Cookies, Privacy and Cyber Security

Weerasinghe S.D.R.M.
Faculty of Information Technology
University of Moratuwa
Sri Lanka
ruwan.16@itfac.mrt.ac.lk

Abstract— The 21st century suggests that people live in the so-called digital era. It's the age of the technical evolution. Because there are many things that exist now but not in the past few decades. Any description of any information that is a secure and unique person may be accessed by third parties. There is information and statistics in the past, future and present that it is so devastating ever more than ever. This study reveals some important aspects on cookies, privacy and cyber security.

Keywords— Cookies, Privacy, Cyber Security, Cyber-attack, Cyber crime

I. INTRODUCTION

Cookies are a very important and relevant technology that many people today use on the Internet. Cookies for Internet experience play a crucial role. It was a delightful solution to a missing protocol for small amounts. With that, a client can remember the timetable that a user can access to his / her site. It's also better to have a shopping experience online, personal user content, and accurate advertising. Nevertheless, Cookies can use to realize the history and functions of the cookie and not have security in the design.

The cookie isn't made for security. It doesn't guarantee the security, trusty or integrity of the information. But it's important to note two cookie attributes: Safe and HTTP only. Secure Load limits cookie for secure channels only when client connects to cookie when request exceeds TLS (Transport Layer Security) [1]. While this protects the privacy of the cookie, it does not protect the perfection of an attacker when sending a request to a secure site. The other attribute is HTTP only.

Hackers are accessed to computers and networks to steel information that are confidential and integrated. These details may be belonging to medical, financial or another sector. Keeping information confidentially is important since those parties has been bound with whom that the information belongs.

The most challenging part is with create cyber defense system. Mainly two issues arise when creating a cyber-defense system.

> Organizations or data/information holders are not eager to share private data with others.
>
> With agreeing for a solution that can provide personal protection, a new or unknown cyber event must be prepared for cyber threat information to build a training format for future forecasts [2].

According to the scope of collaborative security, Co-ordination security shares the cyber security knowledge from organizations or nodes to replace "centrally-controlled policies" with organizations or nodes to "make informed decisions". Purpose of this partnership is to make more critical decisions obtaining more information. Using the information can be made the right decision. Therefore, "Collaborative Safety" is a joint effort by sharing diverse safety data to provide the most potent choices among a variety of safety systems. [2] Collaborative security system has used in high security contacts, spam, malicious software, unauthorized identifications, etc. Collaborative protection comes from desktop and mobile environments [3].

A large number of information in world and increase in the number of cybercrimes day by day. Different computer-based learning technology-based learning techniques that try to obtain unauthorized entree to data need to build an active cyber security system, and unusual behavior or anomalies make a correct decision or predicting that it will save user from any offense before damaging the system. This can be achieved by learning the existing dataset containing information about various intrusions or attacks as well as their responses. Once the system has finished learning from the formed dataset, it is able to detect if a new intrusion occurs [3].

In worldwide security concern as highly. Detection and reaction ability for such a threat is increased with technological advancement. Historically, information security has been safeguarded by dangerous actors and the continuing information cycle collected by the information community is a dangerous quest. Detecting new risks and risks, malicious signatures or patterns created. To detect such kind of malicious activity, Intrusion Detection Systems (IDS) uses these signatures [4] . The IDS warn human analysts. Unfortunately, there are some alarms that are False Positive (FP). Applying Machine Learning could be beneficial for such scenarios like a daily operational routine of Security Operation Center. Each organization would like to benefit from various CTI data from other institutions. CTI participants be able to find out aware of different types of reasoning. Of those threats, they can be prepared earlier the actual threat. Therefore, as all companies share information, still determine about threats and how to bargain with them. Companies can increase accuracy to ensure that any activity is not malicious or malicious. Certain challenges are with regards of threat intelligence exchange collaboration [5].

