Browser Security: An Assessment

Srimant Mishra*, Satya Swain, Arundhati Sahoo
Department of Computer Science and Engineering
Gandhi Institute for Education and Technology,
Baniatangi, Bhubaneswar

SWARUPA PATTANAIK, Department of
Computer Science and Engineering
Rajdhani Engineering College, Bhubaneswar

Abstract - The initial design of internet and web protocols assumed an environment where servers, clients, and routers cooperate and follow standard protocols except for unintentional errors. However, as the amount sensitivity of usage increased, concerns about security, fraud and attacks became important. In particular, since currently internet access is widely available, it is very easy for attackers to obtain many client (and even host) connections and addresses, and use them to launch different attacks, both on the networking itself and on other hosts and clients. Today's attackers are more likely to host their malicious files on the web. They may even update those files constantly using automated tools. When you are surfing the Internet, it is easy to visit sites you think are safe but are not. These sites can introduce malware when you click the site itself, when you download a file from the site manually and install it, or worse, when you are conned into believing the site you are visiting is a real site, but in fact is nothing more than a fake used to garner your personal information. From a network security perspective, a browser is essentially a somewhat controlled hole in your organization's firewall that leads to the heart of what it is you are trying to protect. While browser designers do try to limit what attackers can do from within a browser, much of the security relies far too heavily on the browser user, who often has other interests besides security. There are limits to what a browser developer can compensate for, and browser users will not always accept the constraints of security that a browser establishes.

Keywords: Security, Cryptography, Algorithms, Web Browser Security

I. INTRODUCTION

In the globalization era, the web browser is a consumer's window to the world that gives the user an interface to do a variety of activities that included social networking, email correspondence, personal business, personal finance management, and shopping [1]. It is a computer application used for presenting, transmitting and retrieving information resources on the World Wide Web (WWW). Web browsers are the most commonly used client applications on the Internet. It is helpful in accessing information provided by a web serves in files in a file system or a private network. There are many Web browsers are available for the user, such as Internet Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox, Safari, and other browsers [2]. Browser security is the application of Internet security in web browsers to protect network data and computer systems from malware or privacyinfringement.

Nowadays, hacking is an enormous problem in the wireless local area network (WLAN) [3]. If the web browser is not secure well, this will make the hackers to easily get your computer and enable malware such as adware, spyware, and viruses to be downloaded. Vulnerabilities in web browsers can help hackers control your computer, damage your computer, steal your credentials and identities and monitor your surfing habits. Web browser security plays an important role to secure the information or data from attacking by hackers [2]. Information security has proposed to provide integrity, authentication, non-repudiation, and confidentiality for carrying information between the user and computer[4].

WLAN is one of the fastest growing technologies. It is mostly found in many other public areas and office buildings. The security in WLAN is based on cryptography. Cryptography is the art and science of converting messages to make them secure and protected from attack by validating the sender to the receiver within the WLAN [3].

Cryptography algorithms are designed to secure data transmission and storing between cloud storage services and user [5]. Cryptography is a modern encryption technology that consists of different mathematical processes involving the application of algorithms, usually to secure the and diplomatic communications and discretion of the military. Cryptography is also defined as a subdivision of cryptology, in which decryption or encryption algorithms are designed to ensure the authentication and security of data [6]. Encryption is mainly to scramble the content of the data, such as video, text, audio, images and others, so that the data in the transmission or storage process become unreadable, invisible or incomprehensible.

Decryption is the opposite process of encryption [7]. Cryptography algorithm can be divided into Symmetric (private) key encryption algorithm, Asymmetric (public) key encryption algorithm and Hash Function [3] [4] [6] [7] [8]. The classification of encryption techniques is shown in Figure 1below.

