Privacy and Security Factors of Government Websites versus Private Websites in Bangladesh and USA: A Comparative Study

Merina Tanjin[1], Ishorju Agnes Botlero[1], Mourina Tasnim Hridita[1], Tawsiful Islam Riyadh[1], Md. Mehedi Hassan Onik[1(✉)], and Mahdi H. Miraz[2(✉)]

[1] Department of Computer Science, American International University-Bangladesh (AIUB), Dhaka, Bangladesh
mehedi.onik@aiub.edu, m.miraz@ieee.org
[2] School of Electrical and Computer Engineering, Xiamen University Malaysia, Sepang, Malaysia

Abstract. Security and privacy are the two most vital aspects of the modern technological evolution, to ensure the required level of trust between the customers and the service providers. Personally identifiable information (PII) is mounting at an exponential rate and so does the associated manifold security risks. In fact, there are many state-of-the-art security and privacy-preserving mechanisms in practice, however, the least developed countries (LDC) are often reluctant to maintain those security standards, in comparison to their counterparts i.e. the developed countries (DC). In addition, government managed websites in LDCs are more exposed to security and privacy vulnerabilities compared with the private sector websites. This study provides a security and privacy assessment model that can thoroughly assess government as well as private websites. To validate the proposed model, this study has selected Bangladesh as a representative of the least developed countries and United States of America (USA) for the developed countries. After a detailed empirical analysis of 20 government and private websites of each of these two countries, this study found that the majority of the public websites in LSD (Bangladesh) were less secure than the private ones, in comparison to those of the DC (USA). Several underlying factors, such as corruption, financial variances, policy issues and lack of skilled workforce in security sector, were the main reasons behind this inequality. This study also outlines some guidelines and recommendations for LDC to eradicate prevailing differences amongst public and private websites' security and privacy standards.

Keywords: Security · Privacy · Government websites · LDC · Private websites · Assessment tool

1 Introduction

As the usage of the Internet is mushrooming, websites and other internet-based applications have become a vital part of our everyday live. According to Firstsiteguide, currently

M. H. Miraz et al. (Eds.): iCETiC 2021, LNICST 395, pp. 37–55, 2021.
https://doi.org/10.1007/978-3-030-90016-8_3

(in 2021) there are more than 1.8 billion websites in the world which was 1.7 billion just one year before (in 2020) [1]. Therefore, it is evident that despite the growing number of mobile applications (apps) and other alternatives, the demand for websites is still significantly on the rise. Business organizations are not only questing for personal data but also images, voice, life style, appearance other multifaceted information. In the era of the 4th industrial revolution [2], various sectors such as healthcare, artificial intelligence (AI), robotics, the Internet of Things (IoT), genetic engineering, quantum computing [3] and more. Therefore, the security and privacy of our digital information, data and applications, have become one of the major concerns in both developed and underdeveloped countries. However, major differences have noticed for two different types of countries, particularly in terms of organizational approaches, government initiatives, infrastructure and services. Developed countries have enough financial, technological and political support, whereas least developed countries have limited resources to fight against cybercrimes.

Bangladesh has become one of the most susceptible countries in cyberspace in the recent years, its current ranking is 25th in the 15/8/2021 Global Cyber security index by International Telecommunication Union [4]. As the number of people using the internet grows in Bangladesh, so does the number of attacks (internet penetration 28.8% in 2021) [5]. In Bangladesh, the level of research conducted on privacy and security is very low, compared to the other domains. Particularly, not enough research comparing the standards, policies and strengths of the local privacy and security measures, with those of the advanced countries, was found. Therefore, cyber-security specialists, researchers and policy makers are not yet well prepared. In addition, the users of websites and mobile apps are not well aware of the privacy and security issues. Due excessive corruptions and lack of accountability in the government sectors, the government websites possess risks and vulnerabilities with regards to privacy and security aspects. On the contrary, private websites, with more traffic and adequate cyber-security team, possess comparatively lower the chance of cyber-attacks.

In this study, selected public and private websites from a least developed country (i.e. Bangladesh) as well as from a developed country (i.e. United States) were evaluated, with regards to their overall privacy and security standards. Some common security aspects, such as authentication process, password recovery process, Captcha, HTTPS, cookies sharing, privacy policies, terms and conditions, etc. were critically analyzed to support our hypothesis. Finally, the research results, including adequate statistical data with comparison and ranking for the websites of both the countries, have been presented.

2 Background Study and Literature Review

Cybersecurity deals with both security and privacy. Security deals with unauthorized access of personal information, that is, the method or tool through which our personal data is protected. On the other hand, privacy protects users' rights to control personal information through laws, regulations and technological architecture. However, both security and privacy intend to protect Personally Identifiable Information (PII) that includes contact details, phone numbers, emails, photos, health data, etc. [3]. In fact, since internet based communication, such as through websites, apps and IoT applications, has rapidly

increased in the recent past years, safeguarding users' PII has become a major concern. The main reasons for these intended or unintended privacy and security breaches are poor website and application design, mismanagement of cookies, poor encryption mechanisms, inadequate password protection mechanisms, users' negligence, backdated software, inadequate laws and regulations, lack of law enforcement, etc. [6].

In Bangladesh, government website addresses are formulated as 'XYZ.bd.gov', whereas US government website addresses takes the form of "XYZ.states.gov" [7]. However, private websites may use different domain names with variety of possible extensions such as.net,.com,.bd,.us,.org,.edu, etc. Bangladesh government is rapidly modernizing its public services, though adoption of e-governance to provide various online services to the citizens. These services are mainly provided via different government websites/portals, while some of them are through mobile apps. However, if security measures are not correctly implemented, it can result in great disaster. That is why it is critical to research various aspects of security measures on various websites.