Other participants cannot trust the information exploitation as shared organizations

Concerns about the confidentiality of sensitive information. Attackers or other competitors can be exposed

The organization's reputation can be influenced if organizations can identify risk-bearing information.

II. Cookies

One of the major threats to the network is the robbery of sessions with aid of cookie exploitation. An HTTP cookie is a small data or text file sent from a website or server and stored in the client's web browser while the user is searching. Cookies are created when a user visits a site and the site uses cookies to track the user's movements [6].

Wireless network is important fact and it is very famous in this digital era. The major advantage of wireless networks are mobility and flexibility for the clients. The current wireless networks can be affected to various attacks. The main threat is the snapshot can be exploited by cookies.

When a user visits website, the web-browser sends a cookie value to server and alerts user's past activity. Cookies contains only a plain text but doesn’t contain executable code. Cookies use for various activities on a website [7] . Storing of cookie information and instructs the browser by the server and returns its value with all the request and the information server can be identified for single users.

Mainly a cookie store about following information like cookie name, cookie value, cookie expiration, domain name, cookie path, security information for the cookie [6] . Also, there are so many types of cookies.

Session cookie/ Transient cookie - Session cookies contains about user information. After the closing web browser by user session cookie also delete. This type is a temporary one.

Persistent cookie - Even after closing the browser persistent cookies not deleted. Persistent cookies have specified date and time to delete itself. Using this cookie web server, the user remembers the user's settings and information when they visit web site [6] .The major data like authentication information, language, menu preferences and bookmarks or website accessibility stored in this type of cookie.

Secure cookie - The main difference of secure cookies is transfer after encrypting.

HTTP Only cookie - HTTP Only cookies are transmitting through the HTTPS protocol. This is stored in user storage like hard drive. HTTP only cookies can’t be steel over the risk of XSS.

Third-party cookie - These cookies are not absolutely visited by user but write on the relevant server. Third party cookies are created by a web page which loads from another website’s page content. The major use of these cookies audits the user behaviors. After auditing the behaviors of users, this type of cookies share information with advertising companies.

Super cookie - Super cookies are storing permanently in user computers. These cookies have newer technologies that doesn’t depend on http cookies. The major specification of t is that can’t delete like other cookies from the storage. Super Cookies store information such as browser history, verification data and advertising information.

Zombie cookie - Zombie cookies are naturally re-generated after deleting from a client-side script. The zombie cookies are stored in user hard drive directly or online server. Because of this reason these cookies breach the browser security and very hard to delete these types of cookies [7].

Main uses of Cookies are

1) Store a current web site on a cookie user's web site. This information can be used to navigate between websites efficiently.

2) The number of visitors to the website using cookies can be identified.

3) Cookies may store client settings, preferences then the user can return to the same website. All those options are provided by the web server.

4) Cookies makes users to settings up a site of their choices and preferences [8].

A. *Working Process of Cookies*

For the relevant URL, web server gets requests from the browser. After receiving the request that sent from browser, it first searching for cookies. If can’t find a cookie itself then creates a cookie with unique identification. The created cookie store in the user’s hard drive or storage. Varity of settings are stored of web site database and linking to the cookie [9]. After that if the corresponding user come back to the same web site cookies also forward again web server sends same preferences to user.

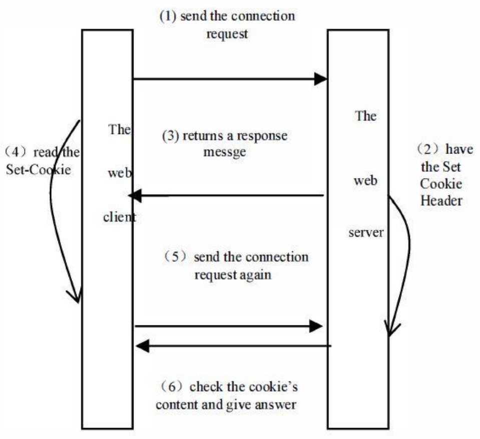
(1) send the connection request
(4) read the Set-Cookie
The web client
(3) returns a response messge
The web server
(2) have the Set Cookie Header
(5) send the connection request again
(6) check the cookie’s content and give answer

Figure 1. Working Process of Cookies

B. *Main Threats related to Cookies*

Sniffing Network Traffic for Cookies - Following are the main software that can be used to steal cookies from sniffing traffic for cookies. Wireshark, Kismet, Microsoft network monitor, Cain and able.

