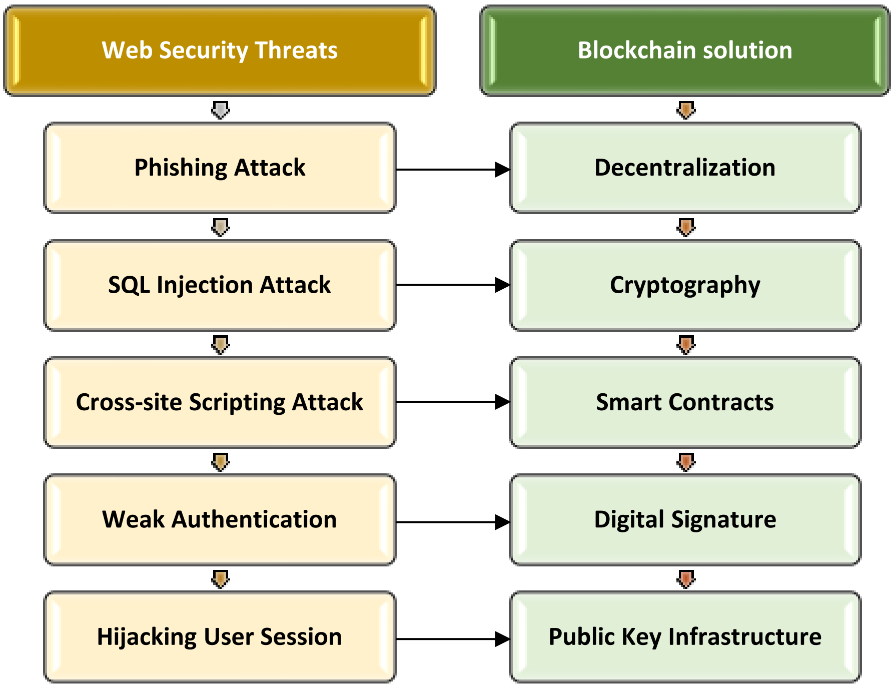
Weak authentication may allow intruders to steal passwords, or exploit other vulnerabilities to discover a user's identity.

2.5 Hijacking User Session

An intruder attacks a web server to take over it and then collects information available on all legitimate user sessions.

3. Role of Blockchain in Web Service Security

Blockchain can prove to be a milestone in enhancing web security as it uses a shared and immutable ledger that can only be accessed by permitted members. Blockchain can be used to mitigate the Web security threat following manner.



Above diagram shows that how blockchain solution can improve the Web services by mitigating various security threats. We can use decentralization mechanism of Blockchain to tackle phishing attack. Similarly, we can apply cryptography to address SQL injection attack. Smart contracts can be applied to handle cross-site scripting attack. The major problem with Web services is that how to secure the authentication process. So, digital signatures can be applied to secure the authentication process. Public key infrastructure will be recommended to secure user session.

4. Conclusion

First, a brief introduction to web services and block chain technology is provided. Next, the main web security threats are identified and defined. Finally, an attempt has been made to draw a blueprint of how web security threats can be addressed with the help of Blockchain. In this research, it has been found that if Blockchain technology is used in web services, then the security related concerns in web services can be resolved in a very concrete way. In the future, we hope that we will try to create a framework using web services and blockchain technology that can play a very important role in securing web services.

References

1. N. Dara and S. Emadi, "Enriching Web Services Tags to Improve Data-Driven Web Services Composition," in Journal of Web Engineering, vol. 20, no. 2, pp. 327-358, March 2021, doi: 10.13052/jwe1540-9589.2025.

2. L. Hui, H. Xudong, G. Fan, W. KaiLun and Y. Enze, "Web Service Access Control Based on Browser Fingerprint Detection," in Journal of Web Engineering, vol. 20, no. 5, pp. 1587-1622, July 2021, doi: 10.13052/jwe1540-9589.20512.

3. Bhutta, M.N.M., Khwaja, A.A., Nadeem, A., Ahmad, H.F., Khan, M.K., Hanif, M.A., Song, H., Alshamari, M. and Cao, Y., 2021. A survey on blockchain technology: Evolution, architecture and security. Ieee Access, 9, pp.61048-61073.

4.M. Swan, Blockchain, Blueprint for a New Economy. Sebastopol, CA, USA: O'Reilly Media, 2015.

5.Y. Zhang and T. Zhang, "Research Into the Security Threat of Web Application," in Journal of Web Engineering, vol. 21, no. 5, pp. 1707-1726, July 2022, doi: 10.13052/jwe1540-9589.21514.

6. Canfora, Gerardo, and Corrado Aaron Visaggio. "A set of features to detect web security threats." Journal of Computer Virology and Hacking Techniques 12 (2016): 243-261.