As per the report of the Kaspersky Security Bulletin 2020, Bangladesh was globally ranked 8th where users faced the greatest risk of online infection and the rate was 13.75% [8] The Trend Micro Global Spam Map reveals that about 69.55% Bangladeshi individual users are at computer virus infection risk and about 80% users are already spam attack victims [5]. In fact, there is a recent incident of siphoning $81 million through SWIFT channel from the Federal Reserve Bank of New York account of the central bank of Bangladesh viz. Bangladesh Bank, which was supposedly linked to a customized malware attack [5]. Therefore, banks in Bangladesh needs to implement appropriate security measures, particularly with regards to intrusion prevention and detection [5]. In December 2020, three Bangladeshi local private banks reportedly faced major cyberattacks. Considering three such attacks within the short time span of only one month, has raised great concern regarding the strength of their security systems to withstand the escalating threats from scammers [5]. Out of those three banks, the largest victim was Dutch Bangla Bank Limited (DBBL) resulting in a loss of approximately $3 million by the local as well as global cybercriminals [9]. However, the remaining two banks claimed that they could somehow ward off the financial losses [10]. As a matter of fact, numerous Bangladeshi government websites, such as those of the president's as well as the prime minister's offices, were hacked as well [11].

On the contrary, number of cyberattacks in the USA are less than that of Bangladesh. However, cyber-attacks and privacy breaching is also a common phenomenon there. In May 2021, the chief of the U.S. Cyber Command revealed that the number of operations conducted by them surpassed two dozen operations, in order to resist foreign cyber threats anterior to the 2020 U.S. elections. Amongst them, 11 forward hunt operations were conducted in nine different territories [12]. In 2017, a group of hackers, suspected to be Russian origin, breached U.S. State Department's email server and gained illegitimate access to thousands of confidential emails [13]. Another remarkable attack was conducted by some Iranian hackers, targeting to heist the credentials of some lead medical researchers, particularly oncologists, neurologists as well as geneticists, of both the USA and Israel [14].

There is hardly any website which can be considered as completely secure and without the risk of being exploited. Nonetheless, web services have become so intertwined

into our daily lives that we have been accustomed to storing and sharing vast amounts of personal information on the internet. In this context, the goal of this research is to provide a strategy for detecting maximal web-application vulnerabilities with minimal expense and effort. It has assessed the vulnerabilities of the chosen Bangladeshi websites against a collection of the most popular and prevalent attack vectors using penetration testing and source code analysis methodologies, which respectively constitute black box as well as white box testing [15] introduced a script that demonstrates how to trade off the application's security requirements. SQL infusion and cross website scripting are two examples of client-side embedded scripts for web interactions. Before they have an impact on the security and classification of the information, such attacks must be identified and evacuated [16]. Computers, projectors, printers, smart watches, smart phones, refrigerators, washing machines and other Internet-connected smart applications are vulnerable to a variety of threats and vulnerabilities. There has been a recent rise in deploying HTTPS protocol, instead of classical HTTPS, for secure communicate and transactions. Meanwhile, the number of browser-trusted certificate authority has increased, while baseline certificate issuing due diligence has decreased [17]. Our study also investigates HTTPS protocol and SSL certificate for ensuring user privacy. The number of services offered by the USA government websites is continuously growing, yet customers are concerned about their personal information being protected. In fact, findings of a study [18] which looked at the privacy policies of 50 USA Senate websites, reveals that only few of them had complete privacy policies in place. The study also identified there is an overall lack of protection of personal data in most of the cases.

3 Proposed Method

Figure 1 illustrates the steps followed this study for investigating the privacy and security aspects of the selected websites. Popular and mostly used ten websites from the government and private sectors of both Bangladesh and USA were selected by this study. Four privacy factors, i.e. (i) password authentication, (ii) privacy policy and law, (iii) third-party data sharing policy and (iv) data access, delete and modification right, were considered.

3.1 Privacy Assessment

A password is one of the authentication mechanisms, which belong to the 'something we know' category. A password is fundamentally a shared secret phrase between the service provider and the user. It is assumed that the password will not be disclosed with any third-party by either the user or the service provider. Thus, it provides the mechanism to authenticate a legitimate user and grant access to the desired services through the website or app. For smooth delivery of services, the security of a password is of paramount importance. Our privacy assessment tool has identified six crucial heuristics for password authentication (PA), i.e. P.1: Password Construction Guidelines, P.A2: Password Recovery, P.A3 CAPTCHA, P.A4: Security Question, P.A5: HTTPS Channel, P. A6: Password Strength Meter. The other factors include: third party data sharing and privacy policy. All the aforementioned factors are investigated by exploring each of the

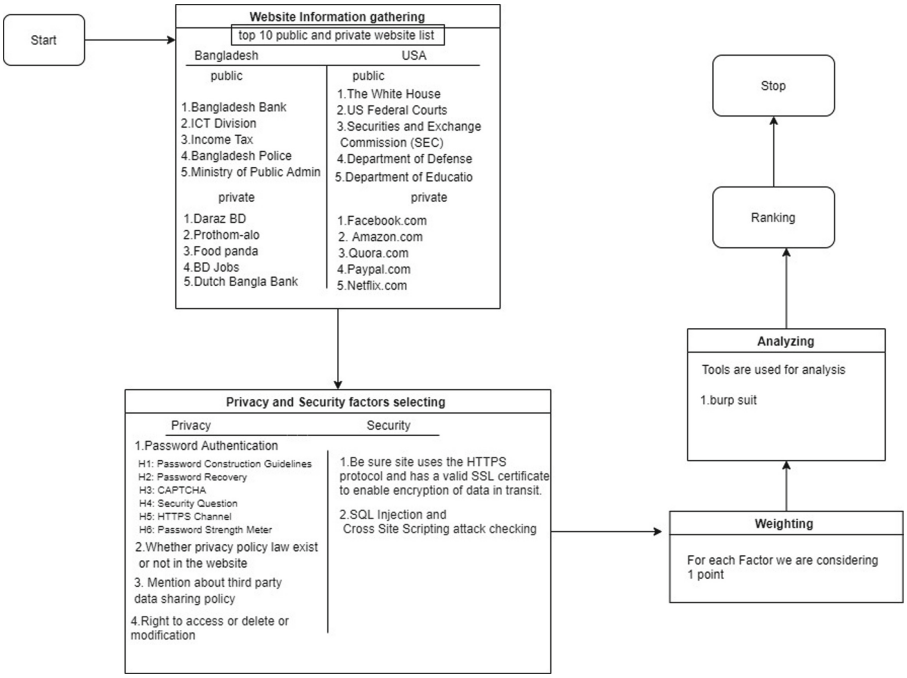

Fig. 1. Architecture of analyzing privacy and security factors

websites considered by this study. Various security measures, such as email verification, user privacy policy and third-party data sharing, have been rigorously investigated.