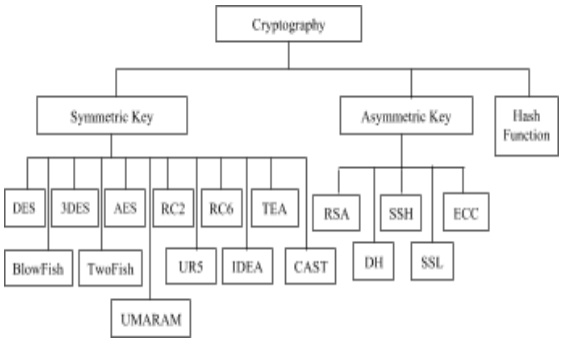

Fig. 1 Overview of Cryptography

Encryption is the process of converting plain text into a cryptic text. Plain text("unhidden") is an original data that is needed to be stored, transmitted, can be readable and understandable by both computer and people. Cryptic text("hidden") is a data that unreadable by both computer and human [7]. Symmetric key encryption algorithm is also known as one-key, private-key and single-key encryption as it uses only one key to encrypt and decrypt data [6]. The key is distributed before communication or transmission. A longer key is needed to use as it is harder to break than using a smaller key. A smaller key will decrypt the data [8]. The symmetric key encryption algorithm is widely used in WLAN [3]. The asymmetric key encryption algorithm is also called public-key and two keys (public and private keys) algorithms. A public key is used for encryption, while the private key is used for decryption [4]. The asymmetric key encryption algorithm is almost 1000 times slower than Symmetric key algorithm as they need more computational processing power [4] [8]. The hash function is a one-way encryption that uses no key to make sure the information will not be altered. It is a mathematical algorithm used to map arbitrary value to a fixed-sized hash value. The input is almost called as a message and the output which is the hash value called as the digest [9][10].

The study in this paper involves the area of web browser security and cryptography algorithm. Web browser security is the features of internet security for web browsers to protect networked data or information [11]. Web browser threats and their solutions are investigated. The study also proposes to investigate the most compatible algorithm for the webbrowser.

II. RELATEDWORK

A. Background ofResearch

According to Statistic of Network Vulnerability from edges can 2018 vulnerability statistic report, it shows that cryptographic occupy around 45% of network vulnerability. This research focuses on the web browser security, that's to investigate different security threat and attack to the web browser, show different criteria of cryptography and compare the encryption algorithm among the webbrowser.

B. Web Browser Threats andAttack

Security attack is an action that tries to modify, destroy or steal the information and make unauthorized access tothe web browser. The security threat is more to system danger or vulnerability that may lead to anattack.

Persistent Malware: The persistent malware will still maintain status active even though the system reboot. The forensic investigators will identify the malware by examining two persistence locations which are the registry and the startup folder first. There are many examples of malware likes virus, trojans, rootkits, worms, spyware, crimeware and adware. A malware DLL can hidethemselves in a specific directory with a specific name. Other than that, an attacker may try to install a botnet client which can cause the infection and make others to be zombies. Bonets can be functioned as the DDos attack, steal information, send spam email and allow the bot header which is mean the attacker to control the devices andthe network links. This is controlled by using the command and control software which is called as C&C.

Inside the client-server model, the Internet Relay Chat (IRC) server will send the command to the infected clients and wait for their reply in certain predetermined-channel. Inside the peer-to-peer network, only the client that proceed with a private key can control the botnet, for example, the GameoverZeuS which is a peer-to-peer botnet based on the ZeuS Trojan (malware package that runs on the Microsoft Office). Especially, the attacker tries to keep the malware survive even the browser is closed. AV-Test Institute registers around 350,000 malware program and potentially unwanted application (PUA) [13] [14].

Transient Keylogger: Transient Keylogger is temporary and cannot be maintained alive after the browser is closed. Keylogger means that the stealer can capture the key that presses by the

user and get the data without awareness of the user. This is mainly for stealing the password, credit card number or private information. It can be done in both hardware and software. For the hardware side, the attacker might modify the BIOS that handles the keyboard event to take note of the action or plug in some external component under the keyboard to get to know which button is pressing. For example, some of the ATM passwords can be stolen by overlapping the keyboards or hidden CCTV. There is some sound detector, they try to differentiate the sound produced by each key and guess the key that might be pressing. Other than that, the detect the electromagnetic emission upon 20 meters of the keyboard. They might sniff and capture the packet from the wireless keyboard too. For the software side, the sniffer might copy the data into clipboard which is also called as data buffer and capture it by using specific program. Brute force attack can be applied in this case, they are using some of the software to guessing the key and character. The recording of searching, instant message or even window also might expose the key password to attacker[15].

Cross-Site Scripting (XSS): Cross-Site Scripting is a security vulnerability that enable the attacker to insert the malicious script inside the web pages. An attacker will attempt to send the script to the end user and the end user execute it without any hesitate. This is because they think the script come from a trusted web page. This kind of script might able to access any cookies, session tokens or gather other privacy information. There is many personal information can be gained from the cookies which is the small piece of data store in the web browser likes name, password, or date. There are many types of XSS which are persistent, nonpersistent, server-sides vulnerability, DOM based vulnerability, self-XSS, mutated XSS. Persistent XSS show up when the data is passing by the web client and immediately used by server. However, non-persistent XSS show up when the data is directly saved into the server. The difference between serversides and DOM-based is that DOM-based is fully run in the client sides only. Self-XSS is reflecting on Social Engineering refer to psychological manipulation of people and trickthem.

