Enhancing Security of Data Exchange through Block Chain Technology

Jeevankumari Chevula, Aruna Varanasi

Abstract: ***Cyber security refers to a set of well-defined techniques used to protect the integrity of networks. It is used to protect vital data of customers and to restrict unauthorised access. In the era of E-Commerce, the demand for websites, web application increasing exponentially day by day. Web security is currently a significant issue for Internet enabled organization. Using websites, managing information through digital way. HTTP is a Hyper Text Transfer Protocol. It is used to transfer information over the internet. HTTP is most popular protocol widely used in web applications and allowed by internet firewalls, operating systems. HTTP is an unsecured information exchange protocol. Integrity is not there, so someone can easily alter with the content. In the internet data transferring over HTTP connection in plain text, this opening new loop hole to attackers to read every data sent over HTTP connection to web or webserver. Http is insecure as there is no encryption methods for it. So, it subjected towards the web attacks such as Man in the middle, cross site scripting, SQL Injection, click jacking, Broken authentication and session management attacks can occur. HTTP interaction with TCP is bad, causes the problems with performances and server scalability. In our proposed system, document which is used by more than one user and if there is in updation of the content user who is modifying the content of thier shared document must take their concern from other users. The process which is being used to authenticate the modifications of content of shared document is done with the help of shared key unless or until all users send the shared keys of each user the document will not be decrypted and hence further the changes in the document will not be possible.***

Keywords **: *HTTP, Blockchain Technology, Security.***

I. INTRODUCTION

The Hypertext Transfer Protocol (HTTP) is a networking protocol for clients, collaborative-services, hypermedia data systems. HTTP has started and used by people since 1990. To provide security over HTTP for communication is big challenge to in network security protocols Because HTTP has high usage in the internet. The development of HTTP traffic likewise pushes foundation suppliers to extend their HTTP impression, making a positive criticism circle and quickening HTTP traffic development.

Revised Manuscript Received on March 17, 2020.
***** Correspondence Author
Jeevankumari Chevula, Department of Computer Science and Engineering , Sreenidhi Institute of Science and Technology, Yamnampet, Ghatkesar, Hyderabad, India. Email: jeevankumari.ch@gmail.com
Dr.Aruna Varanasi, Professor & HOD Department of Computer Science and Engineering , Sreenidhi Institute of Science and Technology, Yamnampet, Ghatkesar, Hyderabad, India. Email: arunavaranasi@sreenidhi.edu.in

Taking this pattern to its obvious end result, it has been contended that HTTP has become the "thin midsection" of the Internet, as most by far of traffic runs over HTTP rather than straightforwardly over IP. Usage of HTTP is becoming more and more every day because present generation people are living in internet only. So to security have to improve more and more to secure the users. HTTP an intuitive instrument called HTTP Explorer was created. The device permits to explore different avenues regarding HTTP utilizing any web-server associated with the web. It makes the information flow between a customer and a server totally obvious. Contrasted with a HTTP-Simulator utilizing a usage which is completely consistent with HTTP. The Hypertext Transfer Protocol is an application-level protocol with the lightness and speed necessary for distributed, collaborative, hypermedia information system. HTTP headers are the code that moves information between a webserver and a program. It is a conventional, stateless, object-situated convention which can be utilized for some assignments, for example, name servers and disseminated object the executives frameworks, through expansion of its solicitation strategies. HTTP headers are for the most part intended for the correspondence between the server and customer. HTTP demand header contains data in a book record structure, which incorporates specifics, for example, the sort, abilities and rendition of the program that creates the solicitation, the working frameworks utilized by the customer ,the page was mentioned ,the different kinds of yields acknowledged by the program, etc. HTTP reactions Header will get the solicitation header; the web server will send a HTTP reaction headers back to customer. A HTTP reaction header remembers data for a book record structure from that an internet browser transmits back to the customer's program. The reaction header contains points of interest, for example, the sort, date and size of the document sent back by the server, just as data in regards to the server.HTTP is designed to communicate between user and web browser. It enables better services to client and server. In Http/1.1 system has to keep in on state because association could reuse the connection for establishment. With this users no need to re-establish the connection with server or website this can save lots of time to users or servers. While establishing the connection with server HTTP uses TCP handshakes with clients. http does different types of verification to check weather user is valid or not. HTTP always comes with different types of verifications to find correct user for data transferring between client and server. HTTP performs different strategies to show on ideal activities on connected services for better security purpose.