3.2 Security Assessment

For security purpose, SQL injection and cross-site scripting attack, SSL certificate, cookies collection numbers and HTTPS protocols have been analyzed. Cross-site scripting (XSS) is a client-side code injection technique. In XSS, malicious scripts are injected by the cybercriminals into the web applications, to exploit the system. This is done through inserting scripts via the data input field of any websites, which accepts data without proper validation. These scripts are treated as the source codes of the targeted [15]. Burp Scanner is a tool which can automatically crawl and scan various websites for collecting contents and identifying possible vulnerabilities. Depending on the configuration, the scanner has the capability to discover the contents and functionalities and audit to determine vulnerabilities [19]. SQL injection is considered as the most vulnerable threat because it can exploit the entire database running behind any web application [20]. SQL injection attacks are administered at the application level, regular firewall and or intrusion detection systems (IDS), placed at the network layer, fails to withstand such attacks [21]. If a script is vulnerable, the attacker can put malicious input to alter the SQL statements. To check vulnerability, concatenated 'OR 1 = 1' in the URL. So, after the input the query becomes like:

Query – SELECT id FROM users WHERE username = 'ABC' AND password = '123' OR 1 = 1. To analyze SSL certificate, HTTPS protocol and cookies, all the selected websites were individually visited and tested rigorously to ensure high accuracy of the results of this study.

Table 1 lists the notation with description which were used in calculation equations. The overall risk level notations are also included. Table 2 presents the websites ranking levels whereas Table 3 represent the calculation equations for the websites which were used for the ranking purpose.

Table 1. Notation table

Factors		Risk level	
Notation	Description	Notation	Description
Pf	Privacy factor	High	Privacy and security status of chosen websites is strong
Sf	Security factor		
Pf1	Password authentication		
Pf2	Privacy policy law	Medium	Privacy and security status of chosen websites is average

Table 2. Overall websites' rankings

	Low	Medium	High
High	Medium	High	Highest
Medium	Low	Medium	High
Low	Lowest	Low	Medium

Table 3. Privacy factors checking of USA and Bangladesh government websites

Equations	Use
For 1st Website, $W_1P_f = (P_{f1} + P_{f2} + P_{f3})$ $W_1S_f = (S_{f1} + S_{f2} + S_{f3})$ Similarly for Nth websites, $W_nP_f = (P_{f1n} + P_{f2n} + P_{f3n})$ $WnSf = (S_{f1n} + S_{f2n} + S_{f3n})$	In terms of privacy factor: [Sorting from high to low ($W_1P_fP_{fn}$……$W_nP_fP_{fn}$)] In terms of security factor: [Sorting from high to low ($W_1S_fS_{fn}$……$W_nS_fS_{fn}$)]

4 Result and Analysis

In this part of the research, we counted the number of privacy factors fulfilled by each of the investigated websites for both Bangladesh (private government) and the USA

(private government). Here, S = secure, NS = not secure, NA = not available, A = available (Table 4 and Table 5). Table 4 presents the overall state of privacy factors in the government websites of Bangladesh and those of the USA. Overall Password authentication states in both cases are almost similar but the privacy policy deemed to be better in the USA websites than those of Bangladesh.

Table 4. Privacy factors checking of USA and Bangladesh government websites

Bangladeshi govt. websites								
	Password authentication guidelines	Password recovery	Captcha	Security question	HTTPS channels	Password strength meter	Privacy third party	Privacy policy law
Passport [22]	S	S	S	NS	S	NS	NA	NA
Income Tax [23]	NS	S	S	S	S	NS	S	A
Bangladesh Police [24]	S	S	S	NS	S	NS	NA	NA
Teletalk [25]	S	S	S	NS	S	NS	NS	A
National University [26]	S	S	NS	NS	S	NS	NA	NA
USA Govt. websites								
US Federal Courts [27]	S	S	NS	NS	S	NS	S	A
Securities and Exchange Commission (SEC) [28]	S	S	NS	NS	S	NS	NS	A
Department of Defense [29]	S	S	NS	NS	S	NS	NS	A
Department of Education [30]	NA	NA	NA	NA	NA	NA	NS	A
The White House [31]	NA	NA	NA	NA	NA	NA	NS	A

4.1 Total Calculation for Privacy (Government Websites)

Weighting: Here, in Table 4 and Table 5, secure/available = 1, not secure/not available = 0. From the previous equation as shown in Table 3, $W_1P_n = (P_{f1}n + P_{f2}n + P_{f3}n)$.

- **For Bangladesh government website*:*** (Calculating total weight (0/1) of each privacy factors for Bangladesh government websites) *Web1(Passport) = ((1 + 1 + 1 + 0 +*

1 + 0) + 0 + 0) = 4, Web2(Income Tax) = [(0 + 1 + 1 + 1 + 1 + 0) + 1 + 1] = 6, Web3 (Bangladesh Police) = [(1 + 1 + 1 + 0 + 1 + 0) + 0 + 0] = 4, Web4(Teletalk) = [(1 + 1 + 1 + 0 + 1 + 0) + 0 + 1] = 5, Web5(National University) = [(1 + 1 + 0 + 0 + 1 + 0) + 0 + 0] = 3

$$\textbf{Total calculation},\ W_5P_f\ =\ (4\ +\ 6\ +\ 4\ +\ 5\ +\ 3)\ =\ 22 \tag{1}$$

- **For the USA government website:** (Calculating total weight (0/1) of each privacy factors for the USA government websites) *Web1(US Federal Courts) = [(1 + 1 + 0 + 0 + 1 + 0) + 1 + 1] = 5, Web2 (Securities and Exchange commission (SEC)) = [(1 + 1 + 0 + 0 + 1 + 0) + 0 + 1] = 4, Web3 (Department of Defense) = [(1 + 1 + 0 + 0 + 1 + 0) + 0 + 1] = 4, Web4(Department of Education) = [(0 + 0 + 0 + 0 + 0 + 0) + 0 + 0] = 0, Web5(The White House) = [(0 + 0 + 0 + 0 + 0 + 0) + 0 + 0] = 0*

$$\textbf{Total calculation},\ W_5P_f\ =\ (5+4+4+0+0)\ =\ 13 \tag{2}$$

Here, S = secure, NS = not secure, A = available. Table 5 represents the scenario of privacy factors in private sector websites of both Bangladesh and the USA. The overall result shows similar trends in both the cases.