Cross-Site Scripting Attack - This is intensely base method for stole cookies. In this cross-site scripting attack, the user steals cookie data and information by click on link which contains malicious scripts. In this attack’s client clicks information unknowingly that containing malicious scripts and after that open that script and sends user information to the attackers automatically.

CSRF Attack - This CSRF attack, the attacker allows to user to do critical action without user preference. This can even be used to reform the firewall settings, publish illegal data, perform fraudulent economic transactions.

Session Fixation Attack - This attack imposes emerge of system that grants one user for find separate users session ID [10].

III. Cyber Security

There are so many areas in cyber security such as use security analytics to identify the threats, define organizational anti-threats requirements, develop IT security strategies, create cloud-based IT security, migrate information to cloud based strategy, maintain IT security platform [11].

Cyber security is a domain that has a great impact on the concept of privacy and national security. Cyber threats have been confronted at all levels and user information has been used to protect users' assets. Cyber-attacks are carried out with specific intentions of exploitation [12] .These are the phases that have in cyber-attack.

Phase 1 - Cyber attackers monitor the operations of the system across various applications as spyware and determine target locations.

Phase 2 - Penetrate the system. As long as the attacker cannot get into the system, it may not be able to access some services or make it unavailable to others

Phase 3 - Examining resources and rights to access the system and the information it stores.

Phase 4 - The attacker retrieves that information and steals it with damage or serious data.

A. *Different Cyber Threats*

Nowadays, cyber-attacks are carried out by malicious code and messaging via email known as phishing. Interrupt data and modify or delete data. Denial of services to prevent access to the network. Recording passphrases by recording by pressing the keys called a brute force. The encryption key used to encrypt information, known as key restarting attacks, is stealing and altering, and in many other ways, using cyber-attacks.

B. *Prevention Against a Cyber Attack*

Use encryption and encryption and its protocols such as WPA and WPA2

Using public networks and virtual private network (VPN)

Setting a password is recommended to use a password

Create various passwords for various online accounts

Use anti-virus and antivirus services

Store the firewalls

Continue to install the updated versions of the operating system / applications and applications installed on the system [2].

C. *Principles of Cyber Security*

Increased confidence from restrictions and restrictions is less expensive and calls to small sections with well-developed interfaces, well-proved security principles, such as privilege principle.

Protective covers Multiple layers (for example, the principle of freedom of freedom) are split into several layers [13] of layers by both the constellation elements and both.

Artificial and natural diversity (known as the principle of diversity) underscores the need for a variety of defenses with invisible targets to attackers [14].

Learning systems (known as the learning principle) emphasize the need for dynamic learning from past activities, data, and even from users.

D. *Cyber Security Strategies*

1) Prevention Strategies.

2) Detection Strategies.

3) Data Driven sciences.

Detecting cyber threats using text analysis.

Detecting Attacks using Graph Grammars

Stream-based Classification

E. *Challenges, Threats and Policy Implications to Compromise Privacy and Security*

Most users are scarifying of privacy, and contain a network of several people, especially internet or users.