Some times documents can be executable in the server so to protect remaining users data or connections it will check the security aspects according to security tests. Blockchain technology is used to record transactions in the world wide because it works as blocks wise so if any person wants to change information in it then the person has to change information in all blocks, so it becomes impossible to attacker to change information in blockchain technology. Every block holds lot of security information regarding keys and exchanging of blocks and sequence of blocks and hash's. every block contains previous block information when they are taking long time to process the chain then it will goes back to genius block or it creates new block to process the chain very fast.

II. EXISTING WORK

A.Simple and Lightweight HTTPS Enforcement to Protect Against SSL Striping Attack

HTTPS networks are weak against for man in the middle attacks. The man in the middle attack technique works as hijacking the networks in the HTTPS or network protocols and changes information between client and user. They both doesn't know what's going on in between them but attacker can change information in between them. Web browsers uses java scripts to check the network certificates like SSL and etc., if they don't find any certificates then it send some error message to user and some times it will users site while browsing. When server gave replay to users request then attacker starts to communication in between user and client and server because server doesn't know about the attacker but it thinks as user only. The aggressor arranges the MITM attack and uses the SSL Sniff system to deliver a self-stamped statement with the verification information of server, and sends to the individual being referred to. For each message of the client sending to the web server, the attacker can without quite a bit of a stretch unscramble it. right when the site is ambushed by SSL Strip, the client can't check the show in correspondence. HTTPS affiliations can be undermined and a short time later wrecking security on web applications. In particular, the SSL Stripping framework can ambush HTTPS with no disturbing messages at both web programs and web servers. Verification is for distinguishing perfect individual for loggings. It will be in various sorts to recognizing the perfect individual with safety efforts.

B. Packets tokenization methods for web layer cyber security

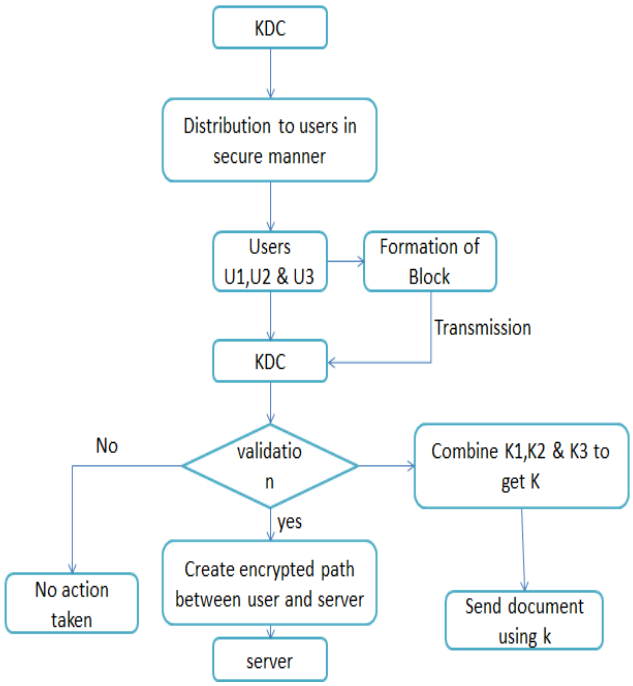
The authors RAFAL KOZIK and MICHAL CHORAs Proposed multiple HTTP sequence clustering algorithm combined with the machine-learnt classifier. It is used to detect anomalous behavior of connections established between client and server. Present security is based on signature-based category of cyber-attacks detection methods which are IPS and IDS. If they have signature then only they can find the attack else they can't find new attacks. Generally these two are used to increase the security levels through networks. WEB APPLICATION FIREWALL also used for web security levels. But finally we can't who are real once because present days people are using VPN's so it's almost waste of time taking process.

C.Analysis of the adoption of security headers in HTTP

Now a days attacking on website or web is getting higher and higher with new techniques. To provide better security to users , we have to approach new methods to avoid risks with attackers. SSL and transport layer security (TLS) completely guaranteed the substance of the message exchange, the extension of CSP – content security approach – [6] coordinates an arrangement language that sets content limitations on a web asset, and where the server transmits the strategy to the customer, for it to uphold the arrangement. The examining of the Alexa destinations is an all around characterized technique for understanding the changing idea of the solicitation, for example, in the ever-changing conduct of HTTP site pages.

HTTP is not an Secured protocol. To enhance the security during data exchange process through HTTP using client side encryption method by performing data encryption process at application level on web browser side. A Cryptographic algorithm was introduced for securing the data is an Advance Encryption Standard dynamic key 128 bits. The AES has balance between security and flexibility in various software and hardware.