4.2 Total Calculation for Privacy (Private Websites)

Weighting: Here, secure/available = 1, not secure/not available = 0.

- **For Bangladeshi private websites:** (Calculating total weight (0/1) of each privacy factors for Bangladesh private websites) *Web1(Daraz BD) = [(1 + 1 + 0 + 0 + 1 + 0) + 0 + 1] = 4, Web2(Prothom Alo) = [(1 + 1 + 1 + 0 + 1 + 0) + 0 + 1] = 5, Web3 (Food Panda) = [(1 + 1 + 0 + 0 + 1 + 0) + 0 + 1] = 4, Web4(BD Jobs) = [(1 + 1 + 1 + 0 + 1 + 1) + 0 + 1] = 6, Web5(DBBL) = [(1 + 1 + 0 + 0 + 1 + 0) + 0 + 1] = 4.*

$$\textbf{Total calculation},\ W_5P_f\ =\ (4\ +\ 5\ +\ 4\ +\ 6\ +\ 4)\ =\ 23 \tag{3}$$

- **For the USA Private website***: (*Calculating total weight (0/1) of each privacy factors for USA private websites) *Web1(Facebook) = [(1 + 1 + 0 + 0 + 1 + 0) + 0 + 1] = 4, Web2 (Amazon) = [(1 + 1 + 0 + 0 + 1 + 0) + 0 + 1] = 4, Web3 (Quora) = [(1 + 1 + 1 + 0 + 1 + 0) + 0 + 1] = 5, Web4(Paypal) = [(1 + 1 + 1 + 1 + 1 + 0) + 0 + 1] = 6, Web5(Netflix) = [(1 + 1 + 1 + 0 + 1 + 0) + 0 + 1] = 5*

$$\textbf{Total calculation},\ W_5P_f\ =\ (4\ +\ 4\ +\ 5\ +\ 6\ +\ 5)\ =\ 25 \tag{4}$$

Here in Table 6, S = secure, V = valid. Table 6 represents the scenario of security factors with regards to the private sector websites of both Bangladesh and the USA. The overall result demonstrates a similar outcome in both cases.

Similarly, we counted the number of security factors satisfied by each of the investigated websites for both Bangladesh (private & government) and the USA (private & government).

Table 5. Privacy factors checking of USA and Bangladesh private websites

Bangladeshi private websites								
	Password authentication guidelines	Password recovery	Captcha	Security question	HTTPS channels	Password strength meter	Privacy third party	Privacy policy law
DarazBD [32]	S	S	S	NS	S	NS	NA	NA
ProthomAlo [33]	NS	S	S	S	S	NS	S	A
Food-Panda [34]	S	S	S	NS	S	NS	NA	NA
BD-Jobs [35]	S	S	S	NS	S	NS	NS	A
Dutch Bangla Bank [36]	S	S	NS	NS	S	NS	NA	NA
USA private websites								
Facebook [37]	S	S	NS	NS	S	NS	S	A
Amazon [38]	S	S	NS	NS	S	NS	NS	A
Quora [39]	S	S	NS	NS	S	NS	NS	A
Paypal [40]	NA	NA	NA	NA	NA	NA	NS	A
Netflix [41]	NA	NA	NA	NA	NA	NA	NS	A

Table 6. Security factors checking of USA and Bangladesh private websites

Bangladeshi private websites					
	SSL certificate	Cookies used	HTTPS protocol status	XSS attack	SQL injection
Daraz BD	V	42	Yes/1	S	S
Prothom Alo	V	15	Yes/1	S	S
Food Panda	V	21	Yes/1	S	S
BD Jobs	V	21	Yes/1	S	S
Dutch Bangla bank	V	4	Yes/1	S	S
USA private websites					
Facebook	V	8	Yes/1	S	S
Amazon	V	13	Yes/1	S	S
Quora	V	18	Yes/1	S	S
Paypal	V	102	Yes/1	S	S
Netflix	V	23	Yes/1	S	S

4.3 Total Calculation for Security Factor (Private Websites)

Here, secure/available = 1, not secure/not available = 0.

From the previous equation, as shown in Table 3, $W_1S_n = (S_{f1n} + S_{f2n+} S_{f3n})$.

- ***For Bangladesh private website:*** *(Calculating total weight (0/1) of each security factors for Bangladesh private websites. Web1(Daraz BD) = [1 + (1 + 1) + (1 + 1)] = 5, Web2(Prothom Alo) = [1 + (1 + 1) + (1 + 1)] = 5, Web3(Food Panda) = [1 + (1 + 1) + (1 + 1)] = 5, Web4(BD Jobs) = [1 + (1 + 1) + (1 + 1)] = 5,Web5(DBBL) = [1 + (1 + 1) + (1 + 1)] = 5*

$$\textbf{Total equation},\ W_5S_f = (5 + 5 + 5 + 5 + 5) = 30 \tag{5}$$

- **For USA private websites:** (Calculating total weight (0/1) of each security factors for the USA private websites). *Web1(Facebook) = [1 + (1 + 1) + (1 + 1)] = 5, Web2 (Amazon) = [1 + (1 + 1) + (1 + 1)] = 5, Web3 (Quora) = [1 + (1 + 1) + (1 + 1)] = 5, Web4(Paypal) = [1 + (1 + 1) + (1 + 1)] = 5, Web5(Netflix) = [1 + (1 + 1) + (1 + 1)] = 5*

$$\textbf{Total calculation},\ W_5S_f = (5 + 5 + 5 + 5 + 5) = 30 \tag{6}$$

Here in Table 7, S = secure, NS = not Secure, V = valid = V, NV = not valid. Table 7 represents the scenario of security factors in the government sector websites of both Bangladesh and the USA. In both cases, a similarity is observed with regards to the implementation of SSL certificate and HTTPS protocols. But in case of security attacks, Bangladeshi websites are comparatively more vulnerable as the USA websites were found to be comparatively more secure.