Now, the "data" can be purchased, sold, traded, etc., and is widely used in writing an unusual article or letterhead. Regular information and data costs are usually higher than the costs of PCs and working innovations [15] . Nevertheless, raises the need to protect data from unauthorized access, destruction or theft. Most of the time, Internet users are not aware of the risks involved while being brutal. Risk includes privacy of user as well as Internet security. Over the past decade, the IoT has completely improved productivity and income growth. For example, Internet-based businesses, inventory network administration, and remote access increase customer satisfaction as organizations reduce costs by making their processes more efficient. Applications that combat offensive attacks with blocked activities must still work. Companies are constantly looking to satisfy customers and none of the companies are looking at the slightest risk [16]. In addition, it is important to note that the personal information of the client is considerably reduced to the risk of falling in the wrong direction. To combat these threats and ensure that internet of things exchange isn't compromised, secure innovations and technologies must be embraced in large part within current networking systems [15].

IV. Cyber security breches and cyber crimes

A. *Reasons for Cyber Crimes*

Personal Hostility
Hackers Self-Interest
Users Lack of knowledge about Social Media.
Users poor password
Get entered any sites randomly
Using untrusted link.
Using unauthorized application.
Lack of knowledge to working with email.
Backdated Operating Systems.
Hackers Use Religious Values [1].

Also, hackers use so many kinds of malware malicious software for hacking. Some malwares are Adware, Ransomware, Backdoor, Virus, Key Logger, Root Kit, Spyware, Trojan horse, Identity Thieves/Fishing, Worm [1].

Cybersecurity is about protecting computers, data, networks and programs from unauthorized access and attacks by individuals, groups, businesses and governments. Threats range from cyber fraud to cybercrime and cyber warfare at the national level. Cybersecurity is a growing concern for businesses. Threats are now becoming a major crossroads problem [11]. It defies efforts to protect its staff from cyber-attacks in accordance with policies designed to prevent data breaches.

Cybersecurity is a dimension in the world of the revolution on the Internet, and the rapid increase in cybercrime is risking national and international economies and security and are destabilizing. Cyber security, in brief, online unauthorized access to the Internet and the prevention of hardware and software risks. Different strategies, techniques, models and frames have been established to address the issue for cyber security [17] .The framework and steps taken for address the cyber security with various cyber threats, related concepts and fundamentals, personal, national and global cyber-attacks, models, cyber security measures, with restrictions and recommendations for improving cyber security.

With time, data and information are produced at a high speed at a high speed. Information systems used to manage these massive data are often complex and require network access, such as the Internet. Automating everything, and storing data in the clouds and networks has, in many respects, been used to hide the gloomy world of cybercrime and cybercrime mechanisms. Cyber Security is an all-in-one approach to protecting and protecting cyber space, and all of these are the same mechanisms and policies that both system insecurity and hardware are both. There are two things to ensure cybersecurity: First, assurance of hardware and software example security, encryption, and LAN analytics software. Secondly, the skilled labor required to deal with the workforce is the complex protection of cyber space [17].

A. *A growing Internet Crime*

According to a global economic crime survey conducted in 2016, criminal prosecution has been initiated for the criminal offense committed at the crime scene. This is the second most serious crime committed by 2016, which becomes the second most important crime. Most companies are digital. Continuous increase (Global Economic Crime Survey 2016). 32% of companies were affected and 37% of them attacked online (68% without a response schedule) and 18% reported an attack of 32% in 2016. Companies that are not ready to handle cyberattacks reveal a lack of awareness and a high risk of aggression [18].

B. *Cyber Crime Effects*

Businesses have various repercussions because of networking atrocities against them; Damage to the reputation at the top of the list. Other negative impacts are inside information used in financial losses, loss of paper, intellectual property loss, cyberbullying (intimidation), system crushing and sometimes, physical attack planning. It reflects several IoT formats. However, most of these agree with the above provision. The IOT is the first step for create the most relevant privacy and security mechanisms. Get data on other agents to create a distribution system. Process of sending and receiving data consists of very powerful internet connections from networks that are disabled by a network provider [16].