III. DESIGN & MYTHOLOGY



IV. PROPOSED SYSTEM

Proposing blockchain technology with HTTP(Hyper Text Transfer Protocol) which makes more secure. In this technology, process will be in chain system. Process will works based on blocks with persons, every block contains one person to exchange of keys. The proposed work consists of three block with three people. When three people are in active then only it will progress the work because people will share keys to each other, when one person is not in active

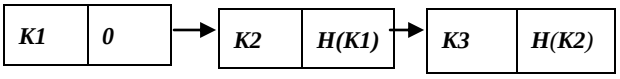
then process will be terminated. Keys will be sharing from first person to second person, second to third person, from third person data exchange will be start in blockchain. For better security used RSA256 bit encryption which makes impossible to break the chains. Encryptions will starts from the user itself only to prevent from then attacks. For authentication of users used SHA256 Hash to provide more security to users. With this method users will get more security levels when they are doing any transactions with HTTP because every person can't buy SSL certificate for their security purpose. In the proposed system whenever it detects any suspicious then blocks with jumps from one to last or another block and checks for the hashes for security, if any mismatch occurs then it will terminate the process.

A. Equations

Equations for exchange of keys

C1 = Eku1 (ks) || Eks (k1)
C1 = Eku2 (ks) || Eks (k2)
C3 = Eku3 (ks) || Eks (k3)

K1 = Dkr1 (Eku1 (ks1))
K2 = Dkr2 (Eku2 (ks2))
K3 = Dkr3 (Eku3 (ks3))



$$K = k1 \parallel k2 \parallel k3$$

U1 = 0
U2 = H (k1)
U3 = H (k2)
Where || = Concatenation

V. RESULTS

Login users

```
Enter Login ID:user1
Enter password: admin
user1
Login success
Enter Login ID:user2
Enter password: admin
user2
Login success
Enter Login ID:user3
Enter password: admin
user3
Login success
```

Login Fails

```
Enter Login ID:user1
Enter password: admin
user1
Login success
Enter Login ID:user2
Enter password: admin
user2
Login success
Enter Login ID:user3
Enter password: user
user3
Login Fail

Process finished with exit code 0
```

Transactions of amount using blockchain by exchanging keys from one user to another

```
enter your amount: 10
enter your amount: 20
enter your amount: 30
[[[1], 10.0], [[1], 10.0], 20.0], [[[[1], 10.0], 20.0], 30.0]]
```

Transferring files using client side encryption

```
Operation (encrypt, decrypt, exit): encrypt
Input file name: text.txt
Output file name: text.encrypted
Encryption completed
Operation (encrypt, decrypt, exit): decrypt
Input file name: text.encrypted
Output file name: text.txt
Decryption completed
Operation (encrypt, decrypt, exit): exit
```

Once application is started hankshaks with http then it will create key.key file which holds key in it. For sample eg: **"v36rmDgL8H4nZEMoiYgwKvz9csgE_wMk5mn-nomOC7M=”** the text in the bold is key to share files between users. It will change for every users

VI. CONCLUSION

Computer security, cyber security or information technologies are used to provide security to networks from the malicious persons or attackers, to protect hardware and software. Proposed system gives far better security for users. It successfully implemented and providing good security for users data exchange process. Because data is exchanging in chain propose but at the end user data with will be as per userdata only. With the blockchain technology in HTTP, users can exchange data in very secure way without any doubt while sharing their personal information. It is impossible to break security system because data is in RSA256 bit encryptions and authentication is in SHA256 bit encryptions which makes very hard to break security of HTTP in online. Proposed method have been successfully implemented in secure way. With the proposed system every one no need to use of SSL certificate. small industries are not able to buy SSL for their website's. with this method people no need to bother while share the information by using HTTP.