SSL = secure sockets layer, HTTPS = Hyper Text Transfer Protocol Secure, XSS Cross Site Scripting

4.4 Total Calculation for Security (Government Websites)

- ***For Bangladeshi government websites:*** (Calculating total weight (0/1) of each security factors for Bangladesh government websites.) *Web1(Passport) = [0 + (1 + 1) + (0 + 0)] = 2, Web2(Income Tax) = [1 + (1 + 1) + (0 + 0)] = 3, Web3 (Bangladesh Police) = [1 + (1 + 1) + (1 + 0)] = 4, Web4(Teletalk) = [1 + (1 + 1) + (1 + 0)] = 4,Web5(National University) = [1 + (1 + 1) + (0 + 0)] = 3*

$$\textbf{Total calculation},\ W_5S_f = (2 + 3 + 4 + 4 + 3) = 16 \tag{7}$$

- ***For USA government websites*:** (Calculating total weight (0/1) of each security factors for USA government websites.) *Web1(US Federal Courts) = [1 + (1 + 1) + (1 + 1)] = 5, Web2 (Securities and Exchange Commission (SEC)) = [1 + (1 + 1) + (1 + 1)] = 5, Web3 (Department of Defense) = [1 + (1 + 1) + (1 + 1)] = 5, Web4(Department of Education) = [1 + (1 + 1) + (1 + 1)] = 5, Web5(The White House) = [1 + (1 + 1) + (1 + 1)] = 5*

$$\textbf{Total calculation},\ W_5S_f = (5 + 5 + 5 + 5 + 5) = 30 \tag{8}$$

Table 7. Security factors checking of USA and Bangladesh government websites

Bangladeshi govt. websites					
	SSL certificate	Cookies used	HTTPS protocol status	XSS attack	SQL injection
Passport	NV	29	Yes/1	NS	NS
Income Tax	V	4	Yes/1	NS	NS
Bangladesh Police	V	5	Yes/1	S	NS
Teletalk	V	33	Yes/1	S	NS
National University	V	2	Yes/1	NS	NS
USA Govt. websites					
US Federal Courts	V	7	Yes/1	S	S
Securities and Exchange Commission (SEC)	V	18	Yes/1	S	S
Department of Defense	V	17	Yes/1	S	S
Department of Education	V	5	Yes/1	S	S
The White House	V	4	Yes/1	S	S

Figure 2 shows the percentage of cookies used in private websites in both the USA and Bangladesh. In the USA the rate of acceptance of cookies is highest in PayPal comparing to the other websites. In Bangladesh, Daraz BD accepts the highest cookies. The number of other Bangladeshi websites also accept similar number of cookies as Daraz BD, which is comparatively more than those in the USA. note that the first paragraph of a section or subsection is not indented. The first paragraphs that follows a table, figure, equation etc. does not have an indent, either.

Figure 3 shows the percentage of cookies used in public sector websites in both the USA and Bangladesh. In the USA, the rate of acceptance of cookies is highest in the website of the Security and Exchange Commission, followed by that of the Department of Defense, both of which are higher than the other websites. Amongst the Bangladeshi ones, Passport as well as Income Tax websites are ranked the top two in accepting number of cookies. The remaining ones accepts little less cookies, however, the exhibit a similar trend. First Section

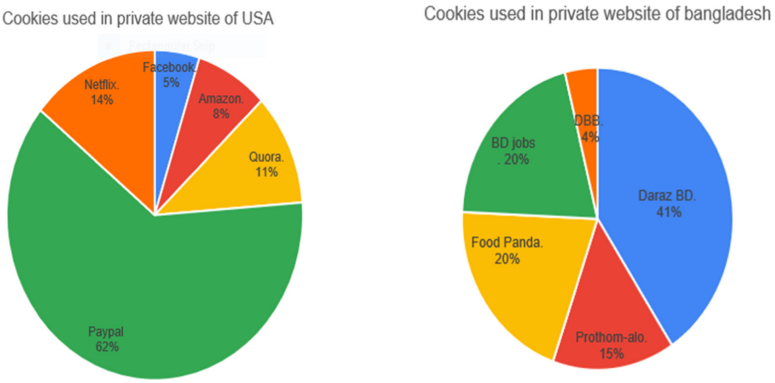

Fig. 2. Cookies of private websites (USA and Bangladesh)

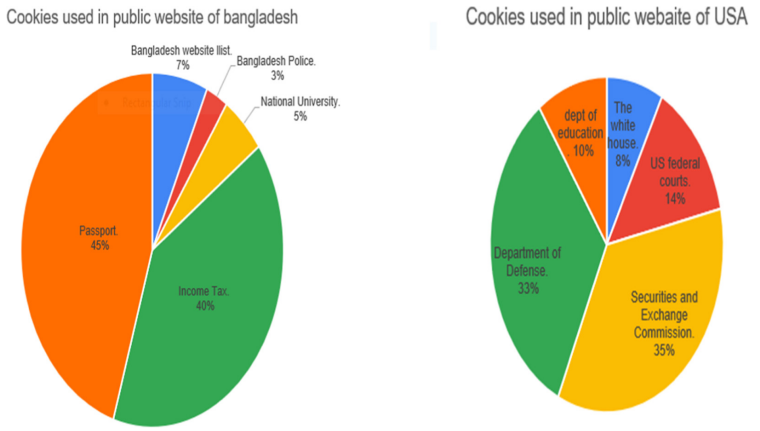

Fig. 3. Cookies of government websites (USA and Bangladesh)

4.5 Total Weight Calculation

Bangladesh government websites:

$$\left(P_f + S_f\right) = 22 + 16 = 38 \qquad (1) + (7)$$

Bangladesh private websites:

$$\left(P_f + S_f\right) = 23 + 30 = 53 \qquad (3) + (5)$$

USA government websites:

$$\left(P_f + S_f\right) = 13 + 30 = 43 \qquad (2) + (8)$$

USA private websites:

$$\left(P_f + S_f\right) = 24 + 30 = 54 \qquad (4) + (6)$$

4.6 A Risk Level Analysis

Low = 1–40, Medium = 41–50, High = 50–70 (range level by total factors point). This table (Table 8) shows the final result of the selected websites' privacy and security status by calculating total weight. As it can be seen from the results, the private websites are more secure than the government ones for both Bangladesh and the USA.