C. *The Challenges for Cyber Security*

Commendable research on RFID technology has taken place. It is very important to protect information against identity threats. However, the data that can be used for anonymous data processing techniques is that the evolution of the IoT can at a given moment identify the unknown data and thus not protect the RFID and anonymous information. In addition, many operating systems are designed for a single market niche or for home-based operations. As a result, it is difficult to prevent data from accessing IoT via distributed devices around the world. Customization of the client, confusion of information, anonymization and obscuration have been implemented to ensure that the data is not profiled [19]. However, for these methods to be effective and must calibrate the metrics and redefine the algorithms. On the other hand, these security services will be provided to individuals and businesses at higher prices that would never be adopted. At the same time, because of such high cost expectations, technicians may choose to make fewer investments for innovations that permanently endanger such data. Once the Internet is broadcast, the deployment technology will be expanded. The subjects do not seem so uninterested to know that they are not aware of what they are pursuing.

In addition, about 15 billion smart devices representing more than $ 15 billion will be more readily available. Interpreters who violate privacy violate their attention. When the world is digital, there is no chance that smart cities, smart homes, and smart businesses will innovate to separate private content from common support. The threat of database connectivity may intensify IoT with evolution [14].

D. *Policy Implications*

Organizations need to Back up through profiling, connectivity, and access paths, enterprise systems could be scanned or deleted. It is very easy to find and fix so that companies do not lose important documents or hackers. Added application firewall and backgrounds in real time. Dual DDoS and XSS not only protect business information, but also allow businesses to recover lost data during an attack [16].

Antispyware must also be acquired. This malware content, the Lavasoft advertising software and the spy robot to search and destroy. User must avoid accessing any content via emails or suspicious links. Otherwise, after receiving such announcements or invitations, they should be removed without opening it.

V. Cyber Security Requirements of Cookies

Confidentiality - Inside of a cookie include data which is used by the user to allocate users and own preferences. So, the security of this information should be assured. The main two ways to loosen up cookie data are immigration and stolen when it is stored in the client's device [20].

Integrity - Integrity of cookies can decrease the attacker from writing malevolent code into the cookie and preventing it from writing to a special mark. When using cookies for user authentication, if cookie details has been changed, the authentication will be failed. The attacker can resist the cookie content of the legitimate user, which will then prevent from accessing a website [20]. The domain and the way in the cookie are a very important part.

Identifiability - The encryption of cookies can be used to fight against unauthorized manipulations. Moreover, an attacker can still appear as authorized user by submitting stolen cookies to the site. So, the requirements should be able to certify that the cookie provider is owner of cookie.

To ensure the confidentiality, integrity, and authenticity of information in the network and site transmission process, the SSL / TLS security authentication protocol can be used to encrypt information transmitted across all websites. The SSL / TLS protocol provides three main areas of security services [20].

A trusted third-party authentication agency using digital certificates provides the identity verification function for communication between the client and the client for identification purposes. All data transmitted between the Internet and the customer is encrypted, prevented and malicious in order to prevent the illegal theft of users. The SSL encryption algorithm and the hash function are used to ensure the integrity of the data transmitted between the Web client and the server.

Also, Event monitoring and user verification of an account can do by using browser cookies. End users on a client system use accounts for connect to the server. The administrator should aware of the security of the data in account and not transmit the data to a third party. Added function of the admin is to monitoring identity of the user accounts but this often doesn't apply. The third thing to watch as an administrator is to monitor events in an account - devices that use the site to open or use multiple devices at once [21]. This context gives a solution to three different problems.

a) The ability to control and control how to use login / password and technical access

b) The user / password information used by the group administrator is not being used by the other person

C) Identifying the login / password simultaneously

For two different parameters, cookies have been used.

a) Protocol ID – each protocol has unique ID

b) Client Identity: Every time a user opens the same account but changes his protocol. This system has the efficiency to address all the above issues.