Mutated XSS is reflecting on modification and rewritten the malicious code to make it seem like reliable [16] [17].

Buffer Overflow: Buffer is a temporary place to store the data when it moves from one program to another program with limited memory. The buffer is same as a bucket when the bucket is full of the water, but users continue to fill in, the water will pour over the side of the bucket and out. It will cause overrun the memory and overwrite the adjacency locations. This makes the erratic program occur and the data memory crash. When sending a lot of data to cause a buffer overflow, it is possible to overwrite the original executable code with malicious code. It is also possible for the attacker to get the privilege escalation that means they have the higher privilege than the original programmer and get unlimited access to the resources. Morris worm which is one of the early computer worms spread over the internet that invented in 1988 and it used the technique of overflow too [19]. JEMalloc Memory allocator which is used in Firefox is possible to lead to heap overflow which is one type of the buffer overflow. There is also a thing called as heap underflows when the object is too small to store the input. Dangling pointer (pointer don't point to a valid object with appropriate type)" use-afterfree" error occurs when the dangling pointer is used after it had been free without allocating new memory location[18].

Browser Cache Poisoning: Browser Cache Poisoning corrupt the data and insert into the cache of Domain Name Server (DNS). There are 6 types of browser cache poisoning which are timing attack, poisoning browser web cache, HTML5, AppCache, HTTP caches, Man-In-The-Middle Attacks (MITM) Cache Poisoning, cross-site scripting attack, shared medium cache poisoning and proxy cache poisoning. The timing attack is used to sniff the credential data that store inside the cache and steal the user password to get personal data. There is one tool called airpoison which is used in the wireless network. MITM Cache Poisoning also is known as ARP(Address Resolution Protocol) Cache Poisoning, the attacker will act as the gateway, so all the information must go through the attacker, and the attacker tries to intercept the ARP request and response as well. ARP is a protocol that used for translating IP Address into link- layer address such as MAC Address which is a critical address mapping feature for communication in TCP/IP as shown in Figure 2. Cross-site is used to inject the malicious code into the web app. Every station can see the traffic of each other over a shared medium under unencrypted or Wired Equivalent Privacy (WEP) encrypted networks. An attacker might observe all the frame under Wi-Fi Protected Access (WPA/2) encrypted network, but cannot block, delay or controlthe frame

above. Proxy cache poisoning attack is mean to attack both directions of proxy. The Malaysian Google domains google.my and google.com.my faces DNS cache poisoning attack in 2013[20]

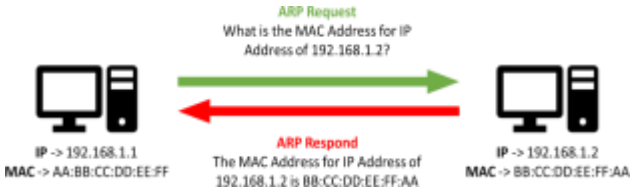

Fig. 2 ARP protocol operation

System Protection for Security Threat andAttack

Disable JavaScript in browser by default is one of the methodto prevent the malware implement into the web browser. Most common language likes PHP and ASP.net are running on server side, but JavaScript is running on clientside. This will break many websites, so users need to reenable it. This action helps users to differentiate which websites need to execute JavaScript and which one don't need to execute JavaScript. Plug-in cannot be the placed inside either rendering engine or browser kernel because the vendor expects there will be at least one plug-in inside the rendering engine. Since the malicious plug-in placed inside the browser kernel, it might affect the entire browser. Plugin is running outside the sandbox by default and able to get the permission of microphone or camera and update the file system. This might lead to the security vulnerability that provides the opportunity for installing malware. For example, a Google researcher found one of the free plugins of AVG Antivirus going through the Google's Chrome browser security and it could be used to steal the browsing history and personal data over 9 million users in the world. Hence, it is better to not install and apply the suspicious browser's extension[21].

To prevent keylogger, add an extra layer of protection by using the virtual private network (VPN). Use VPN to encrypt the data. There are many web browsers have the features of saving the password and credential information and let the user log in again in next time easily. It is too risky to expose the personal information if someone gets unauthorized access to the computer and the account kept a login. A password manager can be used since the password is automatically fill in but not by typing, the keylogger unable to get the password from your keyboard. Egress filter might be used to filter the network traffic to prevent the flow of information outbound from one network to another network. Install application gateway with spyware filtering helps to avoid from the keylogger[22].