Table 8. Overall websites ranking

	Low	Medium	High
Bangladesh government websites	✓		
Bangladesh private websites			✓
USA government websites		✓	
USA private websites			✓

4.7 Website Ranking

Table 9 shows the ranking of the websites according to the privacy factors rating. Table 10 shows the ranking of the websites according to the security factors rating.

Table 9. Privacy-based website rankings (BD and USA)

Bangladesh government website	USA private website
1. Income Tax (6) 2. Teletalk (5), 3. Passport, Bangladesh Police (4) 4. National University (3)	1. US Federal Courts (5) 2. Securities and Exchange Commission (SEC), Department of Defence (4) 3. Department of Education, The White House (0)
Bangladesh private Website	USA private Website
1. BD Jobs (6) 2. Prothom Alo (5), 3. Daraz BD, Food Panda, DBBL (4)	1. Paypal (6) 2. Quora, Netflix (5) 3. Facebook, Amazon (4)

Table 10. Security-based website rankings (BD and USA)

Bangladesh government website	USA government website
1. Bangladesh Police, Teletalk (4) 2. National University (3) 3. Passport (2)	1. US Federal Courts, Securities and Exchange Commission (SEC), Department of Defence, Department of Education, The White House (5)
Bangladesh private website	USA private website
1. Prothom Alo, BD Jobs, Daraz BD,Food Panda, DBBL (5)	1. Paypal, Quora, Netflix, Facebook, Amazon (5)

5 Discussion

In this research, a comparison study of privacy and security factors of the government and private sector websites of both Bangladesh and the USA. From the results of the study, it is evident that the private sector websites outperform the government websites, in terms of maintaining security and privacy aspects, for both of the countries. Analysis of the privacy and security factors reveals the following:

5.1 Privacy Factors

- Financial Issue: From the analysis of our study it is noticeable that the Bangladesh government allocates less funds than the USA, for the purpose of websites' security and privacy aspects. For IT sector's spending of the U.S. federal government, $92.17 billion has been allocated in the 2021 fiscal year budget. The Civilian agencies budgeted $54.36 billion for federal IT spending, while the Department of Defense, a single agency, had the largest funding of $38.8 billion for IT spending as [42]. Considering the financial strength of Bangladeshi, it is neigh impossible to have such a large budget for IT. That being said, the Bangladesh government's budget allocation of $17.2 billion in 2021–2022 fiscal year for the ICT sector is very impressive, which is in fact about 20 percent higher compared to the original budget of the outgoing fiscal year (2019–2020) [43]. Although Bangladesh is gradually expanding its budget allocation for IT sectors, it is still comparatively very low with regards to that of the USA. On the other hand, the local private organization operating in Bangladesh tend to spend comparatively more money for their websites than the government websites, however, the amount is still much less than those of the USA private organizations. For instance, one of the most renowned private e-commerce in Bangladesh, namely Daraz BD, announced to invest 58,948,850.00 $ in 2021 [44] whereas Amazon spent $45.903 billion in the twelve months' time span ending March 31, 2021. This was a 22.97% increase in Amazon's budget compared to the preceding year [45].
- Fewer number of Visitor: In the first 6 months (Feb–July) of 2021, The websites of the government had 90.74k visitors [46] whereas there were 5.29 billion visits to the USA government websites over the past 90 days (April 2021–June 2021) [47]. Therefore, the large difference in the number of visitors between both the countries is clearly distinguishable.

- On the contrary, the total engagement of the Daraz BD website in 6 months is 6.80M [48] while it is 2.72 billion for Amazon [49].
- Maintenance: For the government websites, the maintenance process, such as information updating, security checking, speed optimization, etc. in Bangladesh is much slower than the USA. Figure 4 demonstrates the statistics for daily visitors for the USA government websites. Bangladesh government does not publicly disclose any such information.

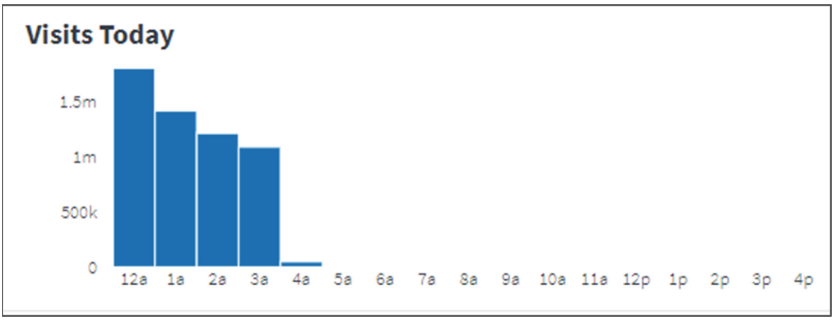

Fig. 4. USA daily website visitor's statistics [47]

5.2 Security Factors

- Vulnerabilities: In 2021 as shown in Fig. 5 till now the most cyber incidents cases were registered in December, 2020.