Various industries around the world still offer customers the ability to view and receive actual data about services using the real-time data system. It is web-based service, servers located in a single location, which provides the customer with important information and allows them to make decisions from their location of work or its origin and does not wait. the information is sent to him by e-mail or otherwise. The real-time data system uses sensitive and confidential customer data. As a result, a login authorization system and access management of the designated client file are implemented. Anyone who registers and requests access to a server data user is only authorized by a client agent or a responsible administrator. [4] After allowing a user to access the client's file in the real-time data system, the data provider may interact with a single user or with another person's real-time connection system. There are two things to consider:

1) Real-time data system enables customers to use both laptops and mobile devices. Customers, such as a tablet or smartphone, can use his real-time database login / password on his mobile phone and mobile device.

2) Although many real-time database systems operate from own workstation to the client's desktop, all computers are often identified under the same static IP address because they all use the corresponding device as a bridge. A global solution is needed to gain technical access on how to control who will use the username / password and not pass it on to another person without notification from the system administrator with real-time data. The solution must be able to detect the simultaneous use of a unique identifier / password.

The solution needed for better understanding and clarification can be divided into 3 separate subsections.

A) Technology access to how to control uses the login system.

B) Login / Password information will not be used by another person without real-time data system administrator notification.

C) Ability to detect simultaneous use of login / password.

Since the cookies are too big in this work, it is the task to ensure that cookies are not removed from the protocol, because any protocol can delete its cookies (what the user can do), then make protocol office. The best way to secure cookies is to convince users to use cookies. In this case, you can use an advertising system to advertise with specific data that varies from user to user. Moreover, these different data are available in an account only if the account is managed correctly by the server. The best way to do this is to use cookies. If users are informed of this news, they will probably not be cleaned by browser cookies. This cookie-based login authorization system, combined with a future real-time data system, can be very effective for the needs of the industry around the world [22].

V. CONCLUSION

With the technology increasement people tend to find more security for information. Hackers are accessed to computers and networks to steel information that are confidential and integrated. Privacy, protection came to special consideration. After emerging digital era concept, internet took a vital role. The cookie isn't made for security. It doesn't guarantee the security, trusty or integrity of the information. Web attacks is the main fact for lots of cybercrimes. This paper describes the cybersecurity and how cookies affect to the cyber security, what the cookie is, categorization of cookies, working process of cookies, advantages of cookies and main threats related to cookies. Cybersecurity section describes different areas of cyber security, cyber threats, prevention against cyber-attacks, cyber security breaches and cybercrimes. In the section of cyber security breaches and cyber-crimes section, reasons for cybercrimes, cybercrime effects, challenges and policy implications have been described. The correlation between cookies, privacy and cyber security reveals in this work.

VI. ACKNOWLEDGEMENT

The authors would like to thank Dr. Shalinda Adikari and Mr. Piyumal Ranawaka of Faculty of Information Technology, University of Moratuwa for supervising and guiding through out of this work.

REFERENCES

[1] K. Lacroix, Y. L. Loo and Y. B. Choi, "Cookies and Sessions: A Study of What They Are, How They Work and How They Can Be Stolen," *Proceedings - 2017 International Conference on Software Security and Assurance, ICSSA 2017,* pp. 20-24, 2018.

[2] G. Fisk, C. Ardi, N. Pickett, J. Heidemann, M. Fisk and C. Papadopoulos, "Privacy principles for sharing cyber security data," *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015,* pp. 193-197, 2015.

[3] S. Badsha, I. Vakilinia and S. Sengupta, "Privacy preserving cyber threat information sharing and learning for cyber defense," pp. 708-714, 2019.

[4] H. Wu, W. Chen and Z. Ren, "Securing cookies with a MAC address encrypted key ring," *NSWCTC 2010 - The 2nd International Conference on Networks Security, Wireless Communications and Trusted Computing,* vol. 2, pp. 62-65, 2010.

[5] A. Maqsood, M. Rizwan and F. Ahmad, Security, Trust and Privacy In Cyber (Stpc Cyber), Lahore: Department of Computer Science, Kinnaird College for Women.