HTTP X-XSS-Protection response header is one of the special features for Chrome, Safari and Internet Explorer. It helps to stop the pages loading when detecting the CrossSite Scripting. It will enable the XSS filter to block the malicious scripts inserted. Content-Security-Policy also helps in protection of web browserfrom XSS attack.

Table. 1 Platform used for X-XSS-Protection and Content-Security Policy [23] [24]

Web Browser	**X-XSS - Protection**	**Content-Security-Policy**
Chrome	Yes	version 25*
Edge	Yes	version 14
Firefox	No	version 23*
Internet Explorer	version 8	version 10*
Opera	Yes	version 15
Safari	Yes	version 7*

Bound Checking should be implemented in the compiler which is used to detect whether the value is within some bound. For example, the month of the calendar must valid the range from 1 to 12. Many of the programming compilers want to raise speed and throw away the bound checking likes the C programming compilers. This might lead to buffer overflow. strcpy and strcat are not encouraged in preventing the buffer overflow because they both copy the string of buffer and append onto another without checking any bound. In opposite of C compiler, OpenBSD has paid attention to bound checking, they implement a more secure function, strlcpy* and strcpy_s* which like the strn write the maximum size of the target buffer[27].

To prevent the browser cache poisoning occur, configure the DNS server to limit recursive queries and DNS transfer zone. Some of the attacker might try to perform the DNS Zone Transfer to more understand the topology of the network. Dig, host and nslookup can be used for testing the transfer zone from remote access. If the recursion is enabled, thirdparty can query the server name as they want, it might lead to browser cache poisoning too. To increase the safety, it is better to

disable the function of recursion. Other than that, Security Trails can be used to review and audit the DNS zones, records and IPs such as A, CNAME and MX records. It is very easily to get the DNS version if bind is using by just simply type the query. Block the unnecessary port in the firewall and only permit some basic service to run through will helps to decrease the chance to get attack [25][26].

C. Encryption Algorithm

To secure the web browser, encryption cannot be ignored. No wonder what kind of security attack or threat, encryption also will give challenges for the attacker to overcome. Here are four encryption algorithms investigated which are DES, 3DES, RC6, and AES.

AES: Advanced Encryption Standard is one of the symmetric encryption. It uses a block cipher to encrypt data. There is different round for each key bit that convert from plain text to final output, 128-bit has 10 rounds, 192-bit has 12 round and 256-bit has 14 rounds[28].

DES: Data Encryption Standard which is a symmetric-key and is implement the Feistel Cipher. Feistel is a symmetric structure used to construct the block ciphers. For DES, the block size is 64-bits and take 16 rounds [29].

3DES: Triple Data Encryption Standard is a symmetric-key and uses block cipher as similar as AES. 56-bit keys are used which encrypts data three times, 56-bit become 168-bit key. The 168-bit[30].

RC6: Riverst Cipher 6 has block size of 128 which support key 128, 192, 256. RC6 similar with two parallel RC5 encryption, but RC6 use extra multiplication operation which is not present inRC5[31].

RSA: Rivest–Shamir–Adleman has 1024 bits which is the public key cryptography used to secure the data transmission[32].

ECC: Elliptic Curve Cryptography usually applied in smaller devices like cell phone. The key size around 16 bits. Elliptic curve is likes a plane curve over a finite field [33]. **DH**: Diffie-Hellman key algorithm is not for encryption or decryptionbut generate shared secret key for communication and exchanging information. The key size is around 1024 bits [33].

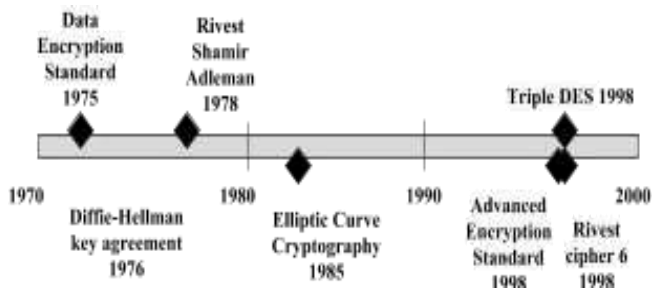

Fig. 3 Timeline of encryption algorithm [28] [29] [30] [31] [32] [33]

III. REVIEWANDDATACOLLECTIONJ OURNAL, CONFERENCE PROCEEDINGS, ARTICLEAND USEFUL WEBSITES

In this paper, the focus on the respond time of symmetric algorithms for encryption and decryption are AES, 3DES, DES, and RC6 on different web browsers which is Mozilla Firefox, Internet Explorer and Google Chrome.