REFERENCES

1. Somnuk Puangpronpitag ,Nattavut Sriwiboon,"Simple and Light weigh HTTPS Enforcement to protect against SSL Stripping Attack" https://ieeexplore.ieee.org/document/6274346
2. Rafal Kozik, Michal Choras, Witold Holubowicz, "Packet Tokenization method for Web layer cyber security" https://ieeexplore.ieee.org/abstract/document/8142532
3. William J. Buchanan, Scott Helme ,Alan Woodward ,"Analysis of the adoption of security headers in HTTP" https://ieeexplore.ieee.org/document/8304878
4. Li Chang, Hsu-Chun Hsiao, Wei Jeng, Tiffany Hyun-Jin Kim and Wei- Hsi cLin, "Security Implications of Redirection Trail in Popular Websites Worldwide", in Proceedings of the 26th International Conference on World Wide Web (WWW '17), 2017, pages 1491-1500. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland. DOI: https://doi.org/10.1145/3038912.3052698
5. William J.Buchanan,Scott Helme,Alan Woodward, "Analysis of the adoption of security headers in HTTP", in IET Journals ,September 2017,pages 1-8DOI: https://doi.org/10.1049/iet-ifs.2016.0621
6. Sterne, B., Barth, A.: 'Content security policy 1.0 [Internet]. W3C. 2012'. Available at http://www.w3.org/TR/CSP/
7. Ming Ying and Shu Qin Li, "CSP adoption: current status and future prospects", in Security and Communication Networks, Vol 9, Issue 17, 25 November 2016, pages 4557-4573. DOI:https://doi.org/10.1002/sec.1649
8. Michal Weissbacher,Tobias Lauinger ,and Willam Robertson," Why Is CSP Failing? Trends and Challenges in CSP Adoption"2014,pages 1-22.International workshop on Recent advances in intrusion detection, https://link.springer.com/chapter/10.1007/978-3-319-11379-1_11
9. Aditya Sood and Richard Enbody, "The state of HTTP declarative security in online banking websites", in Computer Fraud & Security, Volume 2011, Issue 7, July 2011, pages 11-16. DOI: https://doi.org/10.1016/%20S1361-3723(11)70073-2
10. Scott Helme, "Alexa Top 1 Million Analysis - August 2017", blog post, 29 August 2017, https://scotthelme.co.uk/alexa-top-1-million-analysis-aug-2017/
11. Hoskote homemaker loses Rs 50000 to conmen in 2 minutes, https://timesofindia.indiatimes.com/city/bengaluru/hoskote-homemaker-loses-rs-50k-to-conmen-in-2-minutes/articleshow/70235512.cms
12. Xinle Yang, Yang Chen and Xiaohu Chen "Effective scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information" 2019 IEEE International Conference on Blockchain (Blockchain)
13. Tara slaman, Raj jain, Lavgupta " A reputation management framework for knowledge-based and probabilistic blockchain" 2019 IEEE International Conference on Blockchain (Blockchain)
14. Weilin Zheng, Zibin Zheng, Xiangping Chen, Kemian Dai, Peishan Li and Renfei Chen "NutBaaS: A Blockchain-as-a-Service Platform" Citation information: DOI 10.1109/ACCESS.2019.2941905, IEEE Access
15. Harsh Desai, Murat Kantarcioglu, Lalana Kagal "A Hybrid Blockchain Architecture for Privacy-Enabled and Accountable Auctions" 2019 IEEE International Conference on Blockchain (Blockchain)
16. Jae-Seo Lee , HyunCheol Jeong , Jun-Hyung Park , Minsoo Kim , Bong-Nam Noh "The Activity Analysis of Malicious HTTP-based Botnets using Degree of Periodic Repeatability*" 2008 International Conference on Security Technology
17. Kyungroul Lee, Hyungjun Yeuk, Sungkwan Kim, Kangbin Yim "Security Assessment on User Authentication by an HttpSendRequest Hooking in an HTTP Client" 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing
18. Meisam Eslahi , M.S.Rohmad , Hamid Nilsaz , Maryam Var Naseri, N.M.Tahir, H. Hashim "Periodicity Classification of HTTP Traffic to Detect HTTP Botnets" 978-1-4799-8969-0/15/$31.00 ©2015 IEEE
19. Manh Cong Tran, Yasuhiro Nakamura "Classification of HTTP Automated Software Communication Behaviour Using NoSql Database" https://ieeexplore.ieee.org/document/7562957
20. Jiwon Min, Youngseok Lee "An Experimental View on Fairness between HTTP/1.1 and HTTP/2" 978-1-5386-8350-7/19/$31.00 ©2019 IEEE."

AUTHORS PROFILE

Jeevankumari Chevula pursuing Masters Degree in computer Science & Engineering from Sreenidhi Institute of Science and Technology, Hyderabad. She has completed her B. Tech Degree from JNTU Hyderabad. She also published few papers in reputed journals

Dr.Aruna Varanasi Professor & HOD, Department of computer science and Engineering, Sreenidhi Institute of Science and Technology, Hyderabad. She completed Ph.D. and She has great passion in devising solutions to security issues in Information Technology and has been doing lot of research work in Cryptography, Image cryptography, Information Security and Bioinformatics. She is an enthusiastic researcher .she has more than 14 years of teaching , research and administrative experiences.Her research interests in Information Security ,Cyber Security. She has published around 52 research papers in various reputed journals both at national and international level. She received "Best Teacher in Computer Science and Engineering Department, AP & TS" award by ISTE, during December, 2017.