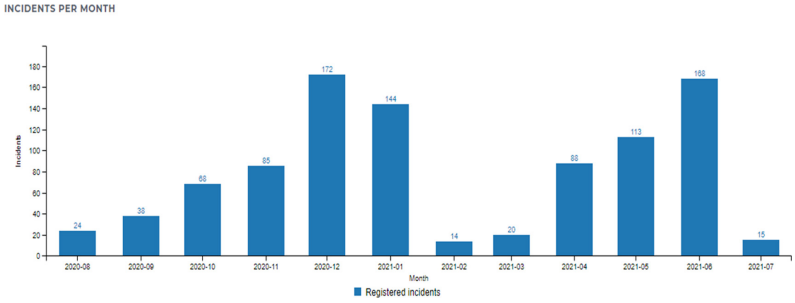

Fig. 5. Bangladesh cyber-attack statistics from 2020–2021 [50]

On the contrary, the cyber security market size of the USA was valued $167.13 billion in 2020 and is predicted to have a 10.9% increase in the compound annual growth rate (CAGR), from 2021 to 2028. In fact, such growth can be attributed to the growing sophistication of the cybercrimes (see Fig. 6).

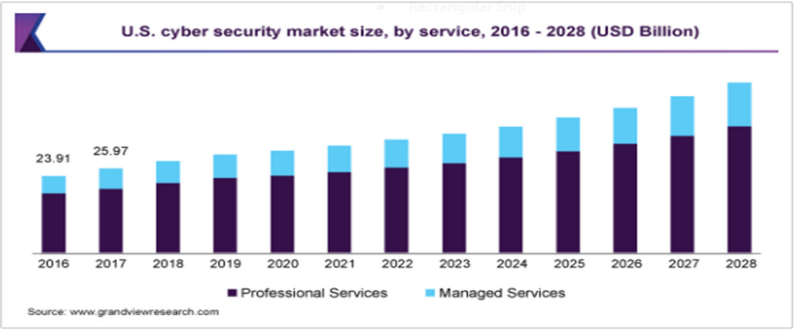

Fig. 6. USA cyber security market size statistics [51]

- Awareness: Fig. 7 represents the findings of a survey [16] which was conducted amongst the internet users of Bangladesh. The respondents were day-to-day internet users from various kinds of professions.

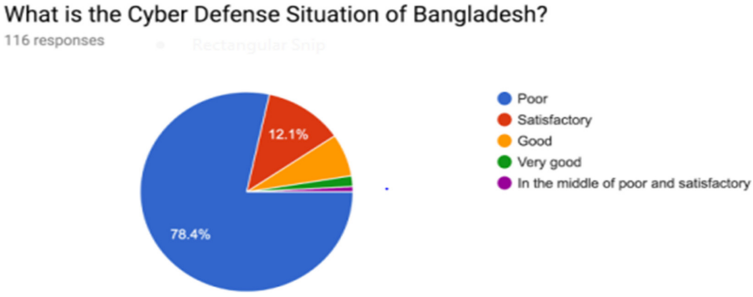

Fig. 7. Bangladesh cyber defense statistics

From the findings of our study, it is clearly noticeable that USA government websites are more secure and protected than Bangladesh government websites. From the calculations and analysis, it is evident that Bangladesh government websites are highly vulnerable with regards to both privacy and security factors. In most websites, password authentication, privacy policy and third-party data sharing is either weak or not available. On the other hand, most of the USA government websites are highly secure and impregnable. However, the private sectors websites in both the countries were found to be similarly secure and reliable, while USA is slightly leading the race. Although http protocols and SSL certificates are available for all the websites of Bangladesh government, most of them are vulnerable for SQL injection and Cross-site Scripting attack. Some of the websites also demand unnecessary cookies. Nevertheless, USA government websites are impenetrable. Security factors for private websites of both countries are as stable as USA government websites.

Finally, based on the outcome of this study, the followings are the recommendations to improve the security and privacy factors for the both countries:

1. Government agencies must be aware of the need to address such flaws and must take the required actions to strengthen the security of these web applications.
2. It is essential to tighten the security of the respective web servers, to prevent the vulnerabilities identified in this research. The foremost tasks in achieving this is to make sure all the plug-ins, libraries, database server software, etc. are always kept up-to-date, particularly by applying the security patches supplied by the vendors.
3. While designing, developing and deploying the websites, the developers must concentrate on the prospective requirements and how to quickly deal with them.

6 Conclusions

The article presented a comparative study of security and privacy aspects of the government and private sector websites of the least developed countries (LDC) vs. the developed countries (DC). While Bangladesh has been chosen as the representative of the LDC, the USA was nominated to represent the DC. Based on the usage and popularity, the websites were selected for inclusion in this study. To ensure representativeness of the sample, a wide variety of government and private sectors websites from both countries were considered, such as government services, news and media, banks, defense, e-commerce, etc. The key goal of the study was to find the most susceptibility and user privacy amongst the selected web services with the least amount of effort, to aid tasks of the future developers and software testers. Most of the selected web applications in this study from Bangladesh, particularly the government ones displayed major security risks and lack user privacy, which need to be resolved with utmost urgency. The USA websites showed comparatively better performance in this regard. In the future, we would like to explore a variety of other web services employing a broader set of vulnerabilities as well as new attack vectors.

References

1. Djuraskovic, O.: How-many-websites. https://firstsiteguide.com/how-many-websites/. Accessed 08 Mar 2021
2. Saad, M., et al.: Exploring the attack surface of blockchain: a comprehensive survey. IEEE Commun. Surv. Tutor. **22**, 1977–2008 (2020). https://doi.org/10.1109/COMST.2020.2975999
3. Onik, M.M.H., Kim, C.-S., Lee, N.-Y., Yang, J.: Privacy-aware blockchain for personal data sharing and tracking. Open Comput. Sci. **9**, 80–91 (2019). https://doi.org/10.1515/comp-2019-0005
4. Global Cybersecurity Index ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. Accessed 05 May 2021
5. Chaudhry, J., Qidwai, U., Miraz, M.H., Ibrahim, A., Valli, C.: Data security among ISO/IEEE 11073 compliant personal healthcare devices through statistical fingerprinting. Presented at the (2017)
6. Onik, M.M.H., Chul-Soo, K.I.M., Jinhong, Y.: Personal data privacy challenges of the fourth industrial revolution. In: 2019 21st International Conference on Advanced Communication Technology (ICACT), pp. 635–638. IEEE (2019). https://doi.org/10.23919/ICACT.2019.8701932