A. Symmetric Algorithms on Different Web Browsers

A comparison of encryption algorithms (symmetric key) in cryptography (RC6, 3DES, DES, and AES) are chosen to test the speed of different web browsers. The data is collected from two desktop computers and analysis the speed of both computers to encrypt a set of text and key for ASP scripts via Web browsers. This method is chosen in the study because it can clearly compare the performance of different encryption algorithm to encrypt ASP scripts of all three different web browsers which are Mozilla Firefox, Google Chrome, and Internet Explorer and the result is shown inTable2.

For Mozilla Firefox version 10, RC6 has better performance in 40 and 50 Text Length while 3DES has less response time in 10, 20, and 30 Text Length. The response time in Internet Explorer version 9 for 3DES and AES are almost the same and have higher performance in all Text Length compare to another encryption algorithm. In Google Chrome version 17, AES is more suited compared to other encryption algorithms because it has less response time and better performance in all Text Length. From the review of the journal, an algorithm performs best on a web browser is as follows:

1. Mozilla Firefox suited for RC6 when text length larger than 40 while 3DES is suited for text length smaller than40.
2. Google Chrome suited forAES.
3. Internet Explorer suited for 3DES andAES.

In overall, the AES algorithm has good performance and good speed test in all web browsers. However, there are a few factors might

affect the response time of web browsers such as the web browser's version, theoperating system installed in the computer and the computer configuration [12].

Table. 2 Comparison of symmetric algorithms in the different web browser [3] [12]

Web browser		Text Length				
		10	20	30	40	50
Mozilla Firefox	DES	Moderate	High	High	High	High
	3DES	Low	Low	Low	Moderate	Moderate
	RC6	High	Moderate	Moderate	Low	Low
	AES	Moderate	Low	Moderate	Moderate	High
Google Chrome	DES	Moderate	Moderate	Low	High	Moderate
	3DES	Moderate	High	High	Moderate	High
	RC6	High	Low	Moderate	Moderate	Moderate
	AES	Low	Moderate	Low	Low	Low
Internet Explorer	DES	Moderate	High	High	High	High
	3DES	Low	Low	Moderate	Low	Low
	RC6	High	Moderate	High	Low	High
	AES	Low	Low	Low	Low	Moderate

IV. CONCLUSION

In this paper, the web browser threats and solution for it are presented. This paper also presents the most suitable and compatible algorithm for the web browser. From the review of some papers, we have concluded that the best algorithm is AES because it consists of the highest encryption rate, smallest memory usage, and the most secure algorithm. AES is a symmetric algorithm with the fastest process of encryption to secure the datatransmission.

REFERENCES

1. M. T. Louw, J. S. Lim and V. Venkatakrishnan, "Extensible Web Browser Security," B. M. H¨ammerli and R. Sommer (Eds.): DIMVA 2007, LNCS 4579, pp. 1-19,2007.
2. N. C. B. Mauritius, "Guideline for Securing Your Web Browser," Enhancing Cyber Security in Mauritius, no. 2,2011.
3. G. Ramesh and D. R. Umarani, "Performance Analysis of Most Common Encryption Algorithms on Different Web Browsers," I.J. Information Technology and Computer Science, no. 12, pp. 60-66, 2012.
4. A. Jain and D. Bhatnagar, "A Comparative Study of Symmetric Key Encryption Algorithms," International Journal of Computer Science and Network, vol. 3, no. 5, pp. 298-303,2014.
5. K. P. Karule and N. V. Nagrale, "Comparative Analysis of Encryption Algorithms for Various Types of Data Files for Data Security," International Journal of Scientific Engineering and Applied Science (IJSEAS), vol. 2, no. 3, pp. 495-498,2016.
6. M. Ebrahim, S. Khan and U. B. Khalid, "Symmetric Algorithm Survey: A Comparative Analysis," International Journal of Computer Applications, vol. 61, no. 20, pp. 12-19,2013.
7. S. Kumari and J. Chawla, "Comparative Analysis on Different Parameters of Encryption Algorithms for Information Security," International Journal of Innovations & Advancement in Computer Science, vol. 4, no. Special, pp. 123-129,2015.
8. D. S. A. Elminaam, H. M. A. Kader and M. M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms," International Journal of Computer Sci 280 ence and Network Security, vol. 8, no. 12, pp. 280-286,2008.
9. S. Northcutt, "Hash Functions," Security Laboratory: Cryptography in Business Series,2008.