[6] D. M. KRISTOL, HTTP Cookies: Standards, Privacy,, Bell Labs, Lucent Technologies, November 2001.

[7] A. M. Hormozi, "Cookies and Privacy," Taylor & Francis, 09 November 2014.

[8] R. Singh and S. Kumar, "A Study of Cookies and Threats to Cookies," DCSA PUSSGRC, Hoshiarpur, Punjab, India, March 2016.

[9] I. Ayadi, A. G. Serhrouchni and N. Simoni, "HTTP session management: Architecture and cookies security," *2011 Conference on Network and Information Systems Security, SAR-SSI 2011, Proceedings,* 2011.

[10] R. Tirtea, C. Castelluccia and D. Ikonomou, "Bittersweet cookies," ENISA – European Network and Information Security Agency.

[11] X. S. Wang, I. Herwono, F. D. Cerbo, P. Kearney and M. Shackleton, "Enabling cyber security data sharing for large-scale enterprises using managed security services," *2018 IEEE Conference on Communications and Network Security, CNS 2018,* pp. 1-7, 2018.

[12] B. Akyol, Cyber Security Challenges in Using Cloud Computing in the Electric Utility Industry, U.S. Department of Energy, September 2012.

[13] M. Patel, Cyber Security for Social Networking Sites: Issues, Challenges and Solutions, Geetanjali Institute of Technical Studies, April 2017.

[14] A. Shrivastava, Cyber Security: Issues and Privacy, Dehradun: University of Petroleum & Energy Studies, November 2015.

[15] N. Shahata, "The challenges, the threats and policy implications to a compromised privacy and security," *Proceedings - 2018 International Conference on Networking and Network Applications, NaNA 2018,* pp. 314-317, 2019.

[16] J. Singh, "Comprehensive Solution to Mitigate the Cyber-attacks in Cloud Computing," PGDAV College, University of Delhi, 2014.

[17] "cybersecurity," May 2018. [Online]. Available: https://searchsecurity.techtarget.com/definition/cybersecurity.

[18] PriceWaterhauseCoopers, "Global Economic Crime Survey," *Economic Crime people culture and controls,* 2016.

[19] M. H. Robin, "Cyber Security," North South University, 2018.

[20] B. Li, S. J. Lv, Y. S. Zhang and M. Tian, "The application research of Cookies in network security," *Proceedings of 2013 International Conference on Sensor Network Security Technology and Privacy Communication System, SNS and PCS 2013,* pp. 152-155, 2013.

[21] P. Paul, B. A. Biswas, Z. Khalid, S. Biswas, N. Dutta, H. N. Saha and M. Das, "Using Browser Cookies for Event Monitoring and User Verification of an Account," *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2018,* pp. 455-460, 2019.

[22] Y. You, J. Lee, J. Oh and K. Lee, "A Review of Cyber Security Controls from An ICS Perspective," *2018 International Conference on Platform Technology and Service, PlatCon 2018,* pp. 1-6, 2018.

[23] F. Nosheen and U. Qamar, Flexibility And Privacy Control By Cookie, Islamabad: National University of Science and Technology, February 2015.

[24] M. Degeling, C. Utz, C. Lentzsch, H. Hosseini, F. Schaub and T. Holz, Measuring the GDPR's Impact on Web Privacy, Ruhr-Universität Bochum, Germany, 16 August 2018..

[25] L. Nazaryan, C. Yue, R. Jin, O. Oksuz, B. Wang, K. Suh and A. Kiayias, "Securely outsourcing cookies to the cloud via private information retrieval," *International Conference on Wireless and Mobile Computing, Networking and Communications,* pp. 1-8, 2016.

[26] A. Aladeokin, P. Zavarsky and N. Memon, "Analysis and compliance evaluation of cookies-setting websites with privacy protection laws," *2017 12th International Conference on Digital Information Management, ICDIM 2017,* Vols. 2018-Janua, no. Icdim, pp. 121-126, 2018.