7. Abu-Shanab, E.A., Baker, A.N.A.: Evaluating Jordan's e-government website: a case study. Electron. Gov. Int. J. **8**, 271–289 (2011)
8. Kaspersky: Kaspersky Security Bulletin 2020 Statistics, 26 (2020)
9. Akinbowale, O.E., Klingelhöfer, H.E., Zerihun, M.F.: Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature. J. Financ. Crime (2020). https://doi.org/10.1108/JFC-03-2020-0037
10. Joveda, N., Khan, M.T., Pathak, A., Chattogram, B.: Cyber laundering: a threat to banking industries in Bangladesh: in quest of effective legal framework and cyber security of financial information. Int. J. Econ. Financ. **11**, 54–65 (2019). https://doi.org/10.5539/ijef.v11n10p54
11. UNB: Several government websites hacked. https://www.thedailystar.net/country/bangladesh-government-websites-hacked-demanding-quota-system-reform-1561267. Accessed 10 Apr 2021
12. Gazis, O.: U.S. launched "more than 2 dozen" cyber operations to protect election. https://www.cbsnews.com/news/election-interference-us-cyber-command-nsa-nakasone/. Accessed 13 May 2021
13. Baezner, M., Robin, P.: Cyber-conflict between the United States of America and Russia
14. Jasper, S.E.: U.S. Cyber threat intelligence sharing frameworks. Int. J. Intell. Count. Intell. **30**, 53–65 (2017). https://doi.org/10.1080/08850607.2016.1230701
15. Moniruzzaman, M., Chowdhury, F., Ferdous, M.S.: Measuring vulnerabilities of Bangladeshi websites. In: 2nd International Conference on Electrical, Computer and Communication Engineering, ECCE 2019 (2019). https://doi.org/10.1109/ECACE.2019.8679426
16. Dikhit, A.S., Karodiya, K.: Result evaluation of field authentication based SQL injection and XSS attack exposure. In: IEEE International Conference on Information, Communication, Instrumentation and Control, ICICIC 2017, 1–6 January 2018 (2018). https://doi.org/10.1109/ICOMICON.2017.8279148
17. Clark, J., Van Oorschot, P.C.: SoK: SSL and HTTPS: revisiting past challenges and evaluating certificate trust model enhancements. In: Proceedings of IEEE Symposium on Security and Privacy, pp. 511–525 (2013). https://doi.org/10.1109/SP.2013.41
18. Kuzma, J.: An examination of privacy policies of US Government Senate websites. Electron. Gov. **7**, 270–280 (2010). https://doi.org/10.1504/EG.2010.033592
19. Kim, J.: Burp suite: automating web vulnerability scanning (2020)
20. Natarajan, S.: Available Online through CODEN : IJPTFI Research Article. 8, 25990–25994 (2017)
21. Salih, A.K., Yousif, M.: Dynamic analysis tool for detecting SQL injection dynamic analysis tool for detecting SQL injection. Int. J. Comput. Sci. Inf. Secur. **14**, 224–232 (2016)
22. Passport. http://www.dip.gov.bd/. Accessed 10 Mar 2021
23. IncomeTax. https://nbr.gov.bd/publications/income-tax/eng. Accessed 10 Mar 2021
24. BangladeshPolice. https://www.police.gov.bd/. Accessed 10 Mar 2021
25. Teletalk. https://www.teletalk.com.bd/bn/. Accessed 10 Mar 2021
26. NU. https://www.nu.ac.bd/. Accessed 02 May 2021
27. US court. https://www.uscourts.gov/. Accessed 10 Mar 2021
28. SEC. https://www.sec.gov/. Accessed 05 Mar 2021
29. Defense. https://www.defense.gov/. Accessed 21 Apr 2021
30. USEducation. https://www.ed.gov/. Accessed 10 May 2021
31. WhiteHouse. https://www.whitehouse.gov/. Accessed 10 Mar 2021
32. Daraz. https://www.daraz.com.bd/. Accessed 16 May 2021
33. Prothom-Alo. https://www.prothomalo.com/. Accessed 10 Mar 2021
34. Food-panda. https://www.foodpanda.com.bd/. Accessed 10 Mar 2021
35. BD jobs. https://www.bdjobs.com/. Accessed 10 Mar 2021
36. DBBL. https://www.dutchbanglabank.com/. Accessed 10 Mar 2021

37. Facebook. https://www.facebook.com/. Accessed 10 Mar 2021
38. Amazon. https://www.amazon.com/. Accessed 10 Mar 2021
39. Quora. https://www.quora.com. Accessed 10 Mar 2021
40. Paypal. https://www.paypal.com/. Accessed 10 Mar 2021
41. Netfllix. https://www.netflix.com. Accessed 10 Mar 2021
42. Mlitz, K.: U.S. federal government IT expenditure 2011–2021. https://www.statista.com/statistics/506409/united-states-federal-it-expenditure/. Accessed 08 Apr 2021
43. Kabir, S.A.: Budget for building Digital Bangladesh (2021). https://www.thedailystar.net/business/economy/news/budget-building-digital-bangladesh-2110485
44. Correspondent, S.: Daraz to invest Tk 500 crore in infrastructure development. https://www.newagebd.net/article/107500/daraz-to-invest-tk-500-crore-in-infrastructure-development. Accessed 08 Apr 2021
45. Amazon Research and Development Expenses 2006–2021. https://www.macrotrends.net/stocks/charts/AMZN/amazon/research-development-expenses. Accessed 03 June 2021
46. Total Visits to bangladesh.gov.bd. https://www.similarweb.com/website/bangladesh.gov.bd/. Accessed 10 Mar 2021
47. analytics.usa.gov. https://analytics.usa.gov/. Accessed 10 Apr 2021
48. Similarweb. https://www.similarweb.com/website/daraz.com.bd/. Accessed 22 Mar 2021
49. Similarweb Amazon. https://www.similarweb.com/website/amazon.com/. Accessed 09 Mar 2021
50. Bangladesh cyber attack. https://www.cirt.gov.bd/incident-reporting/statistics/. Accessed 20 May 2021
51. Cyber Security. https://www.grandviewresearch.com/industry-analysis/cyber-security-market. Accessed 15 Apr 2021