10. Jscrambler, "Hashing Algorithms," Jscrambler, 25 October 2018. [Online]. Available:https://blog.jscrambler.com/hashing-algorithms/.
11. W. Dormann and J. Rafail, "Securing Your Web Browser," Software Engineering Institute Carneige Mellon University, pp. 1-34,2017.
12. S. A. A. Syed Zulkarnain Syed Idrus, S. M. Asi, S. Sudin and B. Ahmad, "Performance Analysis of Encryption Algorithms' Text Length Size on Web Browsers," IJCSNS International Journal of Computer Science and Network Security, vol. 8, no. 1,2008.
13. "Malware Detection in Cloud Computing Infrastructures", International Journal of Recent Trends in Engineering and Research, pp. 223-227, 2018.
14. "Malware definition – What is it and how to remove it", Malwarebytes, 2018. [Online]. Available:https://www.malwarebytes.com/malware/.
15. Reiner Creutzburg, Technische Hochschule Brandenburg, Department of Informatics and Media, IT- and Media Forensics Lab, P.O. Box 2132, D-14737 Brandenburg, Germany, "The strange world of keyloggers - an overview, Part I",2017.
16. LIU and Y. OU, "An Improved XSS Vulnerability Detection Method Based on Attack Vector", DEStech Transactions on Materials Science and Engineering, no.,2018.
17. H. Gaikwad, B. B. and P. Chatte, "SQLi and XSS Attack Introduction and Prevention Technique", International Journal of Computer Applications, vol. 165, no. 2, pp. 23-27,2017.
18. Y. Jang, "Buffer Overflow Vulnerability Instrumentation Technique to Safety Checks of Variables", Korean Society of Technical Education and Training, vol. 23, no. 2, pp. 51-64,2018.
19. A. Jajoo, "A study on the Morris Worm," Purdue University, p. 18, May 7,2018.
20. "Google's Malaysian Domains Hit with DNS Cache Poisoning Attack," Oct 11,2013.
21. "JavaScript Malware – a Growing Trend Explained for Everyday Users", Heimdal Security Blog, 2018. [Online]. Available:https://heimdalsecurity.com/blog/javascript- malwareexplained/.
22. "5 Ways to Protect Yourself Against Keyloggers", MakeUseOf, 2018. [Online]. Available:https://www.makeuseof.com/tag/4-ways-protectkeyloggers/'.
23. "X-XSS-Protection", MDN Web Docs, 2018. [Online]. Available: https://developer.mozilla.org/enUS/docs/Web/HTTP/Headers/X-XSS- Protection.
24. "Content-Security-Policy", MDN Web Docs, 2018. [Online].Available:https://developer.mozilla.org/enUS/docs/Web/HTTP/Headers/ContentSecurity-Policy.
25. "Cache Poisoning Attack", Veracode, 2018. [Online]. Available:https://www.veracode.com/security/cachepoisoning.
26. M. Dargin, "How to protect your infrastructure from DNS cachepoisoning", Network World, 2018.[Online].Available:https://www.networkworld.com/article/3298160/internet/how-to-protect-your-infrastructure-from-dns-cachepoisoning.html.
27. "Detect, Prevent and Mitigate Buffer Overflow Attacks Synopsys",Software Integrity, 2018. [Online]. Available:https://www.synopsys.com/blogs/softwaresecurity/detect-prevent-andmitigate-buffer-overflowattacks/.
28. "The difference between AES encryption and DES encryption",SearchSecurity, 2018. [Online]. Available:https://searchsecurity.techtarget.com/answer/Thedifference-betweenAES-encryption-and-DESencryption.
29. "Data Encryption Standard", www.tutorialspoint.com, 2018. [Online].Available: https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm.
30. Definitions and C. Hope, "What is 3DES?", Computerhope.com, 2018.[Online]. Available:https://www.computerhope.com/jargon/num/3des.htm.
31. "Enhancement of RC6 block cipher algorithm and comparison withRC5 & RC6 - IEEE Conference Publication", Ieeexplore.ieee.org,2018. [Online]. Available:https://ieeexplore.ieee.org/document/6514287.
32. A. Aryanti and I. Mekongga, "Implementation of Rivest ShamirAdleman Algorithm (RSA) and Vigenere Cipher in Web BasedInformation System", E3S Web of Conferences, vol. 31, p. 10007